SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:4777–4803
Published online 17 October 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1642

REVIEW ARTICLE

Comprehensive analysis of the authentication methods in wireless body area networks

Mohammad Masdari* and Safiyeh Ahmadzadeh

Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

ABSTRACT

WBANs are of the promising technologies, applied in the e-healthcare systems, for extracting and transferring critical medical data from patient body. In WBANs, the privacy and integrity of the patient's private medical data are very important, as a result, the WBANs communications and even communication with other E-Healthcare components should be authenticated and secured. This paper provides a complete survey and analysis of the various authentication schemes proposed in the literature to improve the WBANs security. Besides, it classifies the proposed authentication schemes based on the applied techniques for authentication and illustrates each scheme in detail. Furthermore, it highlights the advantages and limitations of the authentication schemes and presents a comprehensive comparison of their capabilities and features. Finally, the paper concludes with open issues and future research directions. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS
wireless body area networks; authentication; security; biometric; IEEE 802.15.6

***Correspondence**
Mohammad Masdari, Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran.
E-mail: M.Masdari@Iaurmia.ac.ir

1. INTRODUCTION

Advances in wireless communication technologies, such as wearable and implantable biosensors, along with recent developments in the embedded computing area enable the design and development of wireless body area networks (WBANs). Generally, a WBAN consists of sensors or devices used for monitoring and transmitting physiological signals to specialized medical servers [1,2].

In WBANs, various sensors are attached on clothing, on the body, or even may be implanted under the patient's skin [3]. These medical sensors are aimed to collect, process, and transmit physiological signals such as body temperature, blood glucose, blood pressure, or other human activity signals and information around the human body to the local base station outside the body [4]. Finally, this information, in the E-Healthcare systems [5], is provided for physicians, emergency centers, and medical information database to be further processed. Figure 1 indicates the architecture of the e-healthcare system and WBAN. Generally, WBANs have numerous medical and non-medical applications, which, in medical applications, need to collect vital information of a patient continuously and forward it to a remote monitoring station for further analysis [1].

Because, WBANs deal with life critical data, reliable, trustworthy, and authenticated data gathered of patient's health information is very important [6]. For this purpose, in November 2007 IEEE 802 established a task group who presented the IEEE 802.15.6 standard [7,8]. This task group considered three security levels and the WBANs communications can be conducted in unsecure authenticated and encrypted manner. However, recently in [9] Toorani analyzed the security of four key agreement protocols of IEEE 802.15.6 and indicated that all of them have a security vulnerability.

To solve these problems and provide strong and efficient authentication services in WBANs and in E-Health systems, many schemes have been developed and proposed in the literature, which provide various authentication methods in WBANs communications [10]. These schemes provide various authentication services such as one-way authentication, mutual authentication, anonymous authentication etc. They often apply cryptographic-based techniques for authentication, and some of them utilize biometric features for creating the required cryptographic keys. Moreover, channel-based authentication schemes are presented, which utilize received signal strength (RSS) for the authentication or creation of the cryptographic authentication keys.

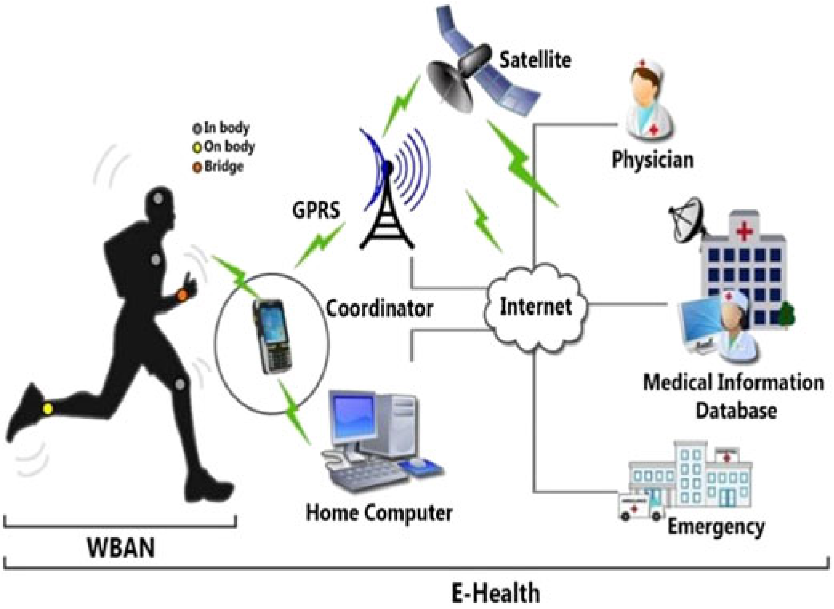


Figure 1. The WBAN and E-Health System.

Recently, the research of authentication in WBAN's security field is a hotspot. In this article, we present a comprehensive survey and analysis of the existing state of the art authentication approaches proposed in the literature for improving the WBANs security. Furthermore, this paper classifies the authentication schemes based on the methods which have been utilized in these schemes. Besides, it completely describes the authentication process applied in each authentication scheme and analyzes their properties, capabilities, and objectives. Also, the advantages and limitations of the authentication schemes are compared in detail. To the best of our knowledge, no previously proposed paper has fully analyzed the authentication methods in the WBANs, and our paper is the first one which provides a complete investigation of the proposed authentication solutions. Conducting this research is very important for highlighting the current authentication techniques and designing the future authentication scheme for WBANs.

The remaining structure of this paper is as follows: Section 2 discusses the security problems of the WBANs. Section 3 provides an overview of the IEEE 802.15.6 standards and focuses on their security capabilities. Section 4 classifies and illustrates the proposed authentication schemes for WBANs. Finally, Section 5 presents the concluding remarks and future research directions.

2. SECURITY IN WIRELESS BODY AREA NETWORK

The current medical sensors can be wirelessly accessed and even upgraded or controlled by external devices which make them vulnerable to the security attacks and threats of the lives of people. Security in WBAN is a critical issue [11] and various security services such as data authenticity, confidentiality, and integrity should be provided for transferring the health-related information in WBANs [3]. Some of the common security attacks conducted in WBANs can be listed as follows [12]:

- **Eavesdropping** [28–30].
- **Jamming Attack**: The adversary tries to prevent the reception of signals at the sensor nodes in the network [13].
- **Tampering Attack**: Sensors are physically tampered which may damage a sensor, replace the entire sensor, or a part of its hardware to acquire patient's information or shared cryptographic keys [14].
- **Unfairness Attack**: Attackers intercept the medium access control (MAC) precedence.
- **Exhaustion Attack**: When a self-sacrificing node always keeps the channel busy, an exhaustion of battery resources may happen [15].
- **Collision Attack** [16].
- **Selective Forwarding**: The attackers may decline to forward some messages [17,18].
- **Spoofing Attack**: The attacker aims the routing information and changes it to interrupt the network [19].
- **Blackhole/Sinkhole Attack**: A malicious node attracts all the traffic in the WBANs [20,21].
- **Replay Attacks**: The attackers may store the previous messages and then resend those messages [22].
- **Sybil Attack**: A node creates illegitimate multiple identity with constructing or stealing the identities of illegal nodes on the network [21,23].
- **Wormhole Attack**: Attacker receives packets at one point in the network, tunnels them to another point

DOI: 10.1002/sec

in the network, and then replays them into the network from that point [15–17].

- **Flooding Attack**: It is conducted to exhaust the WBANs resources by sending a large number of packets [14,24].
- **Denial of Service** (**DoS**) **Attack**: Attacker denies the services to the WBAN users [15,25,26].
- **Data Modification**: Information is partly or fully modified and sent back to the original receiver [27].
- **De-synchronization Attack**
- **Impersonation Attack** [27,28].

These threats and the vital role of the WBAN sensors and security vulnerabilities undermine and argue the need for reliable authentication schemes.

3. IEEE 802.15.6

The IEEE 802.15.6 standard is the first special purpose of WBAN standard, which supports medical sensors communications in the proximity or inside human body [7,29]. Figure 2 indicates the layers defined by this standard. IEEE 802.15.6 standard defines three physical layers, which are Narrowband, Ultra wideband, and Human Body Communication layers [30–32]. The general MAC includes MAC header, MAC frame body, and frame check sequence (FCS) [33].

The MAC header consists of a 32-bit frame control and an 8-bit frame control for each recipient identity (ID), sender ID, and WBAN ID. The MAC frame body includes 0–255 octets (the maximum length is 255 octets) and frame check sequence consists of 18-bit, as shown in Figure 3. The frame control contains information about the type of frame. In recipient’s ID, the information of the recipient data frame address is contained. Also, the sender’s address information is contained in sender ID. WBAN ID includes information about active transmission. The MAC frame body includes frame payload and a 32-bit message integrity code (MIC), in which frame payload carries data frames and message integrity code carries data about the integrity and authenticity of the frame [7,34].

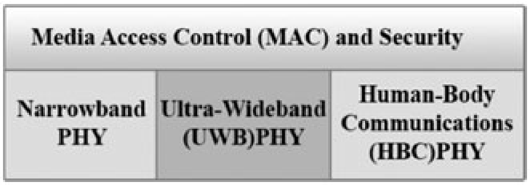

Media Access Control (MAC) and Security
Narrowband PHY
Ultra-Wideband (UWB)PHY
Human-Body Communications (HBC)PHY

Figure 2. The Media Access Control (MAC) layers in IEEE 802.15.6.

3.1. Security support in IEEE 802.15.6 standard

In IEEE 802.15.6 standard, the transmitted messages can be in one of the following three security levels:

- Unsecured Communication Level
- Authentication Level: Provides a medium level of security, where data are transmitted in the secured authentication manner without any encryption and privacy.
- Authentication and Encryption: Message is transmitted in both authenticated and encrypted form in this level. Therefore, it is the highest level of security [7,35].

All medical sensors choose one of these security levels. If nodes do not require any security services, they apply the unsecured communication level or the first security level, that all frames containing beacons will be received without validating the security information. The Level 1 provides measures for authenticity, integrity validation, and replay attack defense. But it provides no privacy protection or confidentiality [36,37]. When the level 1 or the authentication level of security is used, the control frame authentication field is set to one. Because the control frames sent from or to this sender do not need to be authenticated or encrypted, otherwise it is required to have security level 1 or 2 [38].

The hierarchy of the security in the IEEE 802.15.6 standard is described in Figure 4. In the IEEE 802.15.6,

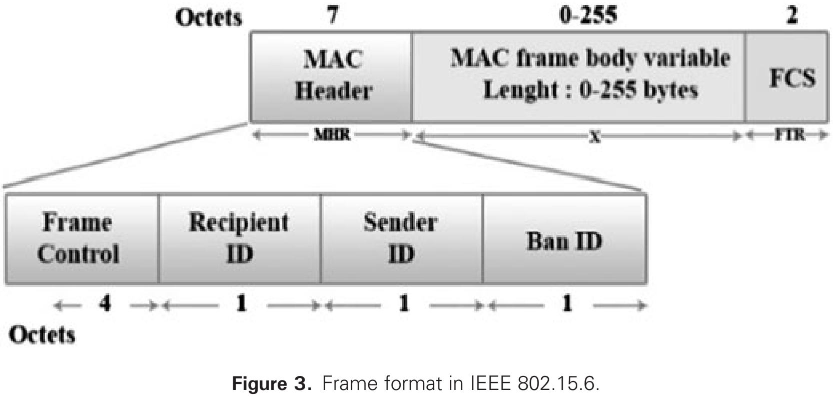


Figure 3. Frame format in IEEE 802.15.6.

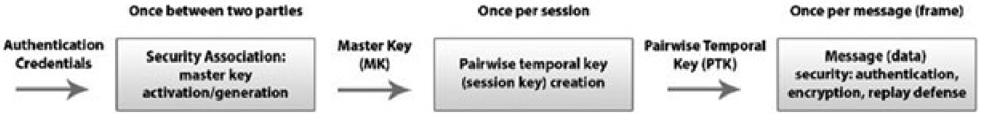

Once between two parties
Once per session
Once per message (frame)
Authentication Credentials
Security Association: master key activation/generation
Master Key (MK)
Pairwise temporal key (session key) creation
Pairwise Temporal Key (PTK)
Message (data) security: authentication, encryption, replay defense

Figure 4. The hierarchy of the security in IEEE 802.15.6 Standard.

the security association is based on four key agreement protocols. Nodes are resource-constrained in WBAN, thus in the IEEE 802.15.6 standard, public keys are self-generated by the involved parties, and the public keys are not accompanied by digital certificates.

In [9] Toorani analyzed the security of the IEEE 802.15.6 standard and its four key agreement protocols to establish a master key in the security community process. He indicates that these key agreement protocols have security problems, and are vulnerable to the key-compromise impersonation (KCI) attack. All key agreement protocols do not have the forward secrecy. Moreover, the first, third, and fourth key agreement protocols are vulnerable to the impersonation attack. Also, the third protocol is resilient to dictionary attacks. Further attacks will be feasible if public keys are not validated. This shows that the confidentiality and authentication are not fully achieved by the current security mechanisms applied in the IEEE 802.15.6. As a result, security schemes are proposed in the literature to solve this problem.

4. CLASSIFICATION OF THE AUTHENTICATION SCHEMES

Authentication is the process also the act of confirming the truth of a property of a person or identity of a sensor and software program [39,40]. Authentication is the first step towards security which prevents the network access to imposters and unwanted users [39]. Entity authentication is defined as the process whereby one party is assured of the identity of a second party involved in a protocol. Absence of authentication may lead to the situations where an illegitimate entity masquerade as a legitimate one reports false data in the E-Health system or gives wrong instructions to the other sensors of WBAN, causing considerable harm to the host [41].

As WBANs are resource-constrained, security solutions proposed for other conventional networks may not be applicable to them. As a result, special purpose authentication schemes are provided for WBANs which consider the special situations of these networks and also benefit from the biomedical data extracted from the patient's body [9].

These schemes support various authentication methods, such as one-way authentication, mutual authentication, anonymous authentication etc. Some of these schemes also support mutual authentication methods that both participating parties in the authentication process authenticate each other. Properties of an ideal authentication scheme for WBAN can be listed as follows:

(1) Low false rejection rate (FRR): FRR is the percentage of the authorized individuals rejected by the system
(2) Low false acceptance rate (FAR): FAR is the percentage of the unauthorized persons that are accepted by the system
(3) Low energy consumption
(4) Plug and play
(5) High security
(6) Low processing overhead
(7) Less needs for other security components such as key distribution center (KDC) and certificate authority (CA)
(8) Anonymity
(9) Ability to integrate with the security infrastructure provided for the E-Health systems
(10) Supporting communication conducted with the E-Health system's components
(11) Providing support for disabled people
(12) Low delay: In the case of medical emergency, any delay proves fatal to the patient
(13) Modularity: For components upgrade
(14) Flexibility: To adapt to the emerging WBAN security technologies
(15) Low overhead
(16) Efficiency

Figure 5 indicates the classification of the existing authentication schemes based on the authentication techniques applied to them. The rest of this section discusses the classified state of the art authentication schemes, presented in the literature for the WBANs and illustrates how these schemes are used to authenticate various elements of WBANs. Table I indicates the acronyms and abbreviations applied in the rest of this paper.

4.1. Cryptography-based authentication

Cryptographic techniques are the main authentication mechanisms which can be arranged into symmetric cryptography (also called secret key cryptography), asymmetric cryptography (also known as public key cryptography [PKC]) [42] and hash functions (also called one-way encryption or message digests) [14,43,44]. Cryptography and authentication methods are used to provide the secure communication between the sensor nodes in WBAN [45]. To decrypt or encrypt the symmetric key cryptography (SKC), for both the sender and receiver, shares the same key. But public key cryptography uses two keys and hash function uses no key or mathematical transformation. Selecting an appropriate cryptographic method is crucial

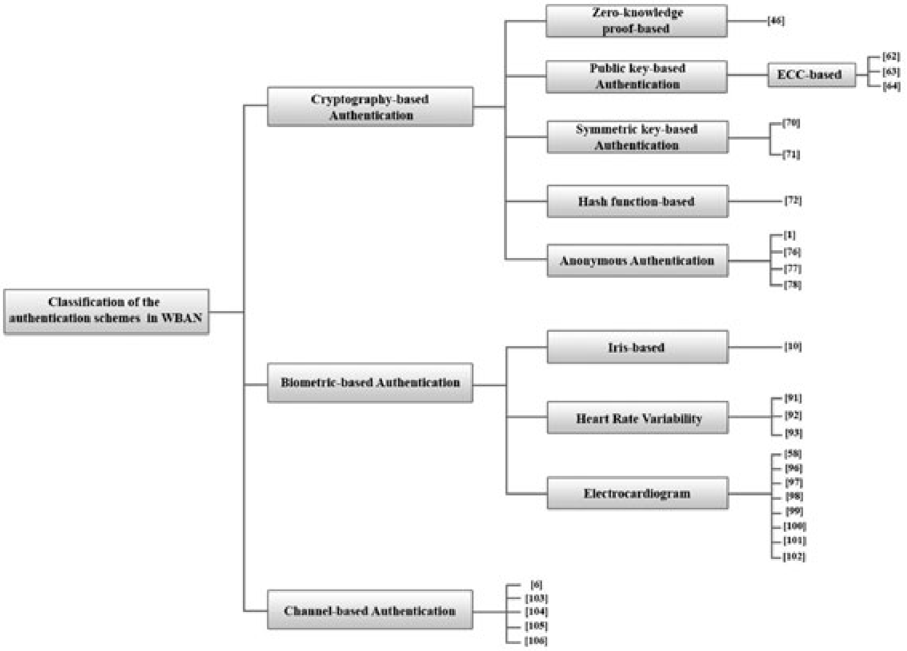

Classification of the authentication schemes in WBAN
Cryptography-based Authentication
Zero-knowledge proof-based
[46]
Public key-based Authentication
ECC-based
[62]
[63]
[64]
Symmetric key-based Authentication
[70]
[71]
Hash function-based
[72]
Anonymous Authentication
[1]
[76]
[77]
[78]
Biometric-based Authentication
Iris-based
[10]
Heart Rate Variability
[91]
[92]
[93]
Electrocardiogram
[58]
[96]
[97]
[98]
[99]
[100]
[101]
[102]
Channel-based Authentication
[6]
[103]
[104]
[105]
[106]

Figure 5. Classification of the authentication schemes presented for WBANs.

Table I. Acronyms and abbreviations.

Abbreviation	Description
WBAN	Wireless Body Area network
MAC	Message Authentication Code
CDHP	Computational Diffie–Hellman Problem
CLS	Certificateless Signature
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECG	Electrocardiogram
EKG	Electrocardiogram
H2H	Heart-to-Heart
HRV	Heart Rate Variability
IMDs	Implantable Medical Devices
IPI	Inter-Pulse-Interval
KDC	Key Distribution center
MAC	Message Authentication Code
RFID	Radio-Frequency Identification
RSSI	Received Signal Strength Indicator

to the security, scalability, and efficiency of the authentication scheme in WBANs. Both symmetric and asymmetric cryptographic methods have been proposed for authentication in WBAN and in the rest of this section, we analyze this scheme in detail.

4.1.1. Zero-knowledge proof-based authentication.

Zero-knowledge proof (ZKP) is an interactive proof protocol, which consists of the prover and verifier. The prover knows some knowledge without conveying the verifier any information or anything else, also ZKP permits the prover to ensure the verifier.

In Ma *et al*. [46] propose a ZKP-based protocol for verifying the identity of sensor nodes, named TinyZKP. The TinyZKP is a lightweight authentication scheme, which tries to resist, a variety of attacks in the WBAN such as guessing attack and replay attack, without leaking any information regarding the secret keys to the adversary. In the TinyZKP scheme, no information about secret key is revealed during the authentication process. The sink, in the TinyZKP, acts as an authentication center and the sensor proves its identity to the sink by proposing ZKP algorithm in the authentication phase. The TinyZKP uses Secure Hash Algorithms (SHA), SHA-1 a 160-bit function, to encrypt the password of the data information. Also, the proposed scheme uses the elliptic curve digital signature algorithm (ECDSA) to create a digital signature based on the elliptic curve cryptography (ECC). In the authentication phase, first, the sensor node ascertains its identity to the base station (sink) based on ZKP algorithm, for this purpose in step 1, in the sink (the base station) a random challenge vector is generated, and a signature is created by using the ECDSA. *Message 1*, which contains identifying the sink, Timestamp 1, accidental challenge vector, and the signature is formed. Then, by using the session key, the *message 1* is encrypted, and then the sink sends the *message 1* to the sensor node. In step 2, on receiving the *message 1* from the sink, the sensor node decrypts it and verifies the signature. If the signature is valid, then in the sensor node, an integer number is selected randomly. The sensor node uses a member of the SHA, 'SHA-1' for encrypting the *message 2*, then *message 2*, which includes of the sensor identifying and cryptographic hash function and Timestamp 2 is formed, encrypted, and sent to the sink. In step 3, the sink decrypts the *message 2* from the sensor and calculates the hash value, and sends the *message 3* including new session key and identifying the sink is encrypted and sent to the sensor node. Otherwise, the base station denies the sensor node. After the sensor node is authenticated successfully by the sink, its MAC address and node identity are recorded in the sink to form an access control list (ACL). On receiving the packets from sensor nodes, first the sink checks its access control list. Finally, in step 4, on receiving the *message 3* from the sink, the sensor node decrypts it and gets the new session key. *Message 4* contains the corresponding person's data. By using the session key, it is encrypted, then the data is sent to the sink. All authentication steps are shown in Figure 6.

4.1.2. Public key-based authentication.

Public Key-based cryptography concept is using a private and a public key [47]. There are many public key cryptography algorithms such as Rivest Shamir Adleman (RSA) [48,49], Diffie–Hellman (DH), digital signature algorithm (DSA), ELGamal [50,51], and ECC [52]. In the public key cryptography, a public key is made freely available to anyone who might want to send a message and a private key is kept secret. Therefore, the need for complicated protocols would be eliminated by using a public key cryptography [53]. A DSA is a public key cryptography method that is based on public key cryptography and hash function and uses digital signature standard (DSS) [54].

4.1.2.1. Elliptic curve cryptography. Elliptical curve cryptography [55] is an asymmetric key encryption method [56] that signing and verification or decryption and encryption are complicated, unlike other public key encryption methods like RSA [57]. The main benefit of the ECC is that the similar level of security can be provided with keys of smaller size, which uses computing less, more than public key cryptosystems [58–60]. As a result, the ECC is a useful method for small devices with limited memory like a personal digital assistant (PDA). The ECDSA is a type of DSA based on the ECC analogue [60,61].

Sangari *et al.* [62] in present an ECC based scheme for authentication in WBAN. The scheme uses message authentication codes (MACs), which is a cryptographic hash function. In the proposed architecture, the master key is generated by using the electrocardiogram (ECG) signals. The ECDSA is applied to generation signature. The sensor nodes and the data aggregation node (AGN) are deployed on the human subject, while the base station is located away from the subject. As shown in Figure 7, mutual authentication is provided by the proposed scheme between the sensor node and base station. This ECC-based security scheme collects ECG value from the patient's body and generates the master key and nonce values. Then, sensor node sends a message to the sink consisting of the information such as node identity, nonce value, message, and key value. A message authentication code value is calculated for the whole message and encrypted by the base station public key. The sensor node sends the encrypted information and the signature value of the message to the sink. Then, sink verifies the signature and if it is verified successfully, it sends a certification to the sensor node, informing that the signature is verified and the message is received and generates the nonce value '*x*2'. If the signature verification fails, the head node sends a request to the sensor node for another message and its signature. After the signature verification, the sink decrypts the data using its private key and recalculates the message authentication code (MAC) value. Then, sensor sends reply to the sink containing *x1* and *x2*. Then, the key value k is combined with *x1* and *x2* to generate the shared secret key which is used for encryption and decryption processes. Man-in-the-middle is an attack, which intercepts keys and creates a spoof identity, then changes the communication

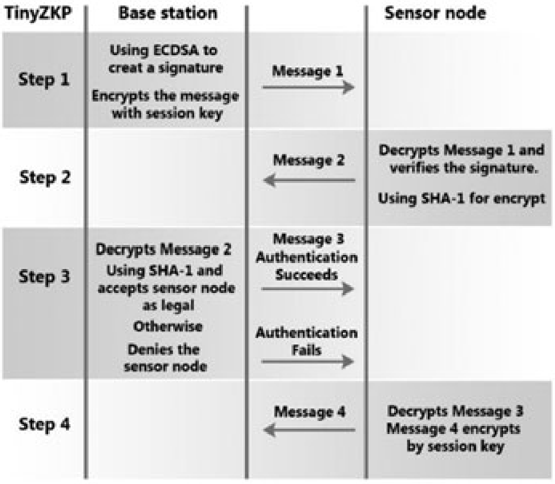

TinyZKP
Base station
Sensor node
Step 1
Using ECDSA to creat a signature
Encrypts the message with session key
Message 1
Step 2
Message 2
Decrypts Message 1 and verifies the signature.
Using SHA-1 for encrypt
Step 3
Decrypts Message 2 Using SHA-1 and accepts sensor node as legal
Otherwise
Denies the sensor node
Message 3 Authentication Succeeds
Authentication Fails
Step 4
Message 4
Decrypts Message 3 Message 4 encrypts by session key

Figure 6. TinyZKP authentication scheme proposed in [46].

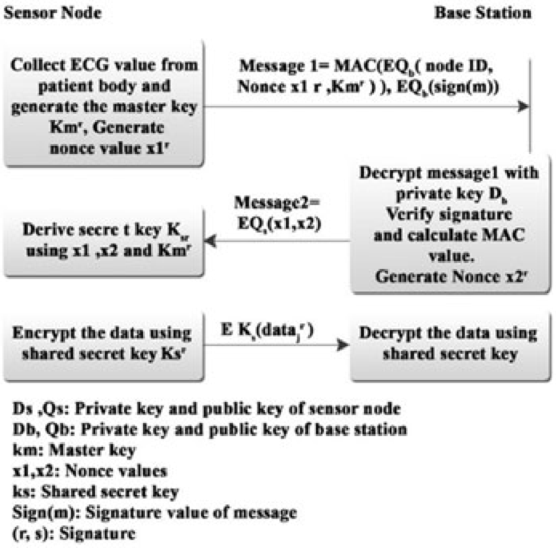

Sensor Node
Base Station
Collect ECG value from patient body and generate the master key Km', Generate nonce value x1'
Message 1= MAC(EQb(node ID, Nonce x1 r ,Km')), EQb(sign(m))
Decrypt message1 with private key Db Verify signature and calculate MAC value. Generate Nonce x2'
Message2= EQs(x1,x2)
Derive secre t key Ksr using x1 ,x2 and Km'
Encrypt the data using shared secret key Ks'
E Ks(dataj')
Decrypt the data using shared secret key
Ds ,Qs: Private key and public key of sensor node
Db, Qb: Private key and public key of base station
km: Master key
x1,x2: Nonce values
ks: Shared secret key
Sign(m): Signature value of message
(r, s): Signature

Figure 7. Mutual authentication method in scheme [62].

between two parties, who have directly communicated with each other.

Chatterjee *et al.* [63] in present a scheme based on ECC, which provides security against man-in-the-middle attack and uses asymmetric key cryptosystem. For authentication, in step 1, the user sends the request message for authentication that includes symmetric encryption, using the key *K*, random number of user, and bootstrapping time for node to the sensor node. In step 2, after receiving the request for authentication, the sensor node computes the key, using the stored parameters and the received user identity, and decrypts the symmetric encryption to retrieve the information checks as the retrieved value of the sensor node bootstrapping time. The sensor node compares its message with the previously received value of the sensor node bootstrapping time. If they match, sensor node computes the hash value and verifies whether this value matches with the received hash value. If there is a match, sensor node proceeds to step 3, otherwise, the authentication phase instantly terminates. In step 3, the sensor node checks the signature verification, when it fails, the sensor node contains it as illegitimate user and the phase terminates immediately, otherwise, the sensor node checks the received group identity of the user with the value received from the sink during the login phase. If it is satisfied, sensor node computes a secret session key to be shared with the user and sends an acknowledgment to the user and the sink. It also responds to the query of the user, depending upon the access privilege mask of the user stored for user using the secret session key. In step 4, after receiving the acknowledgment from sensor node, user computes the same secret session key shared with the sensor node. Therefore, both user and the sensor node can securely communicate using the derived secret session key. At the end of this phase, sensor node deletes all information and messages from its memory for security reasons. User also does it the same. The proposed scheme provides security against denial-of-service (DoS) attack, stolen-verifier, masquerade, privileged insider, and replay attack.

A hybrid security protocol for WBANs is presented by Jang *et al.* [64] in, called Hybrid Security-WBAN (HS-WBAN), which applies a combination of symmetric key and public key cryptography. HS-WBAN uses symmetric key cryptography for the communication between sensors and asymmetric keys for the communication between the sensor and sink. The proposed scheme uses public key cryptography ECC. The HS-WBAN protocol is divided into two procedures, the global authentication and the local authentication, which is limited from the biosensor nodes measuring with physiological signal (BSN). The authentication between the BSN and BSH (the biosensor head to communicate between in-body and out-body) can happen without the CA. As shown in the Figure 8 in the local authentication for WBAN, the BSH produces a new session key and sends it to all BSNs. BSN decrypts the message with the secret key and generates a new session key. At last, BSN sends its reply message including new session key to the BSH.

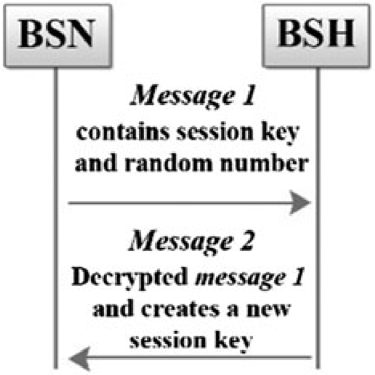


Figure 8. Local authentication in scheme [64].

4.1.2. Symmetric key-based authentication.

Public key algorithms are slower, more than symmetric key algorithms [65]. Because symmetric cryptosystem is using the same key to encrypt and decrypt messages [66,67]. Also, symmetric key cryptography algorithms consume much less computational energy than public key algorithms [20]. For WBAN security, symmetric key cryptography needs less resources like memory capacities and operations or computational as compared with public key cryptography (Asymmetric key cryptography), therefore symmetric key cryptography is preferred for the WBAN [68,69].

An authenticated key exchange scheme for WBAN is proposed in [72] by Yan *et al.* This protocol supports the selective authentication between sensor nodes. Figure 9 indicates the flowchart of the certification process in the proposed protocol.

S is a control sensor node and *B*, *C*, and *D* are the primary nodes; *A* is secondary node; and *k* is key. For authentication, the control node *S* keeps the pre-shared key K_{bs} with primary node *B*, and K_{cs} for *C*, also K_{ds} with *D*, and finally *S* shares the pre-shared key K_{as} with secondary nodes *A* identically. The protocol, first a message broadcasted by secondary node *A*. After receiving the message from *A*, the adjacent nodes *B*, *C*, *D* generate encrypted messages, afterwards they send them to the control node *S*, which determines the most proper primary node to be

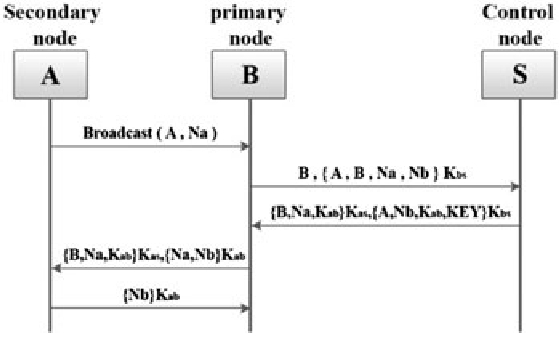

Secondary node
A
primary node
B
Control node
S
Broadcast (A , Na)
B , { A , B , Na , Nb } K_{bs}
{B,Na,K_{ab}}K_{as},{A,Nb,K_{ab},KEY}K_{bs}
{B,Na,K_{ab}}K_{as},{Na,Nb}K_{ab}
{Nb}K_{ab}

Figure 9. Certification process in scheme [70].

conjunct with node A. The protocol assumes that the primary node B is the most applicable one, then accomplishes the authentication between the control node S and the primary node A, also S and B, and the secondary node A and the primary node B. The proposed scheme generates a session key named '*KEY* 'between the control node S and the primary node B, session key K_{ab} between A and B. At the same time, the control node S replies to the primary nodes C and D to apprise the connection is failing. This scheme is resilient against WBAN attacks such as replay attack.

Dirar *et al.* [71] in have proposed a hybrid authentication scheme, which uses elliptic curve Diffie–Hellman (ECDH) algorithm and is based on symmetric key cryptography. The proposed scheme contains two protocols which are resilient against known attacks, and reduces calculation load on sensor nodes, due to mobile node authentication performed by storage site. Mobile node acts as a sink for the data of sensor node and forwards the data to a storage site where they are stored and analyzed. The first protocol describes authentication steps between smartphone and the storage site and key establishment scheme, and the second protocol is between sensor nodes and the smartphone and the storage site, also key establishment scheme. The protocol between the smartphone and the storage site is described in the following steps: in step 1, the smartphone processes by sending a start authentication *message 1*, containing a nonce value n_0, its identity, its user identity, and a timestamp t_0. All those values are hashed, and the result is added to the *message 1* footer. Then, the *message 1* is sent. A nonce value n_0 and a time stamp are present in the *message 1* to enforce its resiliency against replay attacks. In step 2, on receiving the *message 1* checks the smartphone and the user identity, the storage site checks identities to ensure that smartphone is allowed to integrate the network. Then, it checks that the difference between the actual time and t_0 also checks verifying the result of the hash function. If the validation succeeds, the storage site generates its session key of the Diffie–Hellman key. Next, it generates a *message 2*, containing the received nonce value, a new nonce n_1, and a time stamp t_1 and sends the *message 2* to the storage site. In step 3, the smartphone should check the freshness of the message, the authenticity of the received nonce value n_0, a new nonce n_1. Therefore, it checks the difference between the actual time and t_1. Second, it checks the storage site authenticity and knowledge by the verification of the signature using this latter public key. The verifications success means that the message is a fresh response from the storage site. In that case, smartphone generates its session key of the Diffie–Hellman key. Finally, it generates a *message 3* containing a time stamp t_2, then the *message 3* is sent to the received nonce value, a new nonce. In the step 4, after receiving the message 3 from the smartphone, the received nonce value n_1 verifies the hash result, the time stamp t_2. Then, it calculates the Diffie–Hellman key, after that it generates the private key of the smartphone. Finally, it creates a *message 4* containing the received nonce n_2, a new nonce n_3, a time stamp $t_{3,}$ and the validity time, and private key. It encrypts all the fields using the Diffie–Hellman key and sends the message to the smartphone. In step 5, the smartphone decrypts the *message 4*, checks t_3, and generates a *message 5*, signs it using its private key and sends it to the storage site. In step 6, the storage site checks the message fields and the signature to make sure that the smartphone has received its private key successfully. If the confirmation succeeds, then the storage site sends an 'authentication success' message for the smartphone to end the authentication and key establishment protocol, otherwise the message is ignored.

In the second proposed protocol, authentication is between the sensor nodes, the smartphone, and the storage site. At step 1, the sensor nodes start the protocol by sending a *message 1* to the smartphone, including a nonce value n_0, its identity, its user, and a time stamp t_0, it hashes all the fields and its sensor node password shared with the storage site, then it includes the resulted hash to the *message 1* and then sends *message 1* to the smartphone. The smartphone checks time stamp t_0, if it is fresh, the smartphone stores the three first fields and generates its part key of the Diffie–Hellman key, which wants to share with the sensor nodes. Then, it adds its identity, its user identity, and session key, receives a *message 1* from the sensor nodes and hashes all the fields and signs the hash using its private key. Finally, it adds the signature to the *message 1* footer and sends it to the storage site. In step 2, on receiving the *message 1* from the smartphone, the storage site checks all the identities in the *message 1* and the timestamp, it checks the signature of the smartphone using the hash included in the *message 1* to verify that the sensor node has the correct password and the message is not modified on the route. In step 3, first the sensor nodes check the presence of n_0, the validity of t_1, and the signature. If this verification succeeds, the sensor nodes generate its part key of the two the Diffie–Hellman keys and the three parties key and calculate them. After the smartphone has picked a nonce value n_2, it encrypts n_1 and n_2. Then, it builds a *message 2* using its part of the Diffie–Hellman keys. It adds the result of hashing all the fields to the *message 2* and sends it to the smartphone. The smartphone gets the part of the sensor node in the Diffie–Hellman pairwise key and the common key between the three sides and generates them. Then, it decrypts the encrypted field with this latter key and checks that n_1 is present. It gets n_2, picks a new nonce $n_{3,}$ and encrypts them with the key. It adds the result and signs the received *message 2* and the new fields using its private key. Finally, it sends the resulted *message 3* to the storage site. In step 4, the storage site checks both the signature of the smartphone, using the latter public key in the *message 3*. If the authentication succeeds, it gets the part of the sensor node. It decrypts the encrypted field in the *message 3* and verifies the existence of n_1. Then, it gets n_2, if the verification succeeds, and sends a *message 4* to the sensor node, the encrypted values sent from the smartphone and signs the hash of all the fields and n_2. The smartphone just checks that the storage site sends the encrypted fields, and the storage site signature and forwards the *message 4* to the sensor nodes. On receiving the *message 4*, the sensor nodes, check the signature of the *message 4*, that both the storage site and the smartphone have been sending an OK value. Finally, it checks the encrypted values of n_2 and n_3. If verifications succeed, the authentication and key establishment are validated.

4.1.3. Hash-based authentication.

The hash function is a method of the cryptography-based authentication which does not use any key to encrypt and decrypt. Hash function includes message authentication code (MAC), hash-based message authentication code (HMAC), SHA family, and message-digest algorithm (MD) family. MD5 and SHA1 are the most used algorithms in the hash-based authentication.

In Kumbhare *et al.* [72] propose a hash-based authentication scheme using an HMAC function to provide the security in the WBAN. The scheme uses symmetric key cryptographic and by using the MD5 and SHA1 algorithms makes the encryption simple and fast, where MD5 and SHA-1 are used in the calculation of the proposed HMAC-based protocol. Each in-body node does not communicate with base station in this architecture, and the scheme provides security against the man-in-the-middle attack. For authentication in the proposed protocol, as shown in Figure 10, in step 1, a message from the sender is broken into blocks of a fixed size and iterates over them with a compression function. The size of the output of HMAC is the same as that of the underlying hash function. The HMAC algorithm combines a key with a hash function and creates a new *HMAC 1*. Then, a message with *HMAC 1* tag is sent to the receiver. In step 2, the receiver uses the same HMAC algorithm and the same key to create a new *HMAC 2* tag. The receiver checks the *HMAC 1* and *HMAC 2*. If *HMAC 1 = HMAC 2*, the authentication is a success, otherwise there is something wrong. By using this scheme safe, the data of the person is sent to the doctor. The doctor can receive and use the data without any physical communication with the patient.

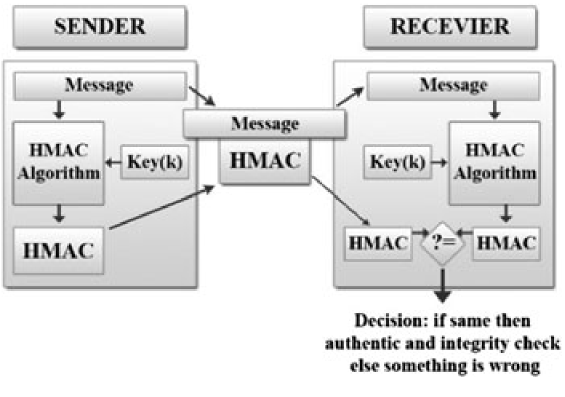


Figure 10. Authentication scheme in [72].

4.1.4. Anonymous authentication.

Anonymous authentication permits a user to access the information without revealing his/her identity. Anonymous authentication is a type of 'group signature' scheme [73], therefore we have classified it as cryptography-based authentication. Anonymous authentication is also known as 'Blind signature', because the content of the message is hidden or blinded before it is signed [74,75]. In some cases, in the WBAN's medical applications, the authorized patients may need medical services anonymously. This means that doctors should know the patients' health-related data, but they should not have any access to the patient's private information such as name and identity number [76].

In Liu *et al.* [1] propose two authentication protocols for WBANs which are named as the preliminary and security enhanced authentication protocols. Also, they propose a new certificateless signature (CLS) scheme, which sets a network manager creating an account index for a client request in the WBANs. The proposed anonymous certificateless preliminary version authentication protocol operates in the following three phases: initialization, registration, and authentication phases. In the initialization, the network manager generates keys and establishes an enrollment system. In the registration, the client must perform some operation with the network manager in order to access the application provider of interest. In the step, a legal client chooses a private key, which obtains another partial private key. The network manager creates an account for the client. Two secure hash functions and MAC are loaded together for access between the application provider and the client. For authentication step, the client creates a random number and *timestamp A*, also computes a session key and sends *message A*, including the random number, *timestamp A*, and session key, to the application provider. The application provider, first, checks the validity of *message A*, digital signature and *timestamp A*, and then rejects the request if *message A*, digital signature, and *timestamp A* are not valid. The application provider, after checking the validation, computes a new *message B*, including *timestamp B*, random number, and new session key. The application provider by using a hash secure function, checks the verification of the *message B*, and computes MAC as a reply. Then, the provider sends a request to the client. The reply from the application provider is received by the client, and then the client checks the validity of MAC. The client authenticates the application provider and uses the session key with the application provider in future communications. In the proposed anonymous certificateless preliminary authentication protocol, authentication request information is carried in the *message*, which can allow an attacker chase the client identity from the information about session key. To remedy vulnerability, they propose an anonymous security enhanced authentication protocol, in which initialization phase is the same as the anonymous certificateless preliminary authentication scheme, and in the registration phase it is the same, but the network manager sends an issue including identity and the verifying index for both the client and application provider. The authentication phase in the proposed anonymous security enhanced authentication protocol is nearly the same as the proposed anonymous certificateless preliminary authentication scheme. The proposed protocols use mutual authentication.

An identity-based, anonymous, and mutual authentication scheme is proposed in [76] by Zhao, which uses elliptic-curve cryptosystem. No certificate is applied in this protocol and it provides resistance against known-key security, unknown key-share resilience, perfect forward secrecy, and mutual authentication. Moreover, it could withstand impersonation attack, replay attack, man-in-the-middle attack, modification attack, and stolen verifier attack. In the authentication phase, when a client wants to get medical services from an application provider, the following steps are performed. In step 1, the client creates *message A*, which includes a random number and current timestamp. Then, it sends the *Message A* to the application provider. Upon receiving the *message A*, in step 2, the application provider checks the freshness of the current timestamp of the *message A*. If it is not fresh, the application provider rejects the request. Otherwise, the application provider produces a random number and computes, the *message B*, including random number and session key, and sends the *message B* to the client. In step 3, the client checks the secure hash function and computes the session key.

In Liu *et al.* [77] present a certificateless anonymous authentication scheme. Figure 11 illustrates the proposed protocol structure, the communication between the network manager, application provider, and the client. The proposed scheme applies an off-line network manager that manages the whole network containing the three phases which are: the initialization, the registration, and remote anonymous authentication phase, as shown in Figure 12. In the remote anonymous authentication phase, in step 1, the client selects a random number and creates a *message 1* including current time, session key, and random number. The client sends the *message 1* to the application provider. When the application provider receives the *message 1*, it checks the validity of current time. The application provider rejects the request if current time is not valid. Otherwise, the application provider after the decryption of the *message 1*, creates the *message 2* including a new session key and computes the MAC as the reply, then gives reply to the client's service request by sending back MAC. The protocol makes the network manager more applicable in real WBAN network application scenarios.

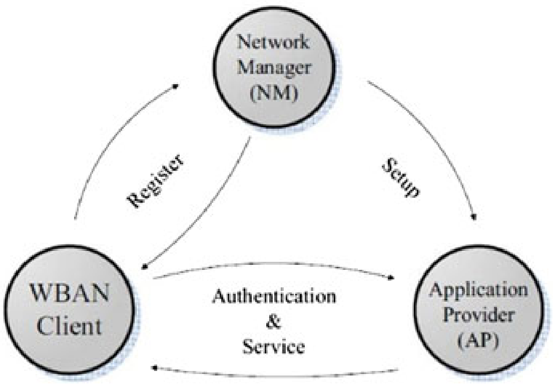


Figure 11. Certificateless anonymous authentication protocols in scheme [77].

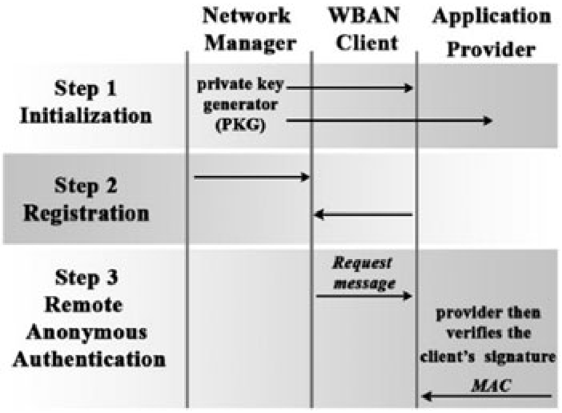

Network Manager
WBAN Client
Application Provider
Step 1 Initialization
private key generator (PKG)
Step 2 Registration
Step 3 Remote Anonymous Authentication
Request message
provider then verifies the client's signature
MAC

Figure 12. Certificateless remote anonymous authentication for WBAN in scheme [77].

An anonymous authentication scheme is proposed in [78] by Wang and Jang, which applies three participants in the authentication process that are client, network manager, and application provider. The network manager is a trusted third party, and the manager is responsible for producing private keys for the clients and the application provider. The application provider is a physician, which is responsible for providing medical services in the WBANs. The client is a patient, who uses a PDA or mobile phone. The proposed authentication scheme includes three phases: the initialization, the registration, and last one, the authentication phase. In the authentication phase, as shown in Figure 13, the client and the application provider

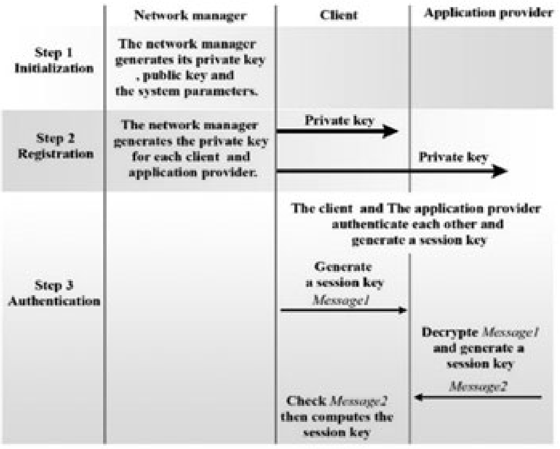

Network manager
Client
Application provider
Step 1 Initialization
The network manager generates its private key , public key and the system parameters.
Step 2 Registration
The network manager generates the private key for each client and application provider.
Private key
Private key
Step 3 Authentication
The client and The application provider authenticate each other and generate a session key
Generate a session key
Message1
Decrypte Message1 and generate a session key
Message2
Check Message2 then computes the session key

Figure 13. The anonymous authentication in scheme [78].

authenticate each other, and then they produce a session key for the encryption of the physiological values. Also, both of the application provider and the client mutually authenticate each other. For authentication, in step 1, the client generates a random number and computes the *message 1*, which includes current timestamp and random number. Then, it sends the *message 1* to the application provider. In step 2, the application provider, after receiving the *message 1*, checks the freshness of the current timestamp. If it is not fresh, the application provider rejects the request to the client. The application provider computes session key and decrypts the *message 1*. The application provider checks if current timestamp and the decrypted one are equal. If they are not equal, the application provider rejects the request. Then, the application provider generates a random number and computes the session key. The application provider sends the *message 2*, including current timestamp and random number, then it sends it to the client. In step 3 the client, upon receiving the *message* 2, checks the freshness of the application provider's current timestamp. If it is not fresh, the client rejects the request. Also, the client checks the equations between its current timestamp and random number with the application provider's current timestamp and random number. If it does not hold, the client rejects the response otherwise computes the session key. This scheme is secure against man-in-the-middle attack and relay attack.

Figure 14 shows the cryptographic algorithms, which are used in the proposed WBANs scheme. As shown in Figure 14, DH is used only for symmetric key exchange, and DH is not for authentication or digital signatures. The SHA family algorithm includes SHA-0, SHA-1, SHA-2, and SHA-3. MD algorithms are a type of hash function algorithms and classified into MD2, MD4, and MD5.

4.2. Biometric-based authentication

Biometric authentication [79] is a method to verify an identity [80], which uses human behavioral and physiological characteristics to ensure safety and security. Also, it provides higher security compared with the pure cryptosystems-based authentication schemes. The biometric authentication goal is to keep FAR (low false acceptance rate) and FRR (low false rejection rate) down [81,82]. There are several types of human characteristics like fingerprint, iris scan [83], face recognition, hand geometry, voice scan, and ECG that can be used to build secure and effective biometric authentication schemes. This is because of the biometric characteristics which are unique for each person, not lost or forgotten, and extremely difficult to copy, share, or distribute [6,84]. As shown in Figure 15, a typical biometric authentication system involves four main steps: data acquisition, feature extraction (including creation and storage of master characteristics, then comparison data), template matching, and decision making [85].

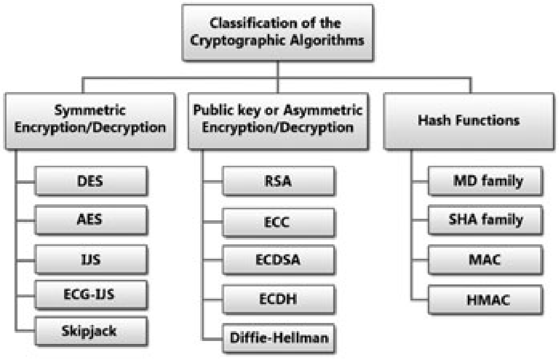

Classification of the Cryptographic Algorithms
Symmetric Encryption/Decryption
Public key or Asymmetric Encryption/Decryption
Hash Functions
DES
AES
IJS
ECG-IJS
Skipjack
RSA
ECC
ECDSA
ECDH
Diffie-Hellman
MD family
SHA family
MAC
HMAC

Figure 14. Classification of the proposed cryptography algorithms.

4.2.1. Iris scans-based authentication.

Iris-scan authentication is based on unique patterns within the ring-shaped region surrounding the pupil of the eye. Each person's iris contains a complex and random pattern that is unique to each individual. Discovered in 1935, Simon and Goldstein specified the uniqueness of the blood vessels in each person, even in the twins. The Iris recognition provides one of the most secure methods of authentication. Once the image of the iris is captured using a standard camera, the authentication process can be performed comparing the current subject's iris with the stored version, with very low false acceptance and rejection rates [86].

Voronoi diagram receives a set of points and its output is a partitioning of the plane into regions of equal nearest neighbors. Based on the Voronoi diagram, Ullah *et al.* in

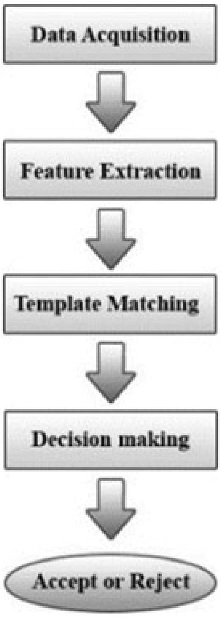


Figure 15. Biometric-Authentication system.

[10] have proposed a protocol for human authentication using iris scan in WBANs. The Voronoi diagram is partitioning a plane consisting of *P* points into sub-planes or areas having characteristics of convex polygons *C* such that every point in the polygon *Ci* is nearby the corresponding point *Pj* as measurement to other points in *P*. In the proposed algorithm, the feature points are token from the bifurcation points of the blood vessel pattern. These bifurcation points are determined using a simple 3×3 size kernel, after the thinning algorithm. Once the feature points are obtained, the Voronoi diagram is generated out of the feature points mapped. Next, the algorithm calculates the points, edges, and the internal angles of the polygons toke of the Voronoi diagram, and are reserved in the template in a sorted order along with the point considered as the closest from every point present within the region allocated to the polygon. The edges are normalized to equilibrate the scaling. The generated template can be stored as the collection of feature points. The matching process consists of three steps. Initially, the number of feature points is counted from the query retinal image. The matching retina is from the claimed identity if *V* is greater than the set threshold value. The process of identification can also be used in the content based image retrieval, where more than one identity may be required. The query template and the templates higher value than threshold match all the stored templates.

4.2.2. Heart rate variability (HRV).

Heart rate variability or Inter-pulse Interval (IPI) [87,88], is the time interval among heartbeats being an authentication method that is used in WBANs. It has chaotic and random characteristics and can be utilized to secure the communications. HRV indicates the fluctuations of heart rate around an average heart rate [89]. In HRV, the electrocardiogram (ECG, or EKG) and blood pressure are used to detect beats. Figure 16 shows the fluctuations of heart rate around an average heart rate and the variation in the time interval between heartbeats. The IPI obtained from physiological signals such as photoplethysmogram (PPG) [88,90].

An HRV-based security system called H2H is presented by Rostami *et al.* [91] in, which is based on the ECG signal and used for authentication, key generation, and key agreement. In H2H scheme, RSA is the choice of key exchange, also Advanced Encryption Standard (AES) for encryption. SHA algorithm serves as the commitment function. In H2H operation, the programmer and implantable medical devices (IMD) take individual ECG readings, α and β, respectively. If β is close to α or $\beta \approx \alpha$, the IMD grants access the programmer or the IMD accepts the programmer as valid. The scheme uses Password authenticated key-exchange (PAKE) protocol for securing against man-in-the-middle attack.

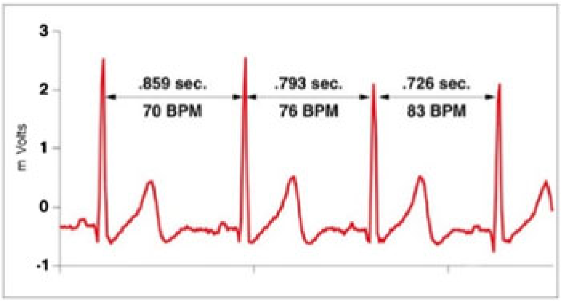


Figure 16. Heart Rate Variability or IPI Signals.

Another biometric-based security framework is proposed by Ramli *et al.* in [92]. They have proposed a scheme for data authentication within WBAN, which has low complexity and power consumption. In this scheme, the sender's ECG feature is applied as the biometric key for data authentication within WBAN. As shown in Figure 17, this scheme applies MAC, which can be generated by the input of biometric feature and hashes calculated based on the original message. Then, the message will be sent to the destination. At the destination, if the received signal matches statistically, it will be accepted and authenticated, otherwise, it will be denied and discarded. The key point of this scheme is to utilize the same biometric information at both ends without any synchronization. Figure 18 describes the steps of the proposed biometric-based security for data authentication.

An authentication signature based on IPI signals is proposed by Wang *et al.* in [93] where the IPI signal pattern at transmitter side is applied as a biometric authentication key. Also, the Gaussian Mixture Model (GMM) is applied to authentication information. The system architecture for ECG signal authentication in a body area network is shown in Figure 19.

To secure the wireless transmission among medical sensors, IPI signals from the human body at the transmitter side are scrambled with medical information data. A signature of stochastic attributes of GMM and log-likelihood function with stochastic attributes of GMM representing the biometric authentication sequence (BAS) for transmitter is created and attached to the medical information data according to the transmitter side of the BAS for transmitter. The scheme is proposed to use simple XOR hash operation of IPI and the message data unit or payload data exchanged among sensors to scramble medical information with ECG

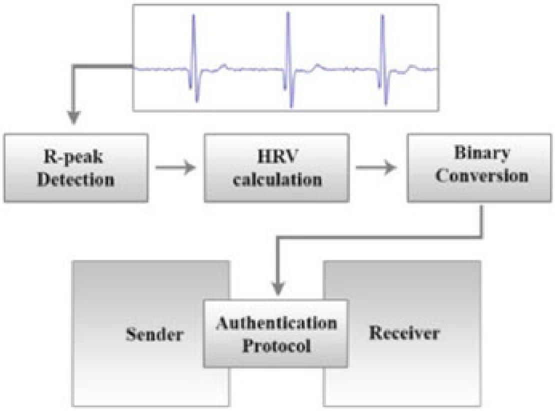


Figure 17. Authentication protocol in scheme [92].

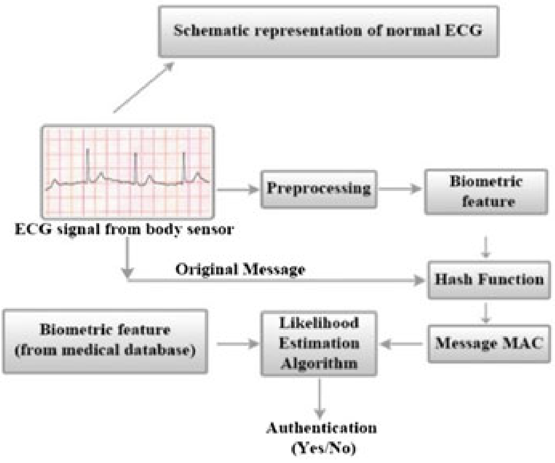

Schematic representation of normal ECG
ECG signal from body sensor
Preprocessing
Biometric feature
Original Message
Hash Function
Biometric feature (from medical database)
Likelihood Estimation Algorithm
Message MAC
Authentication (Yes/No)

Figure 18. Biometric-based authentication in scheme [92].

signal. Then, the transmitter side of the BAS for transmitter is modeled by GMM, and the stochastic characteristics and stochastic attributes of the GMM are extracted as the authentication signature. In the proposed GMM-ECG authentication scheme, a small value of the decision threshold over puny IPI dissimilarity from the same user may lead to a plethora FRR (low false rejection rate), and a large value of the decision threshold overlooking the distinct dissimilarity between different users may lead to an excessive FAR (low false acceptance rate).

4.2.3. Electrocardiogram (ECG or EKG).

The ECG is a graphic record of electric currents that are generated by the heart muscles. Also, it is an example of medical applications that can be used by WBANs [94]. HRV or heart rate variability can easily be obtained from ECG signals [87]. The properties of the ECG signal are unique and have different features from person to person. This difference makes the ECG signal desirable to differentiate between incoming data packets from sensors on the same body and the sensors on another human body. The communications between on-body sensors can be authenticated by the ECG signals attributes [93,95].

In Yao *et al.* [96] present a protocol for the authentication and key establishment in WBAN, called ECG-based Signal Key Establishment (ESKE) which applies the fuzzy commitment and ECG signals. In ESKE, when control unit authenticates, a biometric sensor sends a message which includes the real biometric data and chaff points. The similarity between a biometric sensor set of points, and the set of points from the control is important and if an enough number of points can accommodate within some threshold, the biometric sensor will be proven legal. For authenticating a multi-hop network, ESKE scheme uses two or more wireless hops to convey information from a source to a destination. The sink node, named by a control unit, collects the data from other sensors, and then sends it to the gateways or remote server. In this multi-hop tree of body area network, every biosensor must be authenticated by the control unit before transmitting some data and after successful authentication, a session key between them will be generated. In ESKE scheme, the key is a secret to the third party, and data confidentiality can be assured. Also, in this scheme, a priori distribution of keying material is not required. The ESKE is resistant against man-in-the-middle attack, on-line, and off-line guessing attacks.

In Abina *et al.* [97] have focused on the intercommunication and authentication between the sensor nodes in the WBANs. They propose an electrocardiogram-improved Jules and Sudan (ECG-IJS) key agreement protocol in a plug-and-play manner, which uses symmetric key

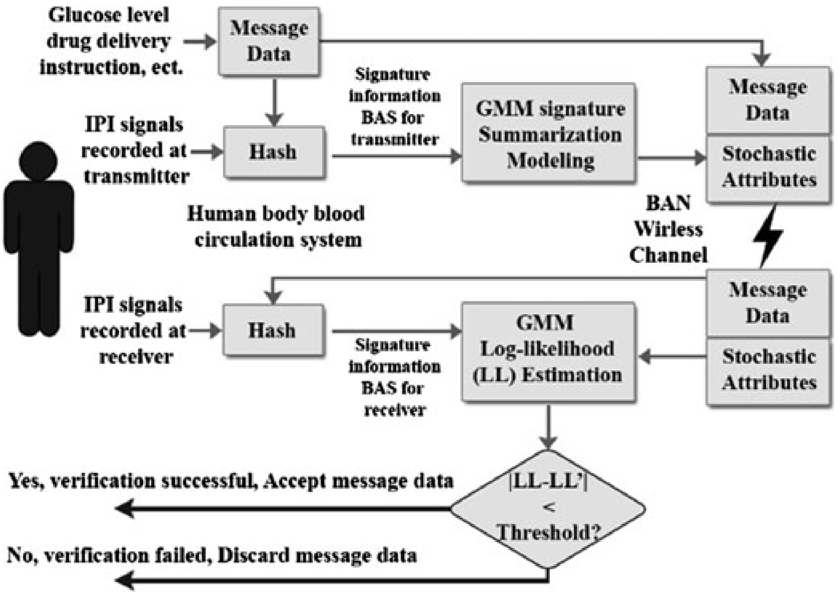

Glucose level drug delivery instruction, ect.
Message Data
Signature information BAS for transmitter
Message Data
IPI signals recorded at transmitter
Hash
GMM signature Summarization Modeling
Stochastic Attributes
Human body blood circulation system
BAN Wirless Channel
Message Data
IPI signals recorded at receiver
Hash
GMM Log-likelihood (LL) Estimation
Stochastic Attributes
Signature information BAS for receiver
Yes, verification successful, Accept message data
|LL-LL'| < Threshold?
No, verification failed, Discard message data

Figure 19. GMM-Based authentication systems in [93].

cryptography and a hash function algorithm. For data authentication in this scheme, after making a key by using the ECG signal, in step 1, the receiver, and the sender share a same key to compute a MAC value, which is calculated from all the data communicated. When a message with the correct MAC arrives, in step 2, the receiver knows that it is from the sender. If the MAC value calculated by the receiver is equal to the MAC value received from the sender, the authentication succeeds. Otherwise, the authentication fails. However, using symmetric key to send data mutually, makes this protocol vulnerable to the attacks, but the proposed protocol uses symmetric primitives and introduces them as asymmetry with one-way function key chains and a delayed key.

In Mana *et al.* [58] present Trust Key Management that uses ECG signals to address security issues and also uses a symmetric key cryptography in the WBAN. The authentication is among the sink and sensor nodes together. The scheme includes key generation, key set-up, key authentication phase, and key update phase. Figure 20 gives a description of Trust key Management scheme for generating cryptographic key from the ECG signal. MAC is used to ensure the integrity computation. The ECG signal generates a binary sequence, which is called biokey. The biokey is a symmetric encryption key. Also, the scheme uses MD5 function to ensure user confidentiality. In authentication steps, the *sensor node* $1_{ID,}$ and the *sensor node* 2_{ID} are two node identifiers, K_{12} is a symmetric key between the *sensor node 1* and the *sensor node 2* and F_E is used as encryption function. When the *sensor node 2* receives the *sensor node* 1_{ID} and the key authentication K_{12}, it tries to authenticate its gateway *1* using a reply. To do so, the *sensor node 2*, generates a nonce $N'2$, then it encrypts $N'2$ with the key authentication K_{12} and broadcasts $N'2$ to the *sensor node 1*. When the *sensor node 1* receives an 'authenticate me' message, it calculates its own copy of $K_{12} = M\ (Ksession_1 \| N_1)$ and replies with the main nonce $N'2$ and a new nonce $N'1$. The newly agreed key K_{12} encrypts $N'2$ and $N'1$. To complete the *sensor node 2*'s authentication, the *sensor node 2* replies with the nonce $N'1$ encrypted with the shared key K_{12}. The authentication steps are described as below:

$$Node2 \rightarrow Node1 : Id_2,\ F_{E\ K12}(N'2)\quad .$$
$$Node1 \rightarrow Node2 : Id_1,\ F_{E\ K12}(N'2,\ N'1).$$
$$Node2 \rightarrow Node1 : Id_2, F_{E\ K12}(N'1)\quad .$$

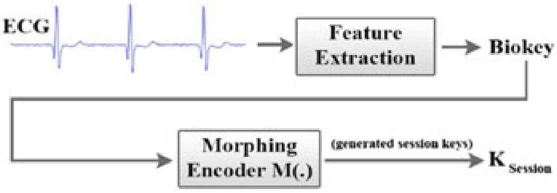


Figure 20. The key generation scheme from ECG-signal in [58].

A biometric-based security framework is presented by Wang *et al.* in [98], where ECG signal is an encryption key. Also, the protocol is based on wavelet-domain hidden Markov Model (HMM), which is used to discern the biometric specification for the authentication. For authentication in the scheme, the sensor node 1 and the sensor node 2 share the same biometric data. Biometric specification and hashes, which are calculated based on the main message, create an authentication message. The sensor node 2 calculates the hash. The scheme uses an hidden markov model likelihood estimation algorithm to manage the authentication process. If the received message matches the signal, then it will be accepted and authentication will succeed. Otherwise, the message is denied, discarded, and authentication fails. The benefit of this method is to operate the statistically same biometric data shared at any positions of the body.

Zhang *et al.* in [99] have proposed a biometric-based authentication scheme for WBAN, which uses ECG signal from the human body. The scheme is also based on the IJS that allows neighboring nodes in WBANs to share a common key, which is generated by ECG signals for the message authentication. The proposed authentication scheme is depicted in Figure 21.

This ECG-IJS-based scheme focuses on authentication and intercommunication between the sensor nodes in the body area network, and both the sender and the receiver use a same algorithm. The protocol has four steps: key hiding, key recovering, authentication, and acknowledgement. In the scheme, F and F' are the keys to encrypt and decrypt. ECG signal extracts the features of the F key to form a secret k. The secret key k is used to encrypt the glucose data or general message, and sends the encrypted message, MAC value, and IJS coefficients. After the receiver gets

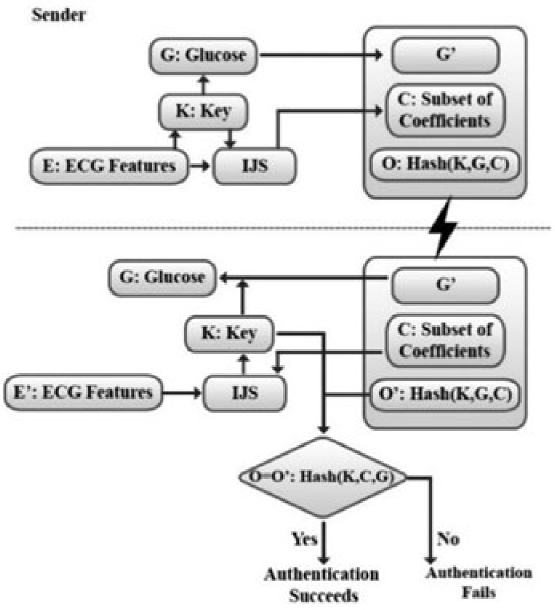


Figure 21. ECG-IJS authentication in scheme [99].

the packet, it could recover the secret *k* using the ECG signal measured at the receiver's site and then it can decrypt the encrypted message using the key *k*. When the message is received at the receiver, the MAC is recalculated from it using the same algorithm. The results will be compared with the received MAC to complete the authentication process. The sender, based on the ECG signal, creates a monic polynomial with a degree *s*, and *t* coefficients are sent to the receiver by using a hash value. Then, the receiver recovers the other $s-t$ coefficients based on the *t* received coefficients. Then, the ECG features the receiver's measures. The ECG features at the receiver should be similar to the ones at the sender, then the receiver will be able to recover the other $s-t$ coefficients of the monic polynomial. The recalculated hash value matches with the received hash value, then the receiver has successfully recovered the $s-t$ coefficients set and the authentication process is completed. The receiver calculates MAC value. Authentication succeeds, if the receiver MAC value is identical to the MAC value from the sender, otherwise, the authentication phase fails. After successful authentication, the receiver sends an acknowledgement to the sender.

Skipjack is a symmetric key cryptography algorithm, which is proposed by Sangari *et al.* in [100]. This algorithm is a low cost and high quality electrocardiography and diagnostic system for healthcare applications, also it protects the patient's data against eavesdropping attack. Skipjack algorithm is a secret key encryption algorithm which provides the secure communication nodes between the sensor and mobile. The following Figure 22 shows the secure data transmission between the sensor nodes and mobile device or laptop.

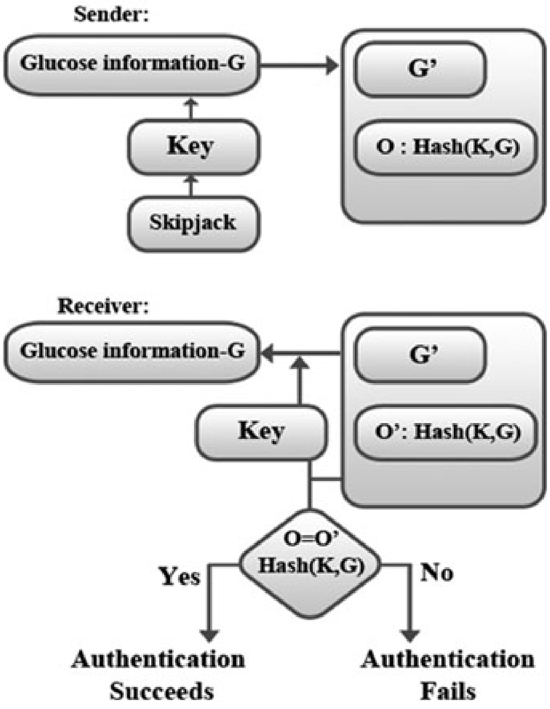


Figure 22. Skipjack authentication in scheme [100].

The sender's information is encrypted by using skipjack algorithm and then it calculates the hash value for a key and sensor data. These results are sent to the receiver side. The receiver again calculates the hash value for the encrypted message. If both values are equal, then only the authentication is successful.

In Kuroda *et al.* [101] evaluate Carousel rotating protocol (CRP), which is a type of Zero-admin mutual authentication system that provides mutual authentication protocol between the two entities. The OneCRP operates among the coordinator and the sensor node, which expects user's specific data as seed data to create a common key between the entities. Both entities update the common key when new data is stored in the top cell in the sensor and use it to encrypt/decrypt the data. The OneCRP has three stages to create secure communication path between the entities as shown in Figure 23. A sensor obtains a seed from itself, such as a production serial number, and puts it into all the cells of the carousel. The sensor then sends the seed to the coordinator. The coordinator verifies the seed by consulting a sensor management system and sets the data into the carousel. At this stage, both entities confirm the data in all the cells and communication between the entities. The second stage is the place where the data in cells are updated with that generated by the sensor. Users can verify the state offline because both entities are located close to each other. The sensor node puts new data into the carousel and rotates it randomly. Next, the sensor node, by using the data creates a key, and then it sends the new key to the coordinator. The sensor node uses the previous key to send the new key. Then, the coordinator rotates the carousel, at the meantime, the coordinator tries to concurrent the carousel with the sensor node. The coordinator decrypts the data. It should update the cell information. The sensor node and the coordinator carousels are concurrent.

In [102] Kanjee and Liu propose two authentication protocols for WBAN that adopts a generic programming concept for cross-layer design of the security in WBAN. This scheme applies data collection nodes (DCNs), aggregation node, and base station node (BSN)/local authentication server (LAS). The data collection nodes, on-body sensors, and the aggregation node are used to cumulate data from data collection nodes and to issue commands. The BSN and the LAS are off-body devices to communicate wirelessly with multiple aggregation nodes. It also serves as a gateway between the WBAN and the master authentication server (MAS) for remote users to access the WBAN system. In the two-tiered authentication protocol, the physiological signals are used to implement a U-key authentication scheme. For on-body nodes physiological authentication, the first tier gets the person's on-body nodes, that is, several data collection nodes and one aggregation node, to authenticate between themselves. They can utilize their shared physiological measures to agree upon a symmetric cryptographic key. This secret key is used for their mutual authentication. They can also conduct non-

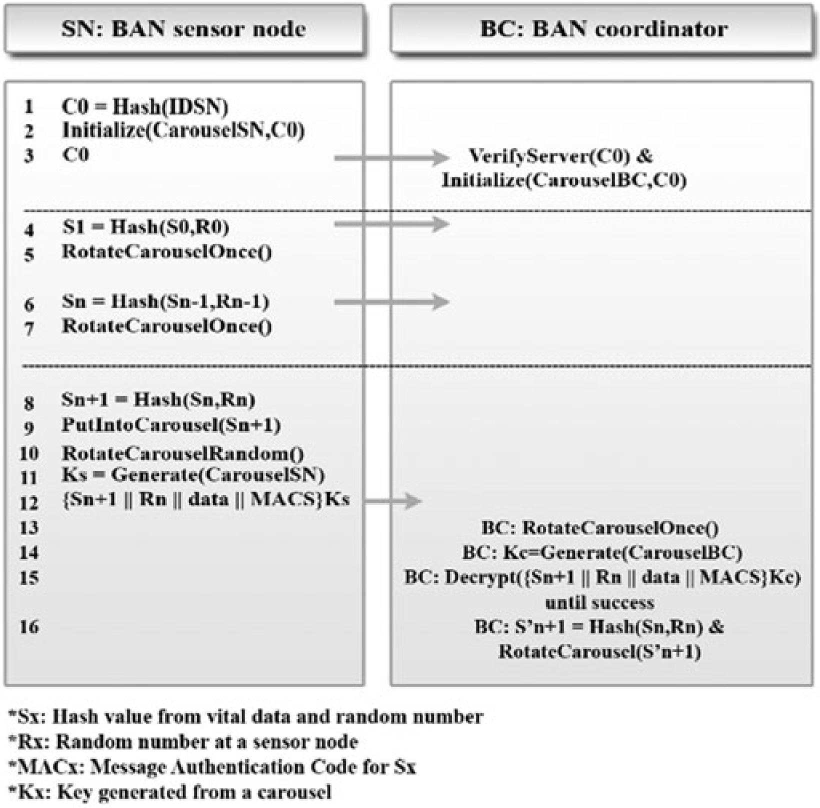

SN: BAN sensor node
BC: BAN coordinator
1 C0 = Hash(IDSN)
2 Initialize(CarouselSN,C0)
3 C0
VerifyServer(C0) &
Initialize(CarouselBC,C0)
4 S1 = Hash(S0,R0)
5 RotateCarouselOnce()
6 Sn = Hash(Sn-1,Rn-1)
7 RotateCarouselOnce()
8 Sn+1 = Hash(Sn,Rn)
9 PutIntoCarousel(Sn+1)
10 RotateCarouselRandom()
11 Ks = Generate(CarouselSN)
12 {Sn+1 || Rn || data || MACS}Ks
13 BC: RotateCarouselOnce()
14 BC: Kc=Generate(CarouselBC)
15 BC: Decrypt({Sn+1 || Rn || data || MACS}Kc) until success
16 BC: S'n+1 = Hash(Sn,Rn) & RotateCarousel(S'n+1)
*Sx: Hash value from vital data and random number
*Rx: Random number at a sensor node
*MACx: Message Authentication Code for Sx
*Kx: Key generated from a carousel

Figure 23. OneCRP protocol in scheme [101].

cryptographic authentication without using any key. Because of the large discrepancy between the on-body and off-body channels RSS variation, the on-body nodes are able to accept each other while rejecting off-body nodes as malicious. Various physiological signals have been demonstrated for key agreement. The aggregation node features two states, reflecting two levels of security status. The first state is valid, when a person sets up his or her WBAN system. The validation procedure involves three automatic steps. In step 1, the aggregation node plugs to the oracle that matches the aggregation node's identification with its entry in the master authentication server. In step 2, the oracle generates a public key or private key pair for the aggregation node upon matching. In step 3, the aggregation node's public key is published to its BSN or LAS, which updates the information to the master authentication server. A valid aggregation node is now ready for authentication as the second part of the two-tiered authenticating WBAN system. In a plug and play manner, the first tier involves three steps, using photoplethysmogram to illustrate the authentication, after the aggregation node validates itself with oracle. Two-tiered authenticating WBAN system has three steps. In step 1, the aggregation node initiates authentication to the data collection nodes. In step 2, the aggregation node and the data collection nodes generate their physiological features, and in step 3, the aggregation node agrees with the shared keys of the data collection nodes or connects in the cluster communication with the data collection nodes.

4.3. Channel-based authentication

Channel-based solutions leverage the RSS variations to achieve authentication and to differentiate between the legitimate nodes and attackers [39].

In Shi *et al.* [6] propose the one way channel-based authentication scheme for WBANs, called body area network authentication (BANA). The proposed BANA can accurately identify multiple attackers with minimal amount of the overhead. As shown in Figure 24, because the on-body sensor and control unit are very close to one another, the RSS received from the reflection off the floors and walls just contributes a small proportion to the all over RSS.

As shown in Figure 25, the authentication process in BANA scheme includes 4 steps, where in step 1, the control unit broadcasts a hello message to the sensor, and then in step 2, the sensor generates a small random number and sends response messages to the control unit. After the control unit has agreed on the random numbers, in step 3, the control unit having collected the RSSs for all the responding devices, calculates the average RSS variation (ARV). Finally, in step 4, based on the classification result, the control unit accepts the sensor devices, that the average

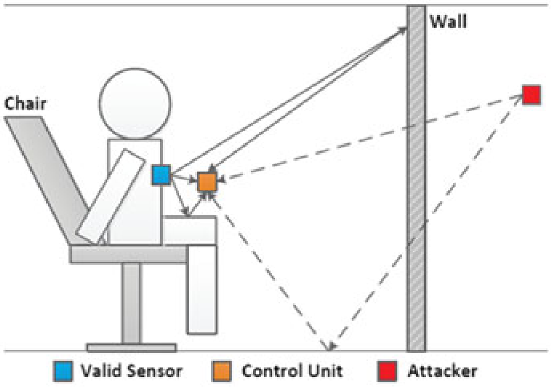
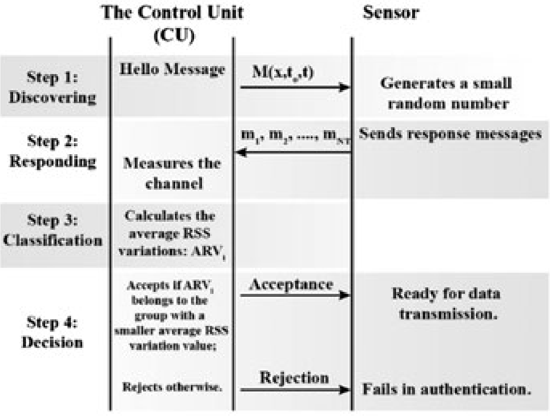


Figure 24. RSS Authentication [6].



	The Control Unit (CU)		Sensor
Step 1: Discovering	Hello Message	$M(x,t_e,t)$ →	Generates a small random number
Step 2: Responding	Measures the channel	$m_1, m_2, ..., m_{NT}$ ←	Sends response messages
Step 3: Classification	Calculates the average RSS variations: ARV_i		
Step 4: Decision	Accepts if ARV_i belongs to the group with a smaller average RSS variation value;	Acceptance →	Ready for data transmission.
	Rejects otherwise.	Rejection →	Fails in authentication.

Figure 25. The authentication process in scheme [6].

RSS variation values belong to the cluster with a smaller average of the average RSS variation, while rejecting the devices in the other group.

A cryptography based authentication scheme is proposed in [103] by Zhang *et al.*, which, body sensors allow to share a common key, is generated from the wireless channel between each sensor. Also, the received signal strength indicator (RSSI) values are sampled and channel features set are generated. The channel features set are used as keys to secure data communications over wireless channels by using IJS algorithm which does not need a key predistribution and uses a dynamic key in a plug-and-play manner. In this authentication scheme, both the sender and receiver measure the RSSI and generate feature sets. Then, the channel features F and F' are extracted from the sender (sensor A) and the receiver (sensor B), respectively. At the sender, the channel features form a secret key, which is used to encrypt the body vital sign messages that need to be transmitted with data or a general message. The IJS algorithm locks the process, *t degree* coefficients of the monic polynomial are sent to the receiver, and also *t degree* sends the encrypted message and the hash value based on MAC are sent. When the receiver gets the packet, it could recover the secret using the channel feature F', it is measured after the unlocking process of the IJS algorithm. Then, it decrypts the encrypted message, and calculates the MAC code using the same hash function. The results are compared with the received MAC to complete the authentication process. The specified authentication method is depicted in Figure 26.

In Javali *et al.* [104] present a channel-based authentication and a key generation for WBAN, named SeAK. In the authentication and key generation phase of SeAK protocol, in step 1, when the user device is close enough to the control unit, it sends requests to the control unit. In step 2, the control unit sends a probe package to the device from one of its antennas. In reply, the sensor device appraises the RSSI of the received package and transfers a probe reply to the control unit. The control unit evaluates the RSS indicator. The index value $i = \{1, 2, \ldots, N\}$ tracks the number of packages N required for the aggregation method. In step 3, the control unit transmits a total of N packets at an interval, randomly switching between the two antennas, in order to evaluate the RSSI difference, the control unit stores the RSSI obtained at the two antennas, respectively. In step 4, the absolute average RSSI difference is calculated, and in step 5, control unit compares average RSSI with the threshold RSSI difference and the device is authenticated as legitimate if average RSSI is greater than threshold RSSI, else it will be discarded. The control unit apprises the user device, that authentication is successful by sending an accept message. After successful, authentication, the control unit, and the device use the RSSI values to generate a shared secret key.

Wu *et al.* in [105] present a channel-based authentication, named R^{2}NA, in which the body area nodes do not need to send request messages at the same time. The authentication phase of this protocol is described between the control unit, the sensor node, and the sender. The control unit may refer to the PDA or a smart phone. For authentication, first, a sender needs to be close to the control unit or to the sensor node in a body area network. In Figure 27, the final protocol is illustrated. At

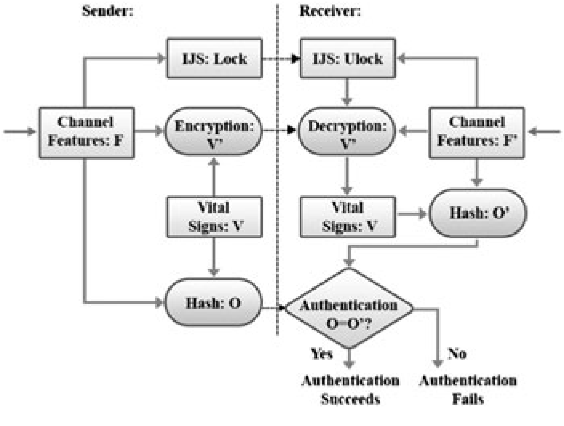


Figure 26. Channel Information based cryptography and authentication scheme in [103].

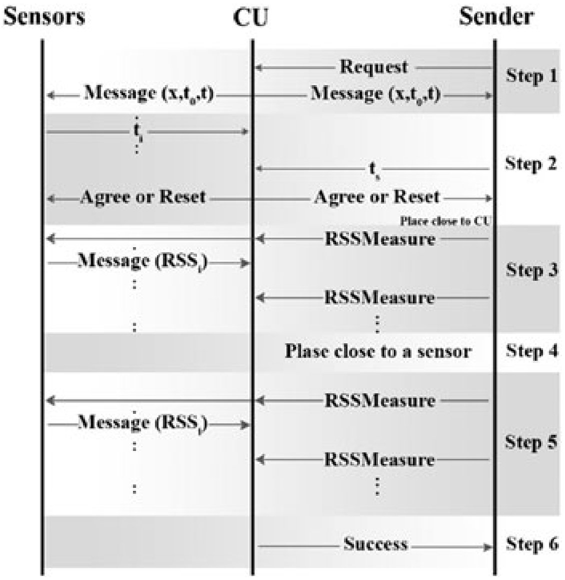


Figure 27. The final R^2NA protocol scheme in [105].

step 1, when the control unit receives a request, it broadcasts a 'hello message' to the devices, close to it. The message contains timestamp 0. In step 2, when the sensor node or the sender receives a message, it creates a random number, and then sends a message to the control unit.

In step 3, random numbers are confirmed by the control unit. Then, the respond devices send messages to the control unit. The control unit gets all RSS readings to calculate the RSS ratio, *r*. Steps 4 and 5 reduce the possibility of attacks in the crowded scenarios, by using RSS measurement. In Step 6, the control unit checks all the RSS values, and the control unit calculates the RSS ratio. If the control unit finds a competent number of successive packets whose mean of *r* is above a threshold, *rh*, then the control unit knows that the requester is close. Also, the control unit detects if the sender is close with a sensor, and by convincing these situations, the control unit sends a 'success message' to the requester.

ASK-BAN is a lightweight and fast certified secret key extraction scheme for internal (intra-BAN) communication, which is proposed by Shi *et al.* in [106]. The ASK-BAN is RSS-based scheme and uses channel measurements. This scheme provides multi-hop authentication between the control unit and on-body sensors with the help of trusted sensors as relay nodes. The proposed authenticated scheme can be described by the following steps: Pairwise key generation, initial authentication, authenticated secret capacity broadcast, deciding maximum entropy, and key aggregation broadcast. First, the control unit forwards a 'hello message' to the sensors which are around it, for initial authentication. Then, the control unit requests replies after *x* seconds, where *x* is a random number of choices by the control unit. When the hello message is received by sensor, each sensor chooses a small number t_r randomly and broadcasts it. The control unit collects all the t_r values, also checks values, and ensures no duplicated ones exist to avoid collision. Then, all the responding sensors broadcast response messages *m* in the time division duplex manner as scheduled, repeatedly

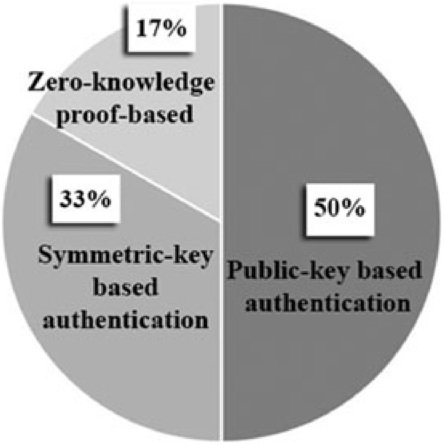


Figure 29. Percentage of the zero-knowledge proof-based, asymmetric and symmetric proposed authentication schemes.

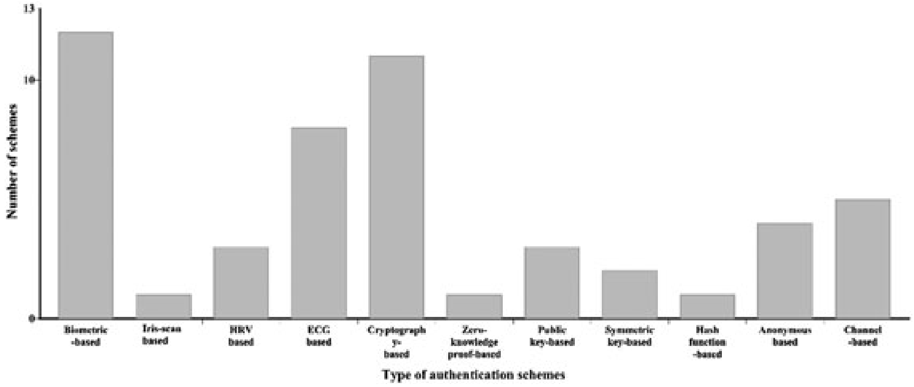


Figure 28. Number of proposed authentication schemes for WBANs.

Table II. Classification of the proposed authentication schemes for WBAN.

	Biometric-based authentication				Cryptography-based authentication					Hybrid authentication		
Scheme	Iris scan	Heart rate variability (HRV)	Electrocardiogram (ECG)	Channel-based authentication	Zero-knowledge proof-based	Asymmetric key (public key)	Symmetric key	Hash function	Anonymous authentication	Biometric-based methods	Channel-based methods	Cryptography-based methods
[1]	—	—	—	—	—	—	—	—	✓	—	—	—
[6]	—	—	—	✓	—	—	—	—	—	—	—	—
[10]	✓	—	—	—	—	—	—	—	—	—	—	—
[46]	—	—	—	—	✓	—	—	—	—	—	—	—
[58]	—	—	✓	—	—	—	—	—	—	✓′	—	✓
[62]	—	—	—	—	—	✓	—	—	—	—	—	—
[63]	—	—	—	—	—	✓	—	—	—	—	—	✓
[64]	—	—	—	—	—	✓	—	—	—	✓	—	✓
[70]	—	—	—	—	—	—	✓	—	—	—	—	—
[71]	—	—	—	—	—	—	✓	—	—	—	—	✓
[72]	—	—	—	—	—	—	—	✓	—	—	—	—
[76]	—	—	—	—	—	—	—	—	✓	—	—	—
[77]	—	—	—	—	—	—	—	—	✓	—	—	—
[78]	—	—	—	—	—	—	—	—	✓	—	—	✓
[91]	—	✓	—	—	—	—	—	—	—	—	—	—
[92]	—	✓	—	—	—	—	—	—	—	✓	—	✓
[93]	—	✓	—	—	—	—	—	—	—	—	—	—
[96]	—	—	✓	—	—	—	—	—	—	—	—	—
[97]	—	—	✓	—	—	—	—	—	—	—	—	—
[98]	—	—	✓	—	—	—	—	—	—	—	—	—
[99]	—	—	✓	—	—	—	—	—	—	✓	—	✓′
[100]	—	—	✓	—	—	—	—	—	—	—	—	—
[101]	—	—	✓	—	—	—	—	—	—	—	—	—
[102]	—	—	✓	—	—	—	—	—	—	—	—	—
[103]	—	—	—	✓	—	—	—	—	—	—	✓	✓
[104]	—	—	—	✓	—	—	—	—	—	—	—	—
[105]	—	—	—	✓	—	—	—	—	—	—	—	—
[106]	—	—		✓	—	—	—	—	—	—	—	—

every t milliseconds and last for t_0 seconds. During the t_0 seconds, each node, including the control unit, measures the RSS value of each received message, and t is required to be no less than the channel coherence time. Then, RSSs is collected from all the responding sensors, and each node calculates the average RSS variation. Applying classification algorithms to the average RSS variation values, that is partitioned into two groups, where one group has a smaller mean of the average RSS variations and the other group has a larger one. Then, control unit accepts the sensors, of the average RSS variations belonging to the group with the smaller average RSS variation mean, then it rejects the remaining ones in the other group and each node authenticates all the other nodes.

5. DISCUSSION

The authentication schemes discussed in the previous section have their own advantages and disadvantages.

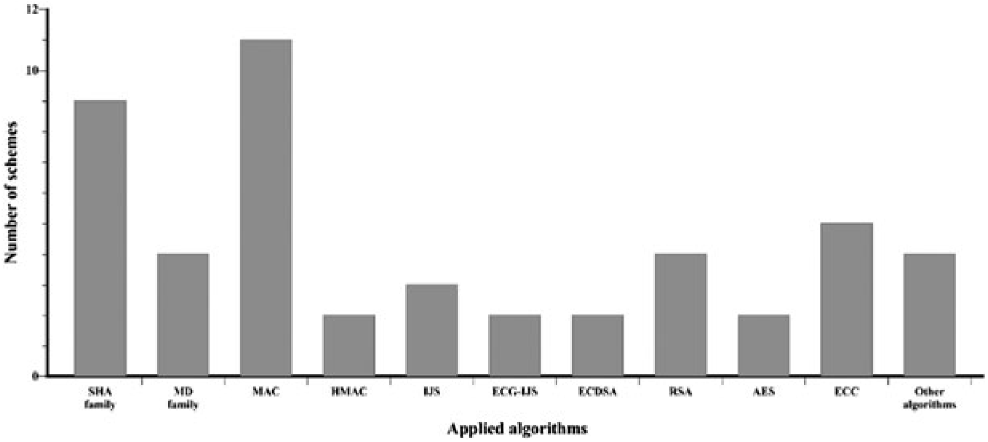


Figure 30. Applied cryptographic algorithms in the proposed authentication schemes for WBAN.

Table III. Applied cryptographic algorithms in the proposed authentication schemes for WBAN.

Scheme	Hash function				Cryptography function						
	SHA family	MD family	MAC	HMAC	IJS	ECG-IJS	ECDSA	RSA	AES	ECC	Other algorithms
[1]	✓		✓	—	—	—	—	✓	—	—	—
[46]	✓	—	—	—	—	—	✓	—	—	✓	—
[58]	—	✓	—	—	—	—	—	—	—	—	—
[62]	—	—	✓	—	—	—	✓	—	—	✓	—
[63]	—	—	✓	—	—	—	—	—	✓	✓	—
[64]	✓	✓	—	—	—	—	—	—	—	—	
[71]	—	—	—	—	—	—	—	—	—	✓	ECDH, Diffie–Hellman
[72]	✓	✓	✓	✓	—	—	—	—	—	—	—
[76]											
	✓	—	—	—	—	—	—	—	—	✓	—
[77]	—	—	✓	—	—	—	—	✓	—	—	—
[78]	✓	—	—	—	—	—	—	—	—	—	—
[91]	✓	✓	—	—	—	—	—	✓	✓	—	—
[92]											
	—	—	✓	—	—	—	—	—	—	—	—
[97]	✓	—	✓	—	✓	✓	—	—	—	—	—
[98]	—	—	✓	—	—	—	—	—	—	—	—
[99]											
	—	—	✓	—	✓	✓	—	—	—	—	—
[100]	—	—	—	—	—	—	—	—	—	—	Skipjack
[101]	—	—	✓	—	—	—	—	—	—	—	—
[103]	✓		✓	✓	✓	—	—	✓	—	—	DES

This section presents a comprehensive comparison and discussion about various features of the authentication schemes proposed for WBANs. As outlined before, various cryptographic and biometric-based methods are applied for conducting authentication in the WBAN. Figure 28 exhibits the number of the proposed schemes for each authentication method. As indicated in this figure, numerous schemes have used biometric features and behaviors for authentication process. In this context, the ECG signals are applied by more authentication and it is often applied to achieve a common cryptographic key.

Figure 29 indicates the percentage of the ZKP-based, asymmetric-based, and symmetric-based authentication schemes proposed for WBANs.

As outlined before, we have classified these schemes into the biometric-based, channel-based and cryptographic-based, and hybrid authentication schemes. Table II determines that each authentication schemes proposed for WBANs utilizes which authentication schemes and provides a brief insight about the techniques combined and utilized in each authentication scheme. The information of this table indicates which methods are not applied together and can be the subject of next researches and studies. Moreover, Figure 30 exhibits the number of authentication schemes which have applied each cryptographic algorithm. Besides, Table III determines that which cryptographic algorithms have been applied by each proposed authentication scheme.

We can classify the proposed authentication schemes for WBAN, based on the type of authentication. Figure 31 indicates the percentage of the one-way and mutual communications between sensors, hubs, and sink.

Moreover, we can classify the authentication schemes into anonymous and non-anonymous schemes. Figure 32 indicates the percentage of the anonymous and non-anonymous authentication schemes proposed for WBAN.

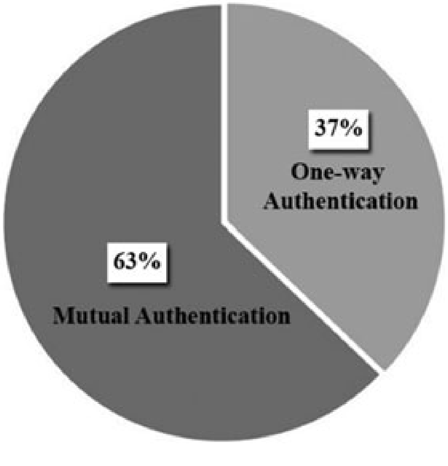


Figure 31. Percentage of the proposed one-way and mutual authentication schemes.

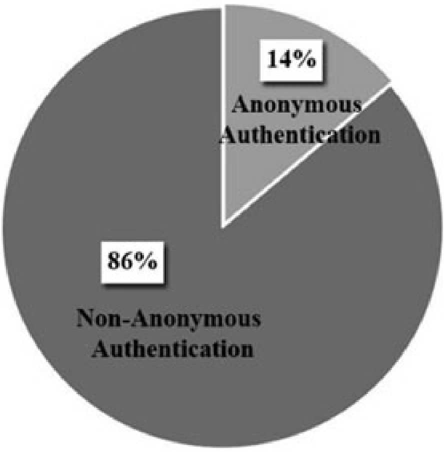


Figure 32. Percentage of the proposed Anonymous and non-anonymous authentication schemes.

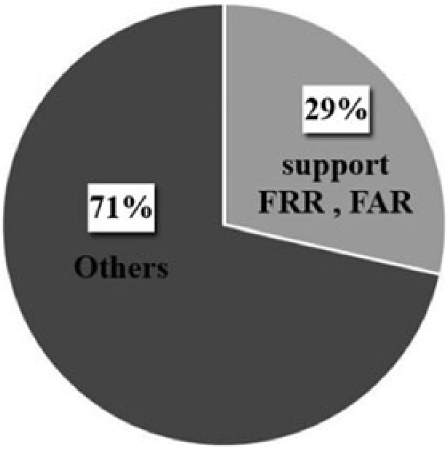


Figure 33. Percentage of the schemes support FRR and FAR.

Also Figure 33 indicates the percentage of the schemes which support low FRR and low FAR. Table IV summarizes the authentication capabilities of the proposed authentication schemes for WBAN and specifies that each proposed scheme can authenticate the communication between sensors, hub, and sink. In this table, a hub may be a PDA and a sink can refer to a function that receives incoming events from another function like a base station. Moreover, it specifies that the provided authentication service can be one-way, two-way, or mutual authentication.

Table V lists some properties of the cryptographic-based authentication schemes and indicates that which solutions have used the key distribution and KDC and trusted third party or certificate authorities. For example, in some cryptographic-based authentication schemes, KDC is used to reduce the risks of key exchanging and shares a different secret symmetric key with each registered user [107]. In addition, some of the proposed schemes use a CA to create and manage the public and private keys.

Table IV. Authentication capabilities of the proposed authentication schemes for WBAN.

	Sensor-to-sensor		Sensor-to-hub		Sensor-to-sink		Hub-to-sink	
Scheme	One-way authentication	Mutual authentication	One-way authentication	Mutual authentication	One-way authentication	Mutual authentication	One-way authentication	Mutual authentication
[1]	—	—	—	—	—	—	—	✓
[6]	—	✓	—	—	—	✓	—	—
[46]	—	—	—	✓	✓	✓	—	—
[58]	—	✓	—	✓	—	✓	—	—
[62]	—	—	—	—	—	✓	—	—
[63]	—	—	—	—		✓	—	—
[70]	—	✓	—	✓	—	✓	—	—
[71]	—	—	—	—	—	✓	—	✓
[76]	—	✓	✓	—	—	✓	—	—
[91]	—	—	—	✓	—	—	—	—
[96]	—	✓	✓	—	—	✓	—	—
[97]	✓	—	—	✓	—	✓	—	—
[98]	—	—	—	—	—	✓	—	—
[100]	—	—	—	—	✓	—	—	—
[101]	✓	✓	✓	—	✓	—	—	—
[102]	—	—	—	✓	—	✓	—	—
[105]	—	—	—	—	—	✓	—	—
[106]	—	✓	—	✓		✓	—	✓

DOI: 10.1002/sec

Table V. Properties of the cryptography-based authentication schemes proposed for WBAN.

Scheme	Key distribution center	Key distribution	Third party/ certificate authority	Plug-and-play
[1]	—	✓	✓	—
[63]	✓	—	—	—
[76]	—	—	Certificate authority	—
[78]	—	—	Certificate authority	—
[92]	—	✓	—	—
[96]	—	—	✓	—
[97]	—	—	—	✓
[99]	—	✓	—	✓
[100]	—	✓	—	—
[102]	—	—	—	✓
[103]	—	—	—	✓
[106]	—	✓	—	✓

Moreover, the plug-and-play feature is also determined for each scheme.

One of the important issues in the authentication schemes proposed for WBANs is simulation scenarios and the software used to simulate these schemes. Table VI indicates some information about the simulation scenarios applied in the proposed schemes. For example, details such as, number of sensors, number of sinks, and their positions, patient's environment, and operating system are investigated for each scheme. The information of this table highlights the scenarios which can be considered in WBANs. For example, as shown in this table, small number of sensors, and sink nodes are considered in each scheme and sensors and sinks can be positioned on the body, or off the body. Besides, Figure 34 indicates the type of the software which are applied for the simulation of the proposed WBAN schemes and the number of schemes which have been used for each software.

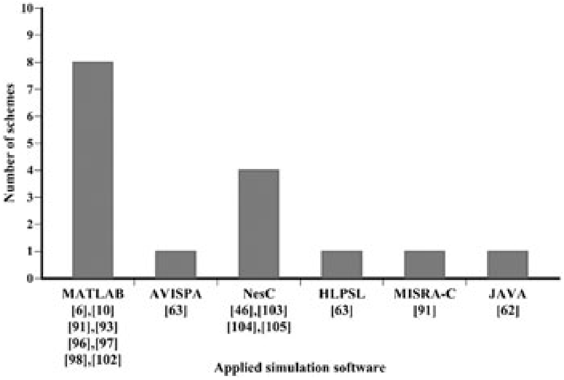


Figure 34. Applied simulation software.

Table VI. Simulation Scenario in the proposed schemes.

			Sensor position			Sink position			Patient's environment	operating system
Scheme	Number of sensors	Number of sinks	On body	In body	Off-body	On body	In body	Near		
body										
[1]	1	1	—	—	—	—	—	—	—	Windows CE 5.2 OS
[6]	7	1	✓	—	✓	✓	—	✓	Room, Corridor and Hospital	—
[46]	2	1	✓	✓	—	—	—	✓	—	TinyOS
[58]	5	1	✓	—	—	✓	—	✓	—	—
[63]	—	—	—	—	—	—	—	—	—	—
[64]	1	1	—	✓	✓	—	—	✓	—	—
[70]	2	1	✓	✓	—	—	—	✓	—	—
[71]	1	2	✓	✓	—	—	—	✓	—	—
[78]	1	1	✓	✓	—	—	—	—	—	—
[91]	—	—	—	✓	—	—	—	✓	—	—
[92]	—	—	—	✓	—	—	—	—	—	—
[93]	1	1	—	✓	—	—	—	—	—	—
[96]	7 or 8	1	✓	✓	—	—	—	✓	—	—
[98]	2	1	✓	✓	—	—	—	—	—	—
[101]	4	1	✓	✓	—	✓	—		—	—
[102]	—	1	✓	—	✓	—	—	✓	—	—
[103]	2	—	✓	✓	—	✓	✓	—	Room	TinyOS
[104]	—	1	✓	—	✓	✓	—	—	Room	TinyOS
[105]	3	1	✓	✓	✓	✓	—	✓	Room	TinyOS
[106]	5	1	✓	—	—	✓	—	✓	Room and Corridor	—

6. CONCLUSION

Wireless Body Area Network or WBAN is a wireless network used for extracting medical data from the medical sensors positioned in or around the human body. WBANs play a key role in the E-Health systems, and their information is applied in various medical and non-medical applications.

However, due to the unreliable wireless media, WBANs are exposed to a variety of security attacks, and it is necessary to provide security services such as authentication to prevent malicious behaviors and attacks. Numerous state of the art authentication schemes have been proposed in the literature for the WBANs which provide one-way authentication, mutual authentication, and anonymous authentication services. In this paper, we present a survey and taxonomy of these schemes and provide a detailed description of each authentication scheme in detail.

In addition, we have classified the proposed schemes based on their authentication methods and analyzed their features, limitations, and advantages. Besides, a complete comparison of the properties of the authentication schemes are presented, which can be very useful in conducting future researches and studies.

In the future research and studies, more effort should be made to better integrate the WBAN to the E-healthcare system and its infrastructure. Also, new secure schemes can be provided to be assisted by mobile cloud computing.

REFERENCES

1. Liu J, Zhang Z, Chen X, Kwak K. Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks. 2014.
2. Xu X, Shu L, Guizani M, Liu M, Lu J. A survey on energy harvesting and integrated data sharing in wireless body area networks. *International Journal of Distributed Sensor Networks* 2015; **11**(10): 438695, 17 pages.
3. Latré B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks. *Wireless Networks* 2011; **17**(1):1–18.
4. Zhang L, Liu J, Sun R. An Efficient and Lightweight Certificateless Authentication Protocol for Wireless Body Area Networks. in *Intelligent Networking and Collaborative Systems* (*INCoS*), *2013 5th International Conference on*. 2013. IEEE.
5. Hamdi O, Chalouf MA, Ouattara D, Krief F. EHealth: survey on research projects, comparative study of telemonitoring architectures and main issues. *Journal of Network and Computer Applications* 2014; **46**: 100–112.
6. Shi L, Li M, Yu S, Yuan J. Bana: body area network authentication exploiting channel characteristics. *Selected Areas in Communications, IEEE Journal on* 2013; **31**(9): 1803–1816.
7. Ullah S, Mohaisen M, Alnuem MA. A review of IEEE 802.15.6 MAC, PHY, and security specifications. *International Journal of Distributed Sensor Networks* 2013; **9**(4): 950704, 12 pages.
8. Huang R, *et al.* Health Information Science. In *Analysis and Comparison of the IEEE 802.15. 4 and 802.15. 6 Wireless Standards Based on MAC Layer*. Springer: Melbourne, Australia, 2015; 7–16.
9. Toorani M. On Vulnerabilities of the Security Association in the IEEE 802.15. 6 Standard. arXiv preprint arXiv:1501.02601, 2015.
10. Ullah MG, *et al.* Wireless body area sensor network authentication using voronoi diagram of retinal vascular pattern. *Wireless Personal Communications* 2014; **76**(3): 579–589.
11. Sampangi RV, Dey S, Urs SR, Sampalli S. A security suite for wireless body area networks. arXiv preprint arXiv:1202.2171, 2012.
12. Qadri SF, Awan SA, Amjad M, Anwar M, Shehzad S. APPLICATIONS, CHALLENGES, SECURITY OF WIRELESS BODY AREA NETWORKS (WBANS) AND FUNCTIONALITY OF IEEE 802.15. 4/ZIGBEE. 2013.
13. Saleem S, Ullah S, Kwak KS. A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors* 2011; **11**(2): 1383–1395.
14. Javadi SS, Razzaque M. Wireless Networks and Security. In *Security and Privacy in Wireless Body Area Networks for Health Care Applications*. Springer: Berlin, Germany, 2013; 165–187.
15. Saleem S, Ullah S, Yoo HS. On the security issues in wireless body area networks. *JDCTA* 2009; **3**(3): 178–184.
16. Bradai N, Chaari L, Kamoun L. A comprehensive overview of wireless body area networks (WBAn). *Digital Advances in Medicine, E-Health, and Communication Technologies* 2013: 1, ISBN13: 9781466627949.
17. Talwar M, Mallikarjun CS. Security threads and quality of service challenges for wireless sensor networks: a survey. *History* 2014; **10**(21): 15–23.
18. Xing K, Srinivasan SSR, Jose M, Li J, Cheng X. Attacks and countermeasures in sensor networks*:* a survey*, in* Network security. Springer: New York, USA, 2010; 251–272.
19. Sivaprasatham V, Venkateswaran J, Omar HTB. Integrated Authentication Based on CDMA Modulation for Physical Layer Security of Wireless Body Area Network. Editors-in-Chief: p. 388.
20. Wang Y, Attebury G, Ramamurthy B. *A survey of security issues in wireless sensor networks*. Nebraska, USA, 2006.
21. Zia T, Zomaya A. *Security issues in wireless sensor networks*. in *Systems and Networks Communications*,

2006. ICSNC'06. International Conference on. 2006. IEEE.

22. Mana M, Feham M, Bensaber BA. SEKEBAN (Secure and Efficient Key Exchange for wireless Body. in *Area Network*)", *International Journal of Advanced Science and Technology*. 2009. Citeseer.
23. Pandey A, Tripathi R. A survey on wireless sensor networks security. *International Journal of Computer Applications* 2010; **3**(2): 43–49.
24. Raazi SMK-u-R, Lee H, Lee S, Lee Y-K. BARI+: a biometric based distributed key management approach for wireless body area networks. *Sensors* 2010; **10**(4): 3911–3933.
25. Hughes L, Wang X, Chen T. A review of protocol implementations and energy efficient cross–layer design for wireless body area networks. *Sensors* 2012; **12**(11): 14730–14773.
26. Shaqiri I. Some Security Aspects at Wireless Sensor Networks.
27. Pathania S, Bilandi N, SECURITY ISSUES IN WIRELESS BODY AREA NETWORK. 2014.
28. Sharma N, Bansal EM. Preventing impersonate attacks using digital certificates in WBAN. *Int. J. Adv. Engin. Sci. Technol* 2011; **9**: 31–35.
29. Wang J, Wang Q. *Body area communications: channel modeling, communication systems, and EMC.* John Wiley & Sons: New Jersey, USA, 2012.
30. Pomalaza-Ráez C, Taparugssanagorn A. *The UWB Channel in Medical Wireless Body Area Networks (WBANs)*. INTECH Open Access Publisher: Rijeka, Croatia, 2012.
31. Kwak KS, Ullah S, Ullah N. *An overview of IEEE 802.15. 6 standard*. in *Applied Sciences in Biomedical and Communication Technologies* (*ISABEL*), *2010 3rd International Symposium on*. 2010. IEEE.
32. Hwang J-H, Kang T-W, Kim Y-T, Park S-O. Analsysis on co-channel interference of human body communication supporting IEEE 802.15. 6 BAN standard. *ETRI Journal* 2015; **37**(2): 439–449.
33. Bradai N, Fourati LC, Kamoun L. Investigation and performance analysis of MAC protocols for WBAN networks. *Journal of Network and Computer Applications* 2014; **46**: 362–373.
34. Alam MM, Hamida EB. Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities. *Sensors* 2014; **14**(5): 9153–9209.
35. He D, Zeadally S. Authentication protocol for an ambient assisted living system. *Communications Magazine, IEEE* 2015; **53**(1): 71–77.
36. Movassaghi S, Abolhasan M, Lipman J, Smith D, Jamalipour A. *Wireless body area networks: a survey.* Manitoba, Canada, 2014.
37. Rui H, Center ET, China S. *Prospect of wireless body area network technology*. Amsterdam, The Netherlands, 2015.
38. IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. IEEE Std 802.15.6-2012, 2012: 1–271.
39. Aqeel-ur-Rehman IUK, Khan AY. A Review on Authentication Schemes for Wireless Body Area Networks.
40. Chen M, Gonzalez S, Vasilakos A, Cao H, Leung VC. Body area networks: a survey. *Mobile networks and applications* 2011; **16**(2): 171–193.
41. Barakah DM, Ammad-uddin M. *A survey of challenges and applications of wireless body area network* (*WBAN*) *and role of a virtual doctor server in existing architecture*. in *Intelligent Systems*, *Modelling and Simulation* (*ISMS*), *2012 Third International Conference on*. 2012. IEEE.
42. Das A, Veni Madhavan C. *Public-Key Cryptography: Theory and Practice: Theory and Practice*. Pearson Education India: Kharagpur, India, 2009.
43. Alia MA, Tamimi AA, AL-Allaf ON. Cryptography Based Authentication Methods. in *Proceedings of the World Congress on Engineering and Computer Science*. 2014.
44. Kandola S. *A Survey of Cryptographic Algorithms*. St. Lawrence University: Minnesota, USA, 2013.
45. Manickam J. *Public key cryptosystem based security in wireless body area network*. in *Circuit*, *Power and Computing Technologies* (*ICCPCT*), *2014 International Conference on*. 2014. IEEE.
46. Ma L, Ge Y, Zhu Y. TinyZKP: a lightweight authentication scheme based on zero-knowledge proof for wireless body area networks. *Wireless Personal Communications* 2014; **77**(2): 1077–1090.
47. Pirbhulal S, Zhang H, Wu W, Zhang Y. A Novel Biometric Algorithm to Body Sensor Networks*, in* Wearable Electronics Sensors. Springer: New Zealand, 2015; 57–79.
48. Saxena S, Kapoor B. State of the art parallel approaches for RSA public key based cryptosystem. arXiv preprint arXiv:1503.03593, 2015.
49. Alam S, Jamil A, Saldhi A, Ahmad M. *Digital image authentication and encryption using digital signature*. in *Computer Engineering and Applications* (*ICACEA*), *2015 International Conference on Advances in*. 2015. IEEE.
50. Martin L. *Introduction to identity-based encryption*. Artech house: Norwood, Massachusetts, USA, 2008.
51. Yi X, Paulet R, Bertino E. *Homomorphic Encryption and Applications*. Springer: New York, USA, 2014.
52. Kang J, Adibi S. Future Network Systems and Security. In *A Review of Security Protocols in mHealth*

Wireless Body Area Networks (WBAN). Springer, 2015; 61–83.

53. Boyle P, Newe T. *A Survey of Authentication Mechanisms*: *Authentication for Ad-Hoc Wireless Sensor Networks*. in *Sensors Applications Symposium*, *2007*. *SAS'07*. *IEEE*. 2007. IEEE.
54. Ali ST, Sivaraman V, Ostry D. Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. *Future Generation Computer Systems* 2014; **35**: 80–90.
55. Bos JW, *et al.* Financial Cryptography and Data Security. In *Elliptic curve cryptography in practice*. Springer: Christ Church, Barbados, 2014; 157–175.
56. Lee YS, Alasaarela E, Lee HJ. An efficient encryption scheme using elliptic curve cryptography (ECC) with symmetric algorithm for healthcare system. *International Journal of Security and Its Applications* 2014; **8**(3): 63–70.
57. Garg V. *Wireless Communications & Networking*. Morgan Kaufmann: Burlington, Massachusetts, USA, 2010.
58. Mana M, Feham M, Bensaber BA. Trust key management scheme for wireless body area networks. *IJ Network Security* 2011; **12**(2): 75–83.
59. Mainanwal V, Gupta M, Upadhayay SK. A survey on wireless body area network: Security technology and its design methodology issue. in *Innovations in Information*, *Embedded and Communication Systems* (*ICIIECS*), *2015 International Conference on*. 2015. IEEE.
60. Hankerson D, Menezes AJ, Vanstone S. *Guide to elliptic curve cryptography*. Springer Science & Business Media: Berlin, Germany, 2006.
61. Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security* 2001; **1**(1): 36–63.
62. Sangari SS, Manickam M. Security and privacy in wireless body area network. *Indian Streams Research Journal* 2014; **4**: 1–10.
63. Chatterjee S, Das AK, Sing JK. A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University-Computer and Information Sciences* 2014; **26**(2): 181–201.
64. Jang CS, Lee DG, Han JW, Park JH. Hybrid security protocol for wireless body area networks. *Wireless Communications and Mobile Computing* 2011; **11** (2): 277–288.
65. Lieman D. *Public-key Cryptography: American Mathematical Society Short Course, January 13-14, 2003, Baltimore, Maryland*, Vol. **62**. American Mathematical Soc: Providence, Rhode Island, USA, 2005.
66. Clark J, Jacob J. *A survey of authentication protocol literature: Version 1.0*. Citeseer: Pennsylvania, USA, 1997.
67. Mollin RA. *RSA and public-key cryptography*. CRC Press: Boca Raton, Florida, USA, 2002.
68. Saha MS, Anvekar MDK. Protocol Design Issues in Implementing Security for Wireless Body Area Network.
69. Zhang GH, Poon CCY, Zhang YT. A review on body area networks security for healthcare. *ISRN Communications and Networking* 2011; **2011**: 21.
70. Yan R, Liu J, Sun R. The Proceedings of the Third International Conference on Communications, Signal Processing, and Systems. In *An Efficient Authenticated Key Exchange Protocol for Wireless Body Area Network*. Springer: Malden, Massachusetts, USA, 2015.
71. Drira W, Renault E, Zeghlache D. A hybrid authentication and key establishment scheme for wban. in *Trust*, *Security and Privacy in Computing and Communications* (*TrustCom*), *2012 IEEE 11th International Conference on*. 2012. IEEE.
72. Kumbhare YL, Rangaree PH, Asutkar DG. Wireless Body Area Sensor Network Authentication using HMAC function. in *2nd National Conference on Information and Communication Technology* (*NCICT*). 2011.
73. Sako K, Yonezawa S, Teranishi I. Anonymous authentication: for privacy and security. *NEC Journal of Advanced Technology* 2005; **2**(1): 79–83.
74. Rass S, Slamanig D. *Cryptography for Security and Privacy in Cloud Computing*. Artech House: London, United Kingdom, 2013.
75. Slamanig D. Communications and Multimedia Security. In *Anonymous authentication from public-key encryption revisited*. Springer: Ghent, Belgium, 2011.
76. Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *Journal of Medical Systems* 2014; **38**(2): 1–7.
77. Liu J, Zhang Z, Sun R, Kwak KS. An efficient certificateless remote anonymous authentication scheme for wireless body area networks. in *Communications* (*ICC*), *2012 IEEE International Conference on*. 2012. IEEE.
78. Wang C, Zhang Y. New authentication scheme for wireless body area networks using the bilinear pairing. *Journal of Medical Systems* 2015; **39**(11): 1–8.
79. Jain AK, Nandakumar K. Biometric authentication: system security and user privacy. *IEEE Computer* 2012; **45**(11): 87–92.
80. Sarier ND. *A survey of distributed biometric authentication systems*. Bonn, Germany update, 2015: p. 11.

81. Todorov D. *Mechanics of user identification and authentication: Fundamentals of identity management*. CRC Press: Boca Raton, Florida, USA, 2007.
82. Kisku DR, Gupta P, Sing JK. *Advances in biometrics for secure human authentication and recognition*. CRC Press: Boca Raton, Florida, USA, 2013.
83. Bodade RM, Talbar SN. *Iris Analysis for Biometric Recognition Systems*. Springer, 2014.
84. Nageshkumar M, Mahesh P, Swamy MS. An efficient secure multimodal biometric fusion using palmprint and face image. arXiv preprint arXiv:0909.2373, 2009.
85. Chong LG, Kiong LC, Letchumanan C. Two-Factor Face Authentication: Topographic Independent Component Analysis (TICA) and Multispace Random Projection (MRP). in *Soft Computing and Pattern Recognition*, *2009*. *SOCPAR'09*. *International Conference of*. 2009. IEEE.
86. Khaw P. Sala de Lectura de Seguridad de la Información. In *Iris recognition technology for improved authentication*. SANS Institute: Swansea, UK, 2002; 1–17.
87. Sufi F, Khalil I, Hu J. ECG-based authentication. In *Handbook of Information and Communication Security*. Springer: Berlin, Germany, 2010; 309–331.
88. Okoh E. Biometrics Solutions in e-Health Security. 2015.
89. Karâa WBA. *Biomedical Image Analysis and Mining Techniques for Improved Health Outcomes*. IGI Global: Hershey, Pennsylvania, USA, 2015.
90. Poon CC, Zhang Y-T, Bao S-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *Communications Magazine, IEEE* 2006; **44**(4): 73–81.
91. Rostami M, Juels A, Koushanfar F. Heart-to-heart (H2H): authentication for implanted medical devices. in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. ACM.
92. Ramli SN, Ahmad R, Abdollah MF, Dutkiewicz E. A biometric-based security for data authentication in Wireless Body Area Network (WBAN). in *Advanced Communication Technology* (*ICACT*), *2013 15th International Conference on*. 2013. IEEE.
93. Wang W, *et al.* Secure stochastic ECG signals based on gaussian mixture model for-healthcare systems. *Systems Journal, IEEE* 2011; **5**(4): 564–573.
94. Thotahewa KMS, Redouté J-M, Yuce MR. *Ultra Wideband Wireless Body Area Networks*. Springer: Zug, Switzerland, 2014.
95. Sujatha S, Govindaraju R. A secure crypto based ECG data communication using modified SPHIT and modified quasigroup encryption. *International Journal of Computer Applications* 2013; **78**(6): 27–33.
96. Yao L, Liu B, Yao K, Wu G, Wang J. *An ECG-Based Signal Key Establishment Protocol in Body Area Networks*. in *Ubiquitous Intelligence* & *Computing and 7th International Conference on Autonomic* & *Trusted Computing* (*UIC/ATC*), *2010 7th International Conference on*. 2010. IEEE.
97. Abina P, Dhivyakala K, Suganya L, Praveena SM. Biometric Authentication System for Body Area Network.
98. Wang H, Fang H, Xing L, Chen M. An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks (wban). in *Communications* (*ICC*), *2011 IEEE International Conference on*. 2011. IEEE.
99. Zhang Z, Wang H, Vasilakos AV, Fang H. ECG-cryptography and authentication in body area networks. *Information Technology in Biomedicine, IEEE Transactions on* 2012; **16**(6): 1070–1078.
100. Sangari AS, Manickam JML. LIGHT WEIGHT SECURITY AND AUTHENTICATION IN WIRELESS BODY AREA NETWORK.
101. Kuroda M, Tamura Y, Kohno R, Tochikubo O. *Empirical evaluation of zero-admin authentication for vital sensors in body area networks*. in *Engineering in Medicine and Biology Society*, *2008*. *EMBS 2008*. *30th Annual International Conference of the IEEE*. 2008. IEEE.
102. Kanjee MR, Liu H. A generic authentication protocol for wireless body area networks. in *Proceedings of the 8th International Conference on Body Area Networks*. 2013. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
103. Zhang Z, Wang H, Vasilakos AV, Fang H. Channel information based cryptography and authentication in wireless body area networks. in *Proceedings of the 8th International Conference on Body Area Networks*. 2013. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
104. Javali C, Revadigar G, Libman L, Jha S. SeAK: Secure Authentication and Key Generation Protocol Based on Dual Antennas for Wireless Body Area Networks. In *Radio Frequency Identification: Security and Privacy Issues*. Springer: Oxford, UK, 2014; 74–89.
105. Wu Y, Wang K, Sun Y, Ji Y. R2NA: received signal strength (RSS) ratio-based node authentication for body area network. *Sensors* 2013; **13**(12): 16512–16532.
106. Shi L, Yuan J, Yu S, Li M. ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks. in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. 2013. ACM.
107. Schneider FB. *Trust in cyberspace*. National Academies Press: Washington, D.C., USA, 1999.