Egyptian Informatics Journal 18 (2017) 113–122

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Review

Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications

Samaher Al-Janabi [a], Ibrahim Al-Shourbaji [b,*], Mohammad Shojafar [c], Shahaboddin Shamshirband [d]

[a] Department of Computer Science, Faculty of Science for Women, University of Babylon, Iraq
[b] Computer Network Department, Computer Science and Information System College, Jazan University, 82822-6649 Jazan, Saudi Arabia
[c] Department of Information Engineering, Electronics and Telecommunications (DIET), Sapienza University of Rome, Via Eudossiana 18, 00184 Rome, Italy
[d] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 16 July 2016
Revised 10 September 2016
Accepted 1 November 2016
Available online 16 November 2016

Keywords:
Wireless Body Area Network (WBAN)
Security
Privacy
Threats
Attacks
Healthcare systems

ABSTRACT

Wireless Body Area Network (WBAN) is a new trend in the technology that provides remote mechanism to monitor and collect patient's health record data using wearable sensors. It is widely recognized that a high level of system security and privacy play a key role in protecting these data when being used by the healthcare professionals and during storage to ensure that patient's records are kept safe from intruder's danger. It is therefore of great interest to discuss security and privacy issues in WBANs. In this paper, we reviewed WBAN communication architecture, security and privacy requirements and security threats and the primary challenges in WBANs to these systems based on the latest standards and publications. This paper also covers the state-of-art security measures and research in WBAN. Finally, open areas for future research and enhancements are explored.

Contents

* Corresponding author.
E-mail addresses: samaher@uobabylon.edu.iq (S. Al-Janabi), alshourbajiibrahim@gmail.com (I. Al-Shourbaji), Shojafar@diet.uniroma1.it (M. Shojafar), shamshirband@um.edu.my (S. Shamshirband).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.eij.2016.11.001

1. Introduction

According to World Health Organization (WHO), Cardio Vascular Disease (CVD) is the prime cause of the deaths in the world [1]. In fact, it is estimated that the number of CVD related deaths, mainly from heart disease and heart stroke will reach up to 23.3 million by 2030. Besides this, more than 246 million people will suffer from diabetes and the rate of CVD patients or diabetics will increase, similarly, the percentage of individuals in the populace with age having more than 60 years will increase in the upcoming years. By 2025, and even without any further increase in the world population, this would betoken a profoundly and astronomically immense number of potential customers [1].

There has been a noticeable increase in the number of computer products used by an individual person, desktop, laptop, tablet, cell phone and an individual often uses more products regularly. Other products are implanted in people to monitor various bodily functions and conditions as well as the surrounding environment [2]. WBAN is a technique that used for remotely monitoring the patient's health and gathering the related information from the embodied sensors. It consists of a small wireless network that contains several small devices, i.e. sensor nodes and actuators. The sensor nodes are placed directly either on the body or under the skin of a person to compute certain body parameters such as, electro cardio gram (ECG), electroencephalogram (EEG), body movement, temperature, blood pressure, blood glucose, Plasmon Biosensor, heart rate, respiration rate levels [3]. These sensors are designed for specific purposes to meet the requirements of end-uses. For example, an EEG sensor was intended to monitor brain-electrical activity. Another example is the ECG sensor which was designed for monitoring heart activities. The IEEE 802.15.6 has suggested taxonomy for WBAN nodes according to the way they are implemented within the body and their role in the network [4]. The node can be classified based on the way they are implemented into the following:

- *Implant Node:* This type of node is planted either underneath the skin or inside the body tissue.
- *Body Surface Node:* It is either placed on the surface or 2 cm away from the human body.
- *External Node:* It is not in contact with the human body and rather a few centimetres to 5 m away from the human body.

There are three types of nodes in WBANs according to their role in the network *Coordinator:* This node acts as a gateway to the outside world, another WBAN, a trust center or an access coordinator. The PDA is the coordinator of a WBAN in which all other nodes can communicate. *End Nodes:* This type of nodes is restricted to perform their entrenched application but they do not have the capability to transmit messages to other nodes. *Relay:* These nodes

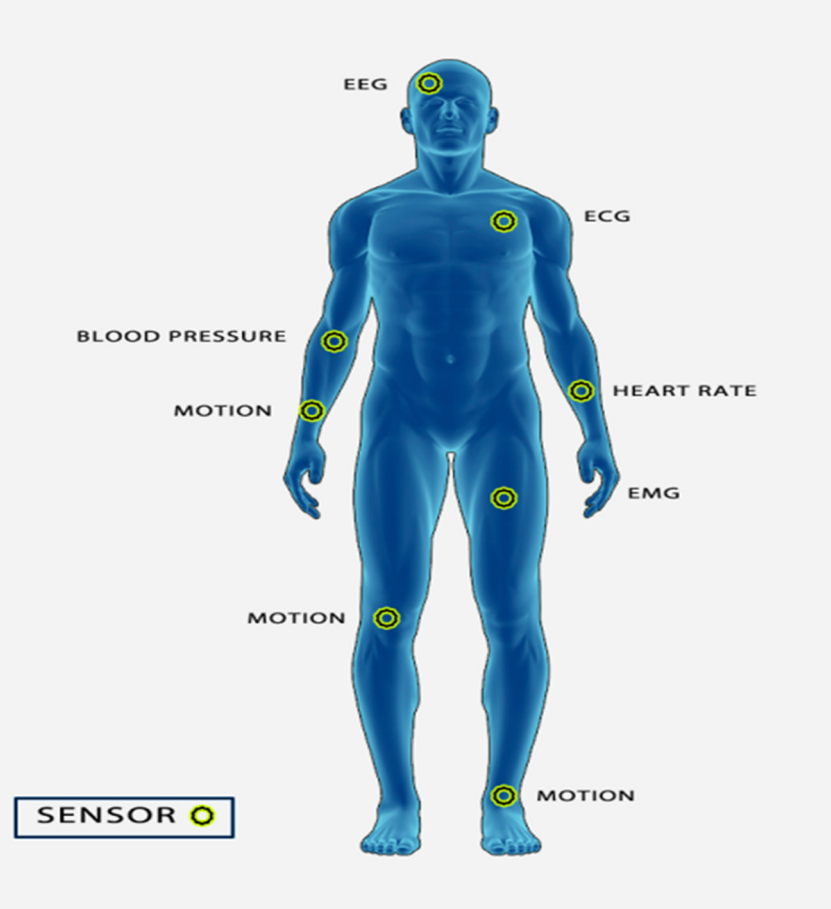

Figure 1. WBAN sensors.

represent intermediate nodes and they are called relays. The relay node consists of a parent and child nodes and relay messages. If a node is at a foot, then it is required for any data sent to be relayed by other nodes before reaching to the PDA. Also these types of nodes can sense data from other nodes.

Actuators act on the information from the sensors based on prescribed instructions. The actuator mechanism is prepared with integral reservoir and administers proper doses of hypoglycemic agent to support the glucose level measurements, For instance patients with diabetes. Fig. 1 typically shows the placement of sensors that communicate by the means of a WBAN [5]. It can be further employed in several other fields and applications such as monitoring pollution levels, physiological and medical monitoring, human computer interaction, education and entertainment [6].

A smart phone can remotely access the information sensed by the sensors or a Personal Digital Assistant (PDA) between the patient and a doctor, nurses, pharmacies who take sensitive decisions or actions depending on the information acquired from those sensors [7]. These critical decisions and medical information must be protected against unauthorized access that could be dangerous to the life of the patient and sometimes lead to death [8], i.e. change of dosage of drugs or treatment procedures, if falls on the wrong hand [9]. Thus, scalable and strict security mechanisms are mandatory and should include secure group management, confidentiality, privacy, integrity, authorization and authentication.

A wireless healthcare application offers and brings many benefits and challenges to healthcare sector. These benefits provide a convenient-environment that can monitor the daily lives and medical situations of patients at anytime, anywhere and without limitations [10,11]. On the other hand, one of the most important challenges to these new technologies in healthcare is the security and privacy issues that often makes a patient's privacy more vulnerable [12,13]. The patient's physiological vital signs are very sensitive, especially if a patient is suffering from an embarrassing disease. Such a patient could suffer humiliation at the least or even psychological upset if his or her disease information or low Quality of Service (QoS) were inadvertently communicated. Also in some instances, disease information could result to a person losing their job. Sometimes the information may make it impossible for the patient to get insurance protection.

Medical sensors sense the patient's body conditions and send messages to the doctor or the hospital server while sending of these messages, the sensors may be attacked. For instance, an adversary may capture the data from the wireless channels and modify the results [14,15]. He/She may later pass the attacked data to the doctor or the server. This could imperil the life of the patients. Given the vulnerability of patient privacy, security should be paramount when considering using technology in the healthcare setting [16].

Any patient's vital information should be stored, used and considered sensitive, but it can be especially so for patients with a socially unaccepted disease. Any failure of this type of patient's health information could lead to humiliation, wrong treatments, relationship issues, or even job loss [14,15]. Health information perceived as negative can also hinder an individual's ability to obtain health insurance coverage. Due to this, it is important to make sure that the security and privacy of these data are kept and sent securely.

The rest of the paper is organized as follows. Section 2 describes the architecture of WBAN. Section 3 introduces WBAN security and privacy requirements, security threats to WBAN. Section 4 presents the current security measures. Research in WBAN security and privacy is provided followed by discussion in Section 5. The main issues and possible open areas for research are presented in Section 6. Conclusion is provided in Section 7.

2. WBAN communication architecture

In order to understand the type of security mechanism to be deployed in a WBAN, we first need to know the structure of the communication within each of these networks as well as their communication to the outside world and with other coexisting WBANs. Therefore, in this section we provide an overview into the communication architecture in WBANs.

Fig. 2 depicts that the devices are spread throughout in a network, with the location of the device being tied to a certain application [17]. As the body continuously changes the position so the location of sensors is not fixed. Hence, WBANs, therefore, cannot be classified as a fixed network [3]. In most of the WBANs system, the communication design comprised into three separate levels as follows:

i. *Tier-1: Intra-WBAN communication*: In this level, the interaction of the sensors is confined around the body of the patient. The communication signals within the region use a

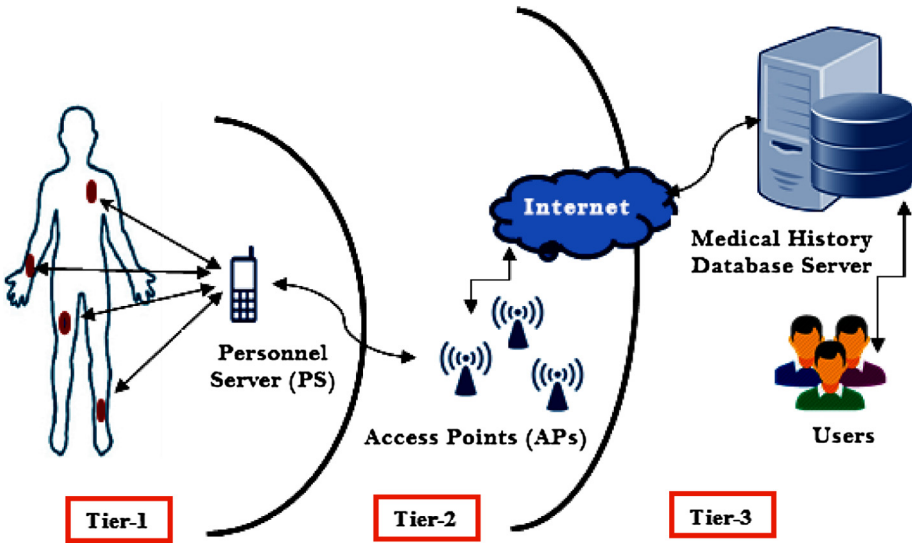

Figure 2. Communication tiers in a wireless body area network.

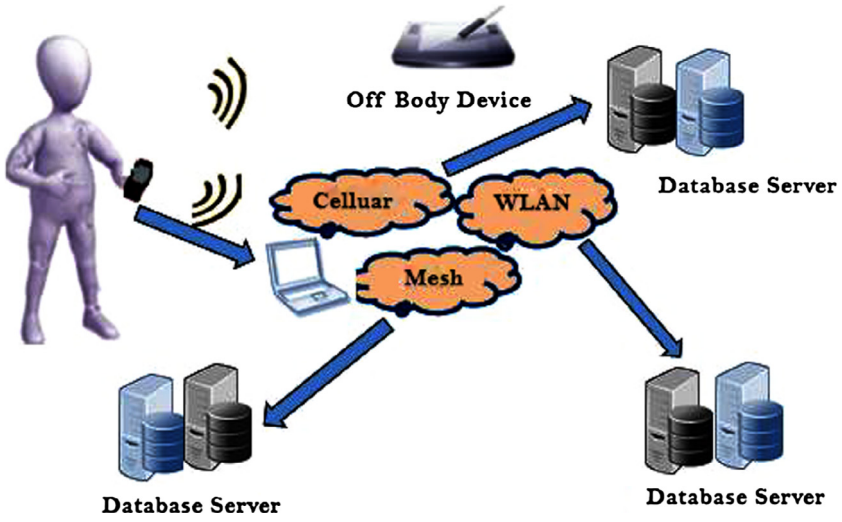

Figure 3. Infrastructure-based mode communication.

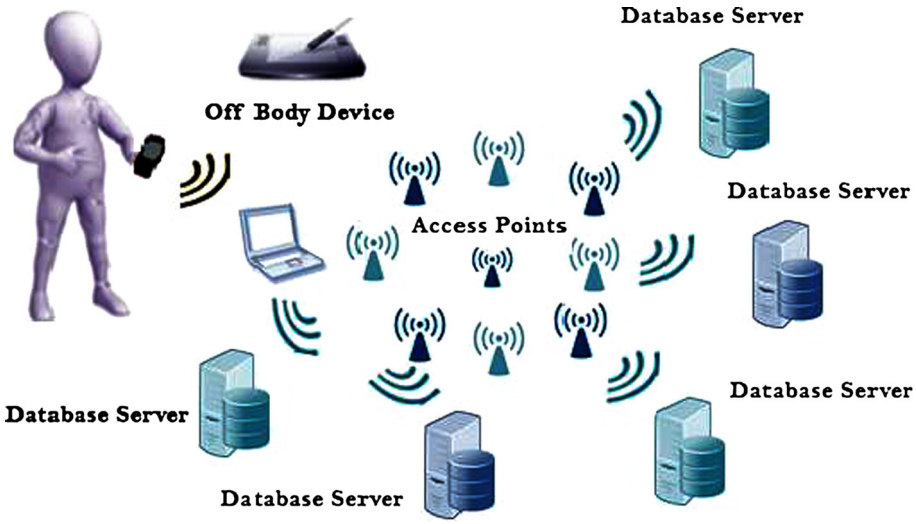

Figure 4. Ad-Hoc based mode communication.

Personnel Server (PS) that acts as a gateway, to transfer the information to the next level (i.e. access point that is present in Tier 2).

ii. Tier-2: Inter-WBAN communication: This level bridge the gap between the PS and the user via access points (APs) that are considered an important part of the network and may be positioned in a way that can allow for emergencies cases. Essentially, communication at this level strives to connect WBANs with other systems or networks so that information can be easily be retrieved through various mediums, such as the internet [14,15].

The model of inter-WBAN communication is divided into two subgroups as follows:

- Infrastructure based architecture is used in most WBAN applications as shown in Fig. 3. These applications allow for active utilization, even in a restricted space.

This type of architecture also provides better control over security and more central management since the AP can perform much like a database server relative to the application [6].

- Ad-hoc based architecture – Fig. 4 illustrates the ability for many APs to relay information in this architecture by forming a lattice that permits more flexible and quick disposition. In this way, more radio coverage can be provided through expansion and non-linear dissemination to more fully support movement. When compared to the infrastructure based coverage, the configuration of the Ad-hoc based architecture is much larger and supports the movement through larger spaces. This type of interconnection extends the coverage area from 2 to 100 m, enabling not only short, but also long term situations [6].

iii. *Tier-3: Beyond-WBAN Communication*: This level of communication is ideal for metropolitan areas, as "gateway." For example, a Smartphone can become a bridge from Tier 2 and Tier 3. "Or, from the Internet to the Medical Server (MS) in a specific application" [9]. A medical environment database is an especially crucial part of Tier 3 communication, since it accommodates the medical history and specific profile of the user. This means that the design would necessarily need to be specific to an application; medical providers and/or patients can be alerted to an emergency situation via the Internet or a through Short Message Service (SMS). Tier-3 also allows for the restoration of important

patient information that can be crucial to plan for appropriate treatment [14,15]. The PS in Tier-1 could also use GPRS/3G/4G that will directly connect it to tier 3 network, without the need of an AP, depending upon the application.

According to IEEE 802.15.6 working group, WBANs considered to work in a one or two-hop star topology with the node being placed in the center of the star technology [16]. There are two types of data transmission including (a) transmission from the device to the coordinator and (b) transmission from the coordinator to the device. There are two ways of communication in start technology: *Beacon mode* and *non-beacon mode*. In beacon mode method, the network coordinator is responsible for controlling the communication and its location in the center of the star topology. In order to allow device synchronization and network control, the network coordinator sends periodic beacons to define the start and the end of a super-frame and the length of the beacon period can be identified by both the user and WBAN's standard. Non-beacon mode represents a node in the network that is capable of sending data to the coordinator and also it uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The nodes need to power up and ask the coordinator to receive data when they only are invited to participate in a communication.

In WBANs such as very low Signal-to-Noise-Ratio (SNR) values and weakness of the body sensors in terms of memory space, energy, communication and computational ability increase the chances of security attacks and threads in WBANs [14,15]. This noise within the network channels could increase of packet loss rate. The attacker could use this vulnerability to damage WBAN network and could also block the entire system from functioning properly. Due to this, a high level of security and privacy mechanism is essential and required in WBANs.

3. Security and privacy requirements of WBANs

WBAN systems require certain security measures to guarantee security, privacy, data integrity and confidentiality of a patient's health records at all the times. A supporting WBAN infrastructure must implement specific security operations that guarantee all of these features [18]. Security and privacy of patient information are the two crucial features for within each WBAN system. Security implies data is protected from unauthorized users when being transferred, collected, processed and remains safely stored. On the other hand, privacy suggests the authority to control the gathering and usage of one's personal information. For instance, a patient may require his details to not be shared among insurance companies who could use this information to restrain his/her from the coverage. More specifically, mission-critical data within a WBAN system is extremely sensitive, that if leaked to unauthorized personnel could lead to several consequences for the patient such as losing the job, public humiliation and mental instability. Another example, when the intruders access information, through physically capturing the node and change the information; and therefore, false information will be passed to the physician that may result in a patient's death. Someone can use the individual's medical data to seek out the personal rivalries with the patient. Consequently, more attention should be given and taken to protect this sensitive and critical information from unauthorized access, use and changes [19,20]. Fig. 5 illustrates a secure mechanism of the data collection and various points of the networking including the final where the data can be retrieved by only the authorized person and through personal identification means of decryption.

The major security and privacy requirements to ensure the safety of a WBAN system and its extensive acceptance by its users are outlined as follows:

1. *Data Confidentiality*: Data confidentiality denotes the protection of a confidential data from exposure that is considered as the vital issue in a WBAN. Since WBAN nodes applied in medical situations are expected and relied upon to transmit delicate and private information about the status of a patient's well-being, hence their data must be protected from unauthorized access that could be hazardous to the patient's life [19–22]. This important, transported data can be "overheard" during transmission that can either damage the patient, the provider, or the system itself. Encryption

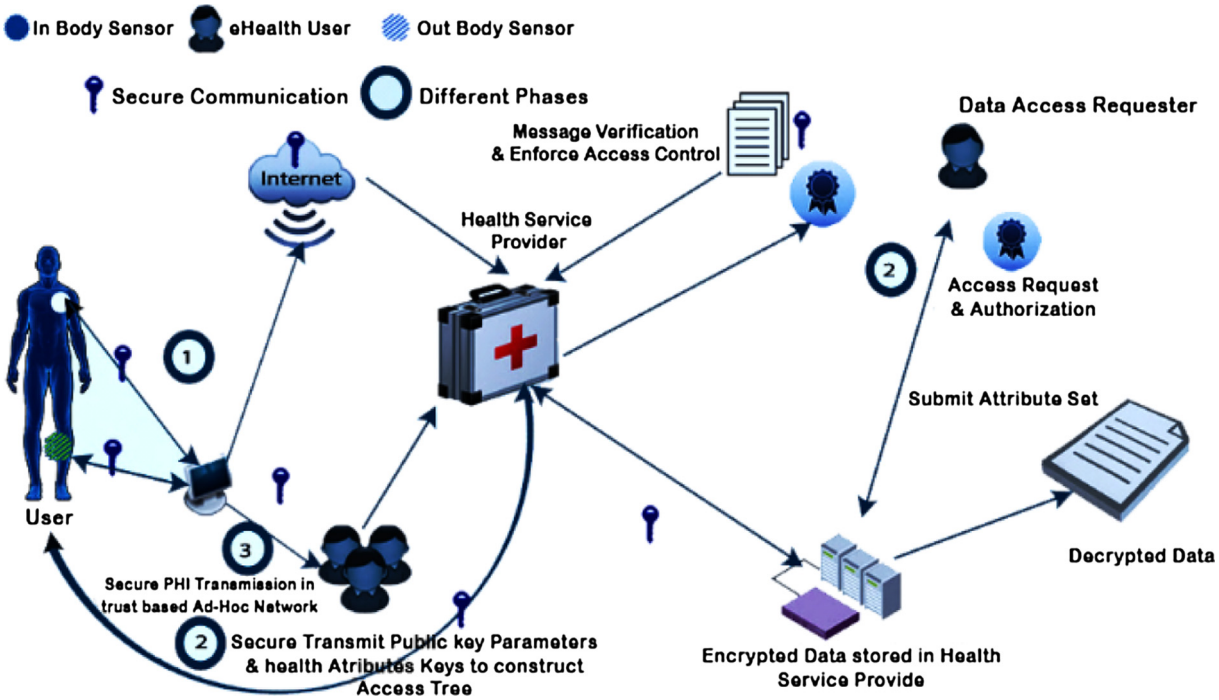

Figure 5. Security and privacy in a WBAN system.

can provide better confidentiality for this sensitive data by providing a shared key on a secured communication-channel between secured WBAN nodes and their coordinators [21].

2. *Data Integrity:* Data integrity refers to the measures taken to protect the content of a message, its accuracy and consistency. It applies to both single messages as well as streams of messages [14,15]. However, data confidentiality does not protect data from external modifications, as information can be illicitly changed when data is transmitted to an insecure WBAN as an adversary that can easily moderate the patient's information before reaching to the network coordinator. More specifically, modifications can be simply made by integrating some fragments, manipulating data within a packet, and then forwarding the packet to the PS. This interception and modification can lead to serious health concerns and even death in extreme cases. Consequently, it is imperative that the information not be accessible and altered by a potential adversary by applying authentication protocols [23].
3. *Data Freshness:* Data freshness techniques can effectively make certain that the integrity and confidentiality of data are protected from recording and replaying older data by an adversary and confuse the WBAN coordinator. It ensures that old data is not recycled and that its frames are correct. There are two types of data freshness are currently in use: *Strong freshness* promises delay in addition to frame ordering; and *weak freshness* which is limited to frame ordering, but does not provides any delay guarantees. Strong freshness is required for synchronization when a beacon is being conveyed to the WBAN coordinator and weak freshness is used for WBAN nodes with a low-duty cycle [21,24].
4. *Availability of the network*: It insinuates a medical practitioner with efficient access to a patient's information. Since such a system carries important, highly sensitive and potentially lifesaving information, it is paramount that the network is available at all the times for patients' usage in case of an emergency [14,15,18]. For this, it is essential to switch the operations to another WBAN in case of availability loss occurs.
5. *Data Authentication:* Medical and non-medical applications may require data authentication. Thus, nodes within a WBAN must be capable to verify that the information is sent from a known trust center and not an imposter. Therefore, the network and coordinator-nodes for all data calculate Message Authentication Code (MAC) by sharing an undisclosed key. Accurate calculation of a MAC code, assures the network coordinator that the message is being conducted by a trustworthy node [24,18].
6. *Secure Management:* To deliver key distribution to a WBAN, the decryption and encryption operation requires secure control by the coordinator. The coordinator role is to add and remove WBAN nodes in a secure way during node association and disassociation [24].
7. *Dependability:* The system must be reliable and dependable. A failure in retrieving the correct data represents another critical concern in WBANs as it may become a life-threatening matter for the patient [25]. In order to address this issue, error-correcting code techniques can be used [26].
8. *Secure Localization*: Most WBAN applications need correct estimation of the patient's location. Lack of tracking methods could let an attacker to transmit improper details such as, by replying with a fake signal about the patient's location [19,20,24]. Authors in [12] discussed about localization systems and their attacks.
9. *Accountability:* In the medical field, it is necessary for healthcare providers to safe guard patient health information. If a provider does not secure this information, or worse, abuses his or her responsibility for it then he or she should be made accountable for this to discourage additional abuses [3,26]. The author in [27] discussed the accountability problem and proposed a technique to defend against it.
10. *Flexibility*: The patient needs to have the flexibility of designating AP control of medical data within a WBAN. For instance, in the case of an emergency, authorization to interpret patient's data could be given on demand to a different physician who is not necessarily listed as having permission [23]. In other example, if a patient changes the hospital or a physician it should be possible to transfer the access controls.
11. *Privacy rules and compliance requirement*: The need to secure private health information is a global concern. One of the most important privacy measure is to set out rules/polices for whom have the right to access patient's sensitive data to protect the patient's privacy [28]. Several regulations and acts are enlisted in health care provisions. Currently there are different sets of regulations/polices for privacy all over the world. The American Health Insurance Portability and Accountability Act (HIPAA) is comprised of a set of directions to for doctors, healthcare providers, and hospitals and is designed to ensure that an individual's health and medical records are secure [4,14,15,28]. HIPAA outlines detailed precautions that must be taken to safe guard patient data when used for administrative or communication needs. The Act provides for both civil and criminal consequences, including a fine as much as $250,000 and/or imprisonment for 10 years if a provider shares private information for monetary gain [25].

Medical health providers are obligated under the Act to ensure that their systems and their associates pursue the following rules and guidelines [28]:

- That the system is secure and confidential and that patient's health information is secured and properly formatted.
- Provides protection against any infrequent of security, confidentiality and integrity when they occur.
- Provide protection against unauthorized access to or usage of the patient's health information. HIPPA Act additionally regulates some other critical areas like:

  - Securing patients health records, in particular from those who do not need the information.
  - Establish systems that need user identification from both consumers and medical staff.
  - Only authorized person has the right to access sensitive data and applications.
  - Ensure integrity of patient health information throughout its life cycle within the system.

The HITECH Act, or Health Information Technology for Economic and Clinical Health Act, expands on how information technology can safely be used to collect, store, share and use sensitive patient information. The Act notes that those who are custodians of patient health information must contact the person affected if a security issue arises [29]. All this is a good example of how such rules and regulations should be enacted at a larger scope if any country adopts the WBAN technology. There are special conditions, for example a disaster or medical emergency that may require the divulging of patient health information to first responders [30]. Table 1 shows the major security threats,

Table 1
Security threats and possible security solutions in WBAN.

Security threats	Security requirements	Possible security solutions
Unauthorized access	Key establishment and trust setup	Random key distribution and Public key cryptography
Message disclosure	Confidentiality and privacy	Link/network layer encryption and Access control
Message modification	Integrity and authenticity	Keyed secure hash function and Digital signature
Denial of Service (DOS)	Availability	Intrusion detection systems and redundancy
Compromised node	Resilience to node compromise	Inconsistency detection and node revocation and Tamper – proofing
Routing attacks	Secure routing	Secure routing protocols
Intrusions and malicious activities	Secure group management, Intrusion detection Systems and secure data aggregation	Secure group communication Intrusion detection systems

security requirements and the possible security solutions when using a WBAN.

3.1. WBAN security threats

WBANs are vulnerable to a huge number of attacks and threats. WBAN are frequently open to several external threats and intrusions, which could hack into the network as shown in Fig. Thus, security and privacy issues should be addressed very well, attacker may target the availability of a WBAN by capturing or incapacitating a particular node, which sometimes results in loss of a patient's life [24]. For example, the adversary can capture or incapacitate an EEG sensor and sends the false information to the physician. This could results in a hazardous life-threatening situation or even a death. An adversary can also use *jamming and tampering*. *Jamming* (radio frequency interference) can be used by an adversary on a few nodes to block the entire network [31]. This method cannot block large networks, but since WBANs are generally small networks, not only chances of network blocking are quite high, but also lead to packet loss. In fact, an adversary sometimes physically tampers WBANs. It is possible that an attacker could electronically interfere, damage, or supplant the WBAN to acquire a patient's personal health information. It can also use a flooding technique to exhaust the memory by repeatedly sending extra unnecessary packets, which the system is unable to handle. This prevents the legitimate users of the network to access the services or the resources [32]. It can be done through *Denial of Service* (DoS) attack that is meant not only to disrupt, subvert and destroy the network, but also to diminish the network's capability of providing the necessary emergency services [31,33]. Table 1 typically shows the security threats and possible security solutions that can be used in WBAN.

3.2. The current security measures

Security in WBAN is important and should not be ignored. This is sensitive medical information is sensitive and must be protected and kept same at all times from unauthorized people who may use the data that may be harmful to the individual. Several security solutions for WBAN have been proposed and they are as follows.

3.2.1. TinySec

TinySec represents as a solution to attain link layer encryption and authentication of the data in biomedical sensors networks. This technique is link-layer security architecture for WSNs and is officially part of TinyOS release. In this system, a group key is used between sensor nodes, with secure encrypted data packets and a MAC being calculated for the entire packet. It relies on a single key by default, which is manually programmed into the sensors nodes before they are deployed. This provides a minimum level of security and cannot protect against physical node capture, since it is shared [3].

3.2.2. Biometrics

This method is widely used to secure communication in biomedical sensor networks using biometrics. The method advocates employing of self-body as a way to manage cryptographic keys for sensors that are attached to the user's body. If the measuring value such as EEG is same from using two different sensors of the body, it will generate a key that can be used distribute the symmetric key securely, either encrypted or decrypted [34,35].

3.2.3. IEEE 802.15.4 and IEEE 802.15.6 security protocols

Under this system, security suites are implemented under the IEEE 802.15.4. The security suites are categorized into two essential modes: secured and unsecured mode. Unsecured mode means that no security suite has selected. The standard defines 8 unique security suites. The first one is the Null suite that gives no security, while the others are categorized according to the different security levels. A detailed description of this standard can be found in [36]. Further, in 2012, the better version, IEEE 802.15.6 standard was approved [37]. This most current standard strives to provide an international norm for reliable low power, short range wireless communication in and around a human body. It supports a wide range of rates varying from narrow band (75.9 Kbps) to ultra wide band (15.6 Mbps), depending on the need [38].

3.2.4. ZigBee security services

ZigBee came together as conglomerate of industry players to give a new meaning to ultra-low power wireless communication. The (NWK) ZigBee network layer defines supplementary security services including processes for authentication and key-exchange in addition to IEEE802.15.4. The ZigBee standard identifies a trust center of which some of the coordinator responsibilities are, to allow nodes to join the network and distribute keys [36,39].

3.2.5. Bluetooth security protocols

It comprises of various protocols such as *Baseband*, *Link Manager Protocol* (*LMP*) and *Logical Link Control and Adaptation* (*L2CAP*). The baseband enables the link between Bluetooth devices and exchange the data in form of packets. LMP is responsible for security issues like encryption, authentication, and exchanging the encryption keys. The L2CAP can support higher level of multiplexing and packets reassembly which can help in providing quality of service communication [40].

3.2.6. Wireless security protocols

Various security protocols are developed to protect the wireless network such as Wired Equivalent Privacy (WEP), Wi–Fi Protected Access (WPA) and Wi–Fi Protected Access version 2 (WPA-2). The original encryption protocols that was developed for wireless network was WEP. It was having many security flaws so WPA and WPA-2 replaced it. WPA use a pre-shared key (PSK) and a temporal key Integrity Protocol (TKIP) for data encryption. The advanced version WPA-2 uses Advanced Encryption Standard (AES) for encryption that is more secure and reliable.

3.2.7. Hardware encryption

Rather than using a software-based encryption as in TinySec, hardware encryption is implemented by use of a ChipCon 2420 ZigBee compliant RF Transceiver. The CC2420 is capable of executing IEEE 802.15.4 security operations with AES encryption by utilizing 128-bit keys. The operations utilize a counter called, CTR, mode of decryption and encryption [37].

3.2.8. Elliptic curve cryptography

This method has appeared as a feasible choice for public key cryptography in WBAN. The primary use of using Elliptic Curve Cryptography (ECC) lies in its features offering high computation, small key-size, and compact signatures. Although the energy requirements are still significant then the other contemporary system provides an alternative for high system security [41].

3.2.9. Encryption techniques

WBAN can be provided the necessary security by deigning the network to encrypt the whole data with different keys. It offers high form of security by three different mechanisms following which an effective encryption can be achieved, Symmetric key encryption, Conventional Public Key Encryption and Identity Based Encryption [42].

4. Research in WBAN security and privacy

WBANs have stringent resource constraints. Additionally, the system is challenged by a hugged and for security and privacy not to mention their practicability and usability [26]. WBAN security schemes are initially set up by symmetric cryptosystems due to shortage of resources. This system has issues with providing weak security comparatively as it is not resilient to physical compromise and delays in revealing the symmetric keys. In addition, the sensor's node primary weakness is their limited computation capacity energy, communication rate and memory space [6,43].

Much research has been conducted to study the security issues in WBANs [41,44–48]. Research conducted in Lee et al. [49] proposed encryption scheme using Elliptic Curve Cryptography (ECC) based on secure key management in healthcare systems. This scheme was divided into three main stages registration, verification and key-exchange. The findings showed that the scheme achieves more reliability and provides better security for the system. Zhao [50] proposed identity (ID) based efficient and anonymous authentication scheme for WBANs using ECC. Due to the use of ID-based concept, no certificate is required while communicating. This technique has the ability to provide mutual authentication between the client and the application provider and also provides client anonymity. The findings showed that the performance analysis of the authentication scheme is improved of 50.58% in the client side and 3.87% in the application provider side.

A common approach for securing communication in WBANs can be accomplished via the use of biometrics; the body is used to manage cryptographic keys for the nodes secured to the body itself [51]. This intends to safeguard the data security and the patient's privacy. Mana et al. [52] proposed a biometric approach using the timing information from the heartbeat, an intrinsic characteristic of the individual's body. This method is based upon symmetric technique and upon availability of a secured key distribution pattern. The findings showed that the proposed approach could be used as a way to safeguard of cipher key distribution during communication in e-health applications of WBANs. Other researchers have put forth [53], an approach that, identity information with mutual authentication from two different parts of the body. The results showed that using unique biometric features is helpful for the identification purpose.

Salem et al. [54] proposed a framework for anomaly detection in WBAN. The proposed architecture combines data mining and machine learning algorithms with modern sensor fusion techniques. It can distinguish between irregular variations and the faulty sensor data in the physiological parameters of the monitored patient. This enables the system to ensure reliable operations and real-time global monitoring from smart devices. Researchers have also examined patient's data privacy in WBAN and various techniques created to secure it from outside intrusions [55–57]. Mana et al. [52] put forth processes to ensure location privacy in WBAN. The foundation of this protocol is temporary pseudonyms, not hardware addresses being used to share information in the WBANs. Thus, both the source and destination in the WBANs are protected on mobile devices. Barua et al. [55] suggested patient-centric control (PEACE) scheme to access personal health information efficiently and securely by establishing diverse access privilege and attribute sets dependent upon who was requesting the information. This approach secures confidentiality and integrity by using pseudo-identity and digital signature methods. Their findings indicate that the approach provides a much needed security requirement.

5. Discussion and recommendations

WBANs have proven to be a great asset in the medical healthcare practice. However, for any health application security and privacy issues must be resolved fast enough to avert a disaster in the society. To deal with the major security threats, two broad levels of security measures of encryption and authentication should be applied [18]. Any information about personal health coming from the system must be encrypted at all times. The fore mentioned attacks can be prevented by unauthorized modification of data meanwhile ensuring only legitimate devices can insert or create data for the network. Authentication methods can be useful in determining the origin of data whether it is from the person that he/she is claiming to become from. In WBAN systems, where patients wear various devices, a centralized control device for the transmission of data in and out of the network can be helpful. A centralized device can behave a gateway or block between internal and external communication on the network. Firewalls, authentication, routers and other types of safeguards can be used as security measures and to monitor the network traffic [58,59], Users should be authorized to use the WBAN system and be able to control and maintain their own important health information.

Aside from sensors design concerns should be focused on designing sensors with Low cost, and size. Most importantly, they should transmit data to several meters. In addition to this, each sensor signal has a different frequency (i.e., not uniform), and therefore, not only each sensor should be optimized according to the frequency band of its sensor, but also, each sensor needs to support different applications with different requirements in frequency, data rate, power-usage and reliability to meet end-users demands and requirements.

In order to meet the satisfaction of the feasibility in Elliptic Curve Cryptography (ECC) of WBAN, it is essential to investigate the implementation of Okamoto's identification protocol that is described in [60]. Moreover, using RFID tags over sensors of the body in order to cope with the feasibility situation of the problems have been investigated in several practical scenarios in [61–63].

Another method that is still at the proposal stage to prevent intrusion is the application of Intrusion Detection Systems (IDS). This method is simulated by the biological immune system that uses a Negative Selection Algorithm (NSA). This application enhances the performance of a WBAN to operate despite the presence of a compromised node [64]. Intrusions detection in WBANs poses a challenging problem, specifically when proactive defense

mechanisms need to preempt attacks. Digital forensics is the process of investigating to identify, trace and analyze illegal and fraudulent occurrences and provide proof to enforce laws against such events. Intrusion Detection and Prevention Systems (IDPS) can be used to provide the information needed to identify suspicious early activities and may even lead to prevention of more serious damage. Thus, an IDPS can be considered as a useful tool for collecting digital evidences that may be used in a court and law also IDPS can early detection of malicious activities, and therefore, the systems activities can be easily monitored and can test the effectiveness of the control environment by identifying polices and attributes that break security and privacy. In a border context, WBAN has to encompass all safety measurements comprising security, privacy, trust, and digital forensics to embrace the legal and social demands [65].

Another important security and privacy measure is to create awareness in the public about WBAN's security and privacy. This is because some end-users do not have any understanding of this type of technology and its use and consequences; therefore may not possess enough knowledge or understanding to make judicious decisions in terms of protecting their own desired level of privacy [66]. It will also require actual and non-actual regulatory and standards bodies, governments, industry and service providers to address the safety measures' issues to synthesize legislations, directives and guidelines for WBAN applications as part of a comprehensive deployment strategy.

6. Issues and open areas for research

Discussion of the security issues related to WBAN clearly demonstrates the needs of further research in this area even though a lot of research is currently going on and some open issue exist. In fact, security, privacy and Quality of Service (QoS) need to be assessed [67,68]. Most studies have focused on security alone as an individual topic, whereas QoS and security along with privacy are a better platform for healthcare applications using WSN. In home care applications, sensory devices send the data to the central device outside their immediate radio range [69]. Message forwarding and routing, therefore, are critical to end-to-end communication and while various approaches to routing have been suggested for sensor networks, none possess strong security measures.

DoS or DDoS attacks are often cited as being at the root of security vulnerabilities in a routing protocol [31,70]. Malicious information can also be inserted into the network via the router. Furthermore, current proposals are mainly designed for the static wireless sensor networks whilst mobility within the network. The mobility of WBANs with respect to each other need to be encountered in WBAN-specific routing protocols [69]. In addition, the need for integrating WBANs with mobile phones for m-Health applications requires further research involving development of dedicated software and applications [71].

Another area of research that needs attention and focus is area of trust management. Trust is the degree to which a node may be considered worthy of trust, reliable and secure while interacting with other nodes. In order for trust to exist, there must be a mutual association of any two trusted nodes. These can be data aggregator or sensor nodes. There must be dependable, distributed cooperation between network nodes for a wireless healthcare application to operate properly [6]. For healthcare applications, trust is evaluated based on the quality, the data delivery and behavior of the nodes [7]. Therefore, trust management systems are useful in detecting degree of trust of a node. Even though trust for mobile healthcare systems has been evaluated, trust management must take place in a real time setting so that all parties can be ensured of the trustworthiness. With such measurements, a WBAN will be trusted both by its patients and by service providers as a tamper proof and efficient system.

The patient's medical information can be accessed by different parities including doctors, nurses, pharmacies and insurance companies who not only can take sensitive decisions, but also have different privilege to access those sensitive data. In the light of this, a high level of consistent policy sets is needed to protect the patient's privacy.

7. Conclusion

Wearable computing employing sensor devices become an integral part in our daily life and activities. Today, people often have implanted sensor devices in their body to provide an enhanced and improved quality of life. This is a tremendous advancement where ICT is contributing to maintain a normal human lifestyle, especially with the deployment of WBANs for providing the convenience. This work reviewed the deployment of WBANs in terms of security and privacy. It has also dealt with WBAN communication architecture, the security and privacy in WBAN and the threats to the integration of sensors and actuators as well as attacks to WBANs. The WBAN current security measures and research in WBAN with regards security and privacy have been discussed along with issues and open areas of researching in the areas have been outlined. The growing interest in these networks dominantly aroused the issues of security and privacy in these networks; the legal problems need to be addressed within a legal framework. This implies that the framework provides for the other substantive safety measures such as trust, audit, digital forensics and IDPS to guarantee compliance within the law and ethical behavior by healthcare workers and system operators who have the access to patient records and information. These implications require the public and health care personnel to be aware of the challenges that come along with WBAN usage to ensure that the application in delivering patient's healthcare is secured at all levels.

References

[1] Mathers CD, Loncar D. Updated projections of global mortality and burden of disease, 2002–2030: data sources, methods and results. PLos Med (World Health Org) 2006:1–8.

[2] Wang J, Zhang Z, Yang X, Zuo L, Kim JU. Data security and privacy of e-healthcare in electronic medical environment. ASTL SIA 2013;22:92–8.

[3] Sharma DA. Wireless health care monitoring system with data security and privacy. Int J Res Comput Eng Electron 2013;2(2).

[4] Yazdandoost KY, Sayrafian-Pour K. Channel model for body area network (BAN). IEEE P802, 15, 08-0780; 2009. <http://math.nist.gov/mcsd/savg/papers/15-08-0780-09-0006-tg6-channel-model.pdf> [accessed 6.9.16].

[5] Naranjo PG, Shojafar M, Mostafaei H, Pooranian Z, Baccarelli E. P-SEP: a prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks. J Supercomput 2016;1–23.

[6] Rocker C, Ziefle M. E-health, assistive technologies and applications for assisted living: challenges and solutions. Med Inform Sci Ref 2011:23–48.

[7] Fragopoulos AG, Gialelis J, Serpanos D. Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures. In: 12th IEEE international conference on E-health networking applications and services (Healthcom). p. 127–34.

[8] Wang J, Zhang Z, Xu K, Yin Y, Guo P. A research on security and privacy issues for patient related data in medical organization system. Int J Security Appl 2013;7(4):287–98.

[9] Crosby GV, Ghosh T, Murimi R, Chin CA. Wireless body area networks for healthcare: a survey. Int J Ad Hoc, Sensor Ubiquitous Comput 2012;3(3):1–26.

[10] Siddiqui MA, Kamal MB, Moinuddin H. Towards the development of cross layer approach for energy efficiency and mobile wireless body area networks. Int J Comput Inform Technol 2013:542–7.

[11] Rocker C, Ziefle M. E-health, assistive technologies and applications for assisted living: challenges and solutions. Med Inform Sci Ref 2011;392. ISBN13: 9781609604691.

[12] Rehman OU, Javaid N, Bibi A, Khan ZA. Performance study of localization techniques in wireless body area sensor networks. In: 11th IEEE international conference on trust, security and privacy in computing and communications. p. 1968–75.

[13] Pathania S, Bilandi N. Security issues in wireless body area network. Int J Comput Sci Mobile Comput 2014;3(4):1171–8.
[14] Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wirel Commun 2010;17(1):51–8.
[15] Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 2012;36(1):93–101.
[16] Tachtatzis C, Di Franco F, Tracey DC, Timmons NF, Morrison J. An energy analysis of IEEE 802.15. 6 scheduled access modes for medical applications. In: International conference on Ad Hoc networks. Berlin Heidelberg: Springer; 2011. p. 209–22.
[17] Latré B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks. Wireless Netw 2011;17(1):1–8.
[18] Kumar R, Mukesh R. State of the art: security in wireless body area networks. Int J Comput Sci Eng Technol (IJCSET) 2013;4(5):622–30.
[19] Kargar MJ, Ghasemi S, Rahimi O. Wireless body area network: from electronic health security perspective. Int J Reliable Quality E-Healthcare (IJRQEH) 2013;2(4):38–47.
[20] Ferdous MS, Chowdhury F, Moniruzzaman M. A taxonomy of attack methods on peer-to-peer network. In: In the proceedings of the 1st Indian conference on computational intelligence and information security. ICCIIS; 2007. p. 132–8.
[21] Han ND, Han L, Tuan DM, In HP, Jo M. A scheme for data confidentiality in cloud-assisted wireless body area networks. Inf Sci 2014;284:157–66.
[22] Tewari A, Verma P. Security and privacy in E-healthcare monitoring with WBAN: a critical review. Int J Comput Appl 2016;136(11).
[23] Fatema N, Brad R. Security requirements, counterattacks and projects in healthcare applications using WSNs – a review. Int J Comput Network Commun (IJCNAC) 2014;2(2).
[24] Kavitha T, Sridharan D. Security vulnerabilities in wireless sensor networks: a survey. J Inf Assurance Sec 2010;5(1):31–44.
[25] Somasundaram M, Sivakumar R. Security in wireless body area networks: a survey. In: International conference on advancements in information technology ICBMG, IPCSIT, Singapore. p. 20.
[26] Li J, Ren K, Zhu B, Wan Z. Privacy-aware attribute-based encryption with user accountability. In: International conference on information security. Berlin Heidelberg: Springer; 2009. p. 347–62.
[27] Javadi SS, Razzaque MA. Security and privacy in wireless body area networks for health care applications. In: Wireless networks and security. Berlin Heidelberg: Springer; 2013. p. 165–87.
[28] Office for Civil Rights, United State Department of Health and Human Services. Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html> [accessed 20.12.15].
[29] Health Information Technology for Economic and Clinical Health Act HITECH. Ways And Means and Science Technology <http://waysandmeans.house.gov/media/pdf/110/hit2.pdf> [accessed 10.11.15].
[30] Kim KJ, Hong SP. Privacy care architecture in wireless sensor networks. Int J Distrib Sens Netw 2013:1–8.
[31] Ullah S, Higgins H, Braem B, Latre B, Blondia C, Moerman I, Saleem S, Rahman Z, Kwak KS. A comprehensive survey of wireless body area networks. J Med Syst 2012;36(3):1065–94.
[32] Latif R, Abbas H, Assar S. Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review. J Med Syst 2014;38(11):1.
[33] Kifayat K, Merabti M, Shi Q, Llewellyn-Jones D. Security in wireless sensor networks. In: Handbook of information and communication security. Berlin Heidelberg: Springer; 2010. p. 513–52.
[34] Ramli SN, Ahmad R, Abdollah MF, Dutkiewicz E. A biometric-based security for data authentication in wireless body area network (wban). In: In the 15th international conference on advanced communication technology (ICACT). p. 998–1001.
[35] Zhang GH, Poon CC, Li Y, Zhang YT. A biometric method to secure telemedicine systems. In: Annual international conference of the IEEE engineering in medicine and biology society. p. 701–4.
[36] Saleem S, Ullah S, Kwak KS. A study of IEEE 802.15.4 security framework for wireless body area networks. Sensors 2011;11(2):1383–95.
[37] Crosby GV, Ghosh T, Murimi R, Chin CA. Wireless body area networks for healthcare: a survey. In J Ad Hoc, Sensor Ubiquitous Comput 2012;3(3):1.
[38] Ullah S, Mohaisen M, Alnuem MA. A review of IEEE 802.15.6 MAC, PHY, and security specifications. Int J Distrib Sens Netw 2013:24.
[39] Misic J. Enforcing patient privacy in healthcare WSNs using ECC implemented on 802.15. 4 beacon enabled clusters. In: 2008 Sixth annual IEEE international conference on pervasive computing and communications (PerCom), Hong Kong; 2008. p. 686–91.
[40] Ahmadi A, Shojafar M, Hajeforosh SF, Dehghan M, Singhal M. An efficient routing algorithm to preserve k-coverage in wireless sensor networks. J Supercomput 2014;68(2):599–623.
[41] Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J Med Syst 2014;38(2):1–7.
[42] Ali SH. Novel approach for generating the key of stream cipher system using random forest data mining algorithm. In: In the sixth of IEEE international conference on developments in eSystemsEngineering (DeSE). p. 259–69.
[43] Tian Y, Peng Y, Peng X, Li H. An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks. Int J Distrib Sens Netw 2014;11:2014.
[44] Liu J, Zhang Z, Sun R, Kwak KS. An efficient certificateless remote anonymous authentication scheme for wireless body area networks. In: IEEE international conference on communications (ICC). p. 3404–8.
[45] Lee YS, Alasaarela E, Lee H. Efficient Encryption Scheme based on Elliptic Curve Cryptography (ECC) and Symmetric algorithm in Wireless Body Area Networks (WBANs); 2013. p. 36–9.
[46] Kovačević T, Perković T, Čagalj M. LIRA: a new key deployment scheme for wireless body area networks. In: IEEE international conference on software telecommunications and computer networks (SoftCOM). p. 1–6.
[47] Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inf Forensics Secur 2014:2327–39.
[48] Liang X, Barua M, Lu R, Lin X, Shen XS. HealthShare: achieving secure and privacy-preserving health information sharing through health social networks. Comput Commun 2012;35(15):1910–20.
[49] Lee YS, Alasaarela E, Lee H. Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system. In: The IEEE international conference on information networking 2014 (ICOIN2014); 2014. p. 453-7.
[50] Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J Med Syst 2014;38(2):1–7. 1.
[51] Zhou J, Cao Z, Dong X, Xiong N, Vasilakos AV. 4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf Sci 2015;314:255–76.
[52] Mana M, Feham M, Bensaber BA. Trust key management scheme for wireless body area networks. IJ Network Security 2011;12(2):75–83.
[53] 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: IEEE international conference on communications (ICC). p. 1–5.
[54] Salem O, Guerassimov A, Mehaoua A, Marcus A, Furht B. Anomaly detection in medical wireless sensor networks using SVM and linear regression models. Int J E-Health Med Commun (IJEHMC) 2014;5(1):20–45.
[55] Barua M, Liang X, Lu R, Shen X. PEACE: an efficient and secure patient-centric access control scheme for eHealth care system. In: IEEE conference on computer communications workshops (INFOCOM WKSHPS). p. 970–5.
[56] Sun J, Zhu X, Fang Y. Preserving privacy in emergency response based on wireless body sensor networks. In: IEEE conference on global telecommunications (GLOBECOM). p. 1–6.
[57] Saleem S, Ullah S, Kwak KS. Towards security issues and solutions in wireless body area networks. In: The 6th IEEE international conference on networked computing (INC). p. 1–4.
[58] Bruce N, Jang WT, Lee HJ. An embedded encryption protocol for healthcare networks security. Network 2014;2:5.
[59] Jang CS, Lee DG, Han JW, Park JH. Hybrid security protocol for wireless body area networks. Wireless Commun Mobile Comput 2011;11(2):277–88.
[60] Arbit A, Livne Y, Oren Y, Wool A. Implementing public-key cryptography on passive RFID tags is practical. Int J Inf Secur 2015;14(1):85–99.
[61] Wheeler DJ, Needham RM. TEA, a tiny encryption algorithm. In: International workshop on fast software encryption. Berlin Heidelberg: Springer; 1994. p. 363–6.
[62] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. SPINS: security protocols for sensor networks. Wireless Netw 2002;8(5):521–34.
[63] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. PRESENT: an ultra-lightweight block cipher. In: International workshop on cryptographic hardware and embedded systems. Berlin Heidelberg: Springer; 2007. p. 50–466.
[64] Sundararajan TV, Shanmugam A. A novel intrusion detection system for wireless body area network in health care monitoring. J Comput Sci 2010;6(11):1355.
[65] Rahman AF, Ahmad R, Ramli SN. Forensics readiness for wireless body area network (WBAN) system. In: The 16th IEEE international conference on advanced communication technology. p. 177–80.
[66] Al-Janabi S, Al-Shourbaji I. A study of cyber security awareness in educational environment in the middle east. J Inform Knowledge Manage 2016;15(01):1650007.
[67] Maskooki A, Soh CB, Gunawan E, Low KS. Opportunistic routing for body area network. In: IEEE conference on consumer communications and networking (CCNC). p. 237–41.
[68] Movassaghi S, Abolhasan M, Lipman J, Smith D, Jamalipour A. Wireless body area networks: a survey. IEEE Commun Surveys Tutorials 2014;16(3):1658–86.
[69] Li M, Yu S, Guttman JD, Lou W, Ren K. Secure ad hoc trust initialization and key management in wireless body area networks. ACM Trans Sensor Networks (TOSN) 2013;9(2):18.
[70] Shrivastava G, Sharma K, Rai S. The detection & defense of DoS&DDos attack: a technical overview. In: Proceeding of ICC, vol. 27; 2010. p. 28.
[71] Wang H, Zhang Z, Lin X, Fang H. Socialized WBANs in mobile sensing environments. IEEE Network 2014;5:91–5.