EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Secure new node ID assignment for internet integrated wireless body area networks

Amit Kumar Gautam[1]* and Rakesh Kumar[1]

[1]Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, India

Abstract

Internet integrated sensor networks have gained much importance and exponential growth in wireless body area networks (WBAN) over the last few years. These networks are used in health services to remotely monitor the health of patients and send/receive sensitive, time critical medical data. Because of the wireless and broadcast nature of WBAN, it is easy for an adversary to get, inject, or update the information transmitted in the medium or launch many security attacks. To protect the sensitive data of the patient, we propose a secure communication strategy for different sensors to form a WBAN. Here, a new node ID is assigned for sensors by using public key cryptography to communicate in the network. An energy utilization and communication cost analysis show that our approach incurs less communication overhead as compared with the recently proposed secure solutions in WBAN. The complexity analysis show that the proposed model works efficiently for secure communication in WBAN.

Keywords: Healthcare, Body area networks (WBANs), Security, New node joining, Cryptography

Received on 16 March 2020, accepted on 06 May 2020, published on 13 May 2020

doi: 10.4108/eai.13-7-2018.164554

*Corresponding author. gautam.biet@gmail.com

1. Introduction

The sensor network continuously provide services to various life changing application such as healthcare, agriculture, nuclear power plant monitoring, water monitoring, air pollution monitoring, weather prediction monitoring and earth sensing monitoring. As the critical applications adopt sensor network and tools, information must be protected, authenticated and secure [1].

One aspect of upcoming Internet is that everything having sensors and actuators have linked and incorporated in a bundle called Internet of Things (IoTs) [2]. Wireless Body Area Networks (WBAN) having sensors attached with the human body and an environment (such as rooms, operation table etc.) and forming WBAN have sensing, transmitting and processing capabilities and are integrated with Internet for immediate and fast healthcare services [3]. Due to security threats, data transferred from sensors should be shielded by an end-to-end (E2E) secured channel between the sensors and any communication object from the world. The establishment of secure channel needs to be authenticated. A strong key management schemes can permit two communication devices mutually authenticated and negotiated with secure keys which are used to protect the data from internal and external security attacks [4].

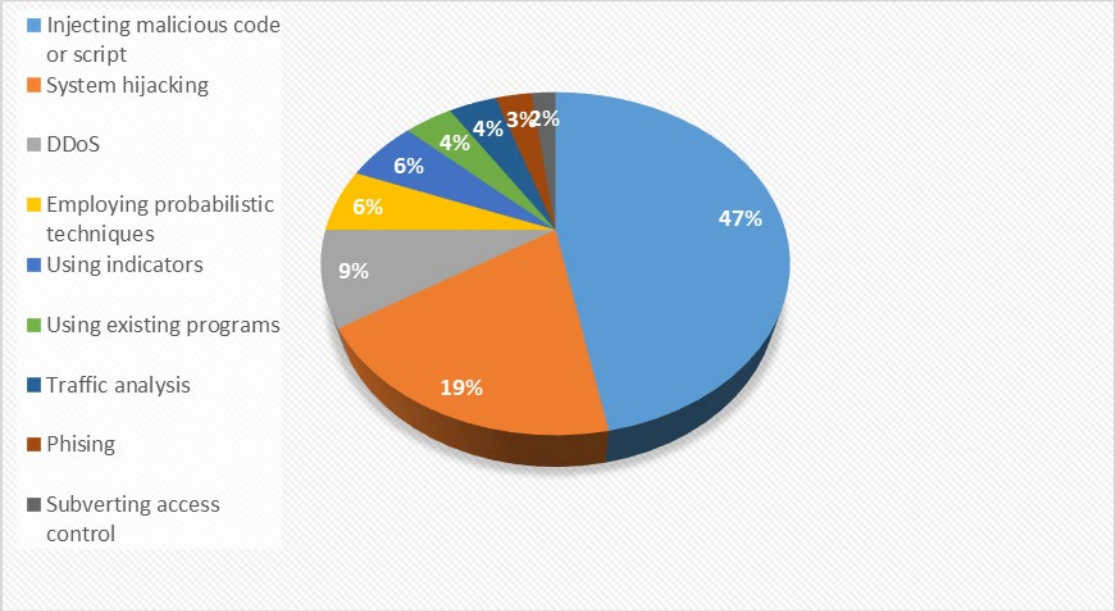

Figure 1. Data analysis of various security attacks on WBAN

In the healthcare industry, various types of data such as electronic medical records, patient identification, biomedical information, patient accounts and doctor prescriptions are present. These records must be confidential and generated from an authenticated source. The security solutions must adopt the new techniques and methods to provide security against intruders, sniffers, malevolent devices, hackers, ransomwares and most importantly human errors. Initially, human errors are not include as a threat for network. But in today's scenarios there are special provision for handling human errors in its security design. The risk attached with healthcare network can cause abdominal changes in reports of patient, mistreatment by doctors, breaching the account of patient, loss of human life and degradation of reputation service providers. Some common network related threats are as follows [5-8].

- **Packet Sniffers:** The malicious users or hackers can analyse the captured message by any legitimate management tool. They can sniff the user id and passwords and uses against the patient or healthcare management.
- **IP Spoofing:** This type of attacks occurs when a malicious user from inside or outside the network can mimics aa a trusted communication device to get access of network information.
- **Data modification:** The malicious user can modify, delete, add and replace confidential and sensitive data and replace with any malicious script on server. As the health data changed, it may result disaster for a person.
- **Denial of Service (DoS):** The services can be prohibited by malicious user through malicious program or script. This is most widely publicized form of attack which causes exhausting resources, blocked processes and services of operating system or applications.
- **Eavesdropping:** Due to broadcast nature of wireless channel, any malicious user can interrupt the radio transmissions among sensor nodes. The stolen data can be used to harm the healthcare users or network.
- **Node Capture:** Resilience against node capture attack is major threat which poses by any adversary in wireless sensor network. In real time WBAN the medical sensors are placed on body and an environment (such as rooms, operation table etc.). So, these sensors are easily accessible by any adversaries. By capturing the node they can access the cryptographic information and posses to big threats for WBAN [9-10] .

The motivation, contribution and organization of the proposed work are as follows.

The healthcare services through internet can offer various facility for patient and medical service providers. It can also invite many attackers and malicious activities to harm the healthcare networks. According to the report published [11] by IBM the hackers and cybercriminals can produce various type of attacks in recent years. According to the data analysis, various security attacks are identified, and their share are depicted in Figure 1. Most of the attacks called injection of malicious code or script which are 47 percent from total attacks can affect healthcare organizations. Other type of security attacks which are affected healthcare network are mainly system hijacking, passive attackers, traffic analysis, Distributed deniel of service (DDoS), phishing and many more. Figure 1 depicted the percentage of various security attacks on WBAN. This data analysis also suggest that organizations must take back up of their data and keep identifying internal threats [11]. The new node might come with new threat and needs to identify that threat to secure the network. WBAN have heterogeneity, domain information, heavy and complex protocol are key challenges to produce a secure solution.

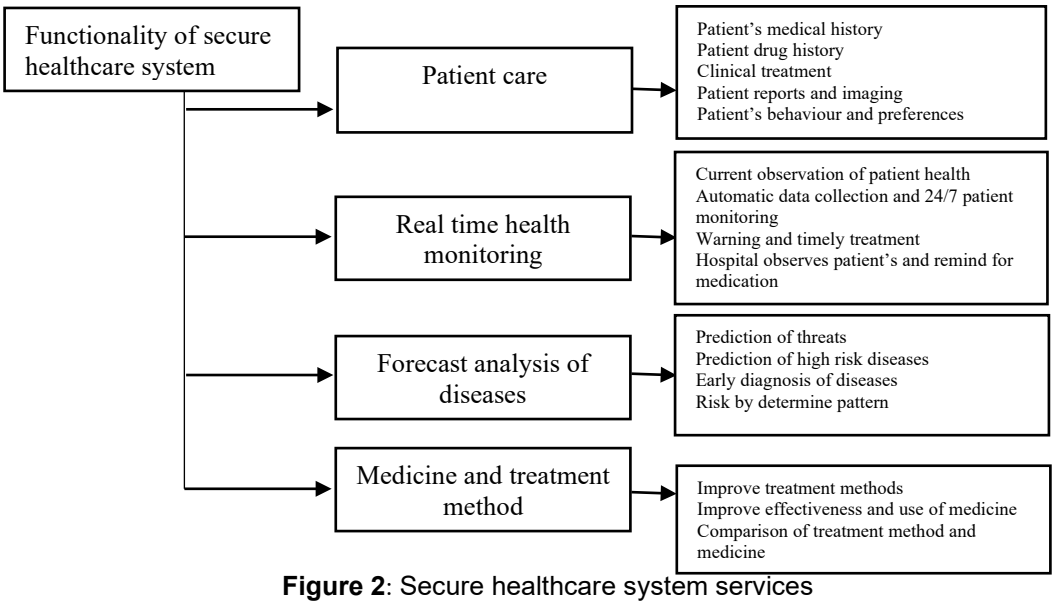

Figure 2: Secure healthcare system services

The major contributions of the paper are as follows:

- The existing security method of WBAN have studied and given their significant characteristics, advantages and disadvantages in a Table 1.
- Design and proposed a new security approach for new node joining in WBAN with the help of access node.
- We present a design requirement analysis, energy utilization and computation cost analysis to prove privacy and security properties of security of WBAN.
- Proposed scheme give cryptographic approach to make sure authenticity, confidentiality and integrity of new node joining in WBAN.

The other part of this paper is systematized as follows. Section 2 presented the background. Section 3 gives system model, adversary model, and design requirements. Section 4 gives a related work and summarize the various recent articles proposed for node joining schemes. Section 5 explains the proposed approaches with schematic analysis. In section 6 various security analysis had given. In section 7 conclusion and future scope has explained.

2. Background

This section explained the effects of poor security measures. Here we also explained the various security and privacy requirements to provide security of WBAN. The basic structure of WBAN are also presents in this section.

2.1. Cost of poor security network

The poor security measures is threatable for loss of important, private, sensible data of patient and healthcare staff. It is also causing loss of patient confidence towards healthcare organization and doctors. In worst case scenario, uncoverable damages can happen due to loss or altered patient information and it can causes sometimes death. The other effects of poor security is as follows.

- High network congestion and busy server
- Loose confidence of patient toward healthcare organizations
- The recovering or financial cost is more

2.2. Benefits of secure healthcare network

Figure 2 depicted the functionality of secure healthcare system. The secure healthcare environment can protect patient data, communication channel and messages from outsider of the network. The secure healthcare environment are able to provide following benefits:

- Anytime, anywhere, anyone can take consultation from doctors and monitored by doctors.
- It can support mobility which provide by labs, tests and prescriptions.
- Easy connection of people from remote area to metro city doctors.
- Reduce cost of consultation by patients.
- Improvised the caring and safety of patients.

The following are the security and privacy requirements of WBAN [6].

- **Confidentiality:** The data confidentiality represents the security of data during transmission among healthcare devices. The data which include private information, status of patient current status, card details must protect which causes hazardous to patient's health and wealth. The confidentiality can be achieved by using encryption and key management.
- **Integrity:** The content of message of data must not change or altered during transmission among healthcare

devices. Data integrity implies to the procedures applied to secure content of data. The modification in data or

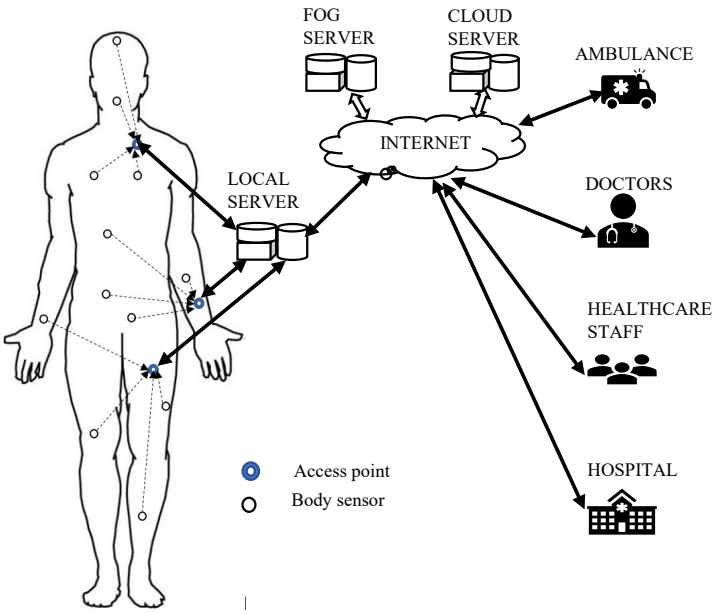

Figure 3. Wireless body area networks

messages through injection some content or modifying content of data. This can be misguided to healthcare service provider and mislead to right prescription and advice through doctors to the patient.

- **Data Freshness:** Data freshness is used to support confidentiality and integrity of data. The old data cannot be used as a new. Data freshness can achieve through monitoring delay, duty cycle, timeliness and synchronization of bits.
- **Authentication:** Every communication device in healthcare application need to be authenticated. So, the receiver of the message trust on sender device. The authentication of the node or device can achieve through cryptographic keys or encryption techniques.
- **Dependability:** The communication devices must be reliable and trustworthy. The correct data need to retrieve from these communication devices, and it fail to deliver correct data then dangerous for human life.
- **Privacy:** Privacy of the patient information is primary concern and private health information is global concern to secure healthcare environment. The access of private data and medical information should be limited, and it is given to authenticated person or devices.
- **Data availability:** Attackers may launch DoS attack on medical cloud and caused medical services inaccessible. Therefore, the WBAN must detect and survive from DoS attacks.

2.3. Overview of WBAN

A WBAN is a collection of various type of body sensors and environment sensors which monitors different activity of body functions and may communicate with each other and connected with different access points. The structure of WBAN is depicted in Figure 3 [12]. These access points work as a mediator between local servers and body sensors and environmental sensors. The body sensors are either fixed or movable. There are various types of body sensor are used to monitor physiological signal detection such as blood pressure, Electrocardiograms (ECG), temperature, heart rate and Electroencephelogram (EEG). These sensors monitor physiological signal continuously and send the data to the remote server for further analysis. The analyzed data checks by the doctors or medical specialist and prescribed medicine for the patient. So, with the help of WBAN the continuous health monitoring in timely manner and the users can access medical history or records anytime from anywhere. The emergency situation can be handled by sending alarm or messages to medical staff or ambulance during any abnormally is found by the sensors.

3. Related Work

In 1996, the concept of WBAN was firstly proposed by Zimmerman [13]. He conducted research which allows communication devices attached with human body to transfer data through near-field electrostatic coupling. Recently fog computing, cloud computing and IoT integration with healthcare together can made emerging area of research.

Mainly two types of security schemes are used in WBAN. First method is called physiological signal-based schemes [25] which uses ECG, EEG, heart rate [24], fingerprints, iris and many bio signals to generate cryptographic keys for key

management in WBAN. Second method uses cryptographic keys-based schemes [26-28] which uses elliptic curve cryptography (ECC), RSA, MD5 and many cryptographic schemes. Cherukuri et al. [12] one of the first researchers which uses the physiological signals and their feature for randomness and distinctiveness. The features of physiological signals are used to secure WBAN. Many other researchers also use the physiological signals for key management to make secure, energy efficient solution. Some other researchers also use fuzzy vault scheme, bloom filter and steganography with the physiological signals to deal with security issues in WBAN.

Xu et al. [14] proposed a method which are using XOR operation and hash function to provide mutual authentication and key management for WBAN. In this method it is using improved fuzzy vault scheme to secure generation of cryptographic keys. Using XOR operation, four hash function and fuzzy vault scheme make this method is lightweight and protect from various security attacks such as eavesdropping, impersonation, replay, capture, man in middle and jamming attack.

Zhang et al. [15] proposed a physiological signal-based cryptography scheme for key agreement. In this scheme uses's ECG signals is used to generate cryptographic keys. It follows plug and play architecture. So, no previous key distribution is required.

Table 1. Comparison of various security approaches in WBAN

Category	Authors	Description	Key elements	Pros and Cons
Physiological signal-based schemes	Zhang et al.[15]	The physiological signal-based cryptography scheme is used for key management.	ECG signals	Follow plug and play architecture. energy and time efficient. Limitation are complexity and cost.
	Reshan et al. [16]	The physiological signal, finger prints, fuzzy algorithm and fuzzy vault scheme is used for key agreement protocol.	ECG signals, fuzzy vault	Support high security, authenticity, reliabilty, and accuracy. Challenges are variation and distinctiveness of signal.
	Shanthapriya and Vaithianathan [17]	The higher order polynomial curve hides the data and securely transfer from one node to another.	ECG signals, Wavelet and Fourier transform	Resisiliance against large-scale node capture attack and lightweight method to secure BAN. It is more complex.
	Yao et al. [18]	This protocol uses interpulse intervals, ECG and Bloom filter is used for key generation and distribution.	ECG signals, Bloom filter	Low communication overhead, high protection, easy to key refreshment, follow plug and play architecture. Complexity is high.
Cryptographic keys-based schemes	Wang et al. [19]	The security framework based on blockchain and distributed storage structure called eHealthcare system.	Blockchain	Less hardware utilization, stable performance, scalability issue. Implementation is costly.
	Sayed Ashraf Mamun [20]	This protocol provides lightweight anonymous and mutual authentication based on bluetooth low energy.	Bluetooth low energy (BLE) security	Support anonymity, reliability, scalability. Variation is the issue of this approach.
	Xu et al. [14]	XOR operation and hash function is used to provide mutual authentication and key management for WBAN.	XOR operation, fuzzy vault scheme	Protection against eavesdropping, replay, capture, man in middle and jamming attack. Limitation is rekeying and refreshing the keys.
	Ostad-Sharif et al. [21]	Provided lightweight and anonymous authenticated key agreement protocol for WBAN	Timestamps, XOR operation	Provide defence against wrong session key and desynchronization attack.

	Kasyokaa et al. [22]	Uses Elliptic curve cryptography (ECC) to provide pairing free authentication for healthcare management system.	Hash function and ECC	Supported resource constrained environments, Low power consumption Replacement of old keys is an issue of this scheme.

The cryptographic keys are unique because of every human have different ECG signals. The ECG signals based cryptographic keys are unique and fulfil the requirement of key management such as longer length of key, dynamic, randomness and time variant. This method takes less energy and time to compute keys. When two nodes want to securely communicate then each node separately measured ECG signals at four seconds and perform feature extraction. In feature extraction phase collect ECG data at interval of four seconds and resample at 120 hz. After taking 512 points of Fast Fourier Transform (FFT) data collect 256 coefficients. After that detect local peak coefficients which uses to generate cryptographic keys.

If the patient's information or medical records is altered or stolen by an adversary, the patient could possibly get the wrong diagnosis or will not get timely treatment.

Shanthapriya and Vaithianathan [17] proposed a steganography technique to fulfil the security requirement such as confidentiality and authentication without altering the privacy of the node. The higher order polynomial curve hides the data and securely transfer from one node to another. The performance of this healthcare network is evaluated by using Wavelet and Fourier transform. The polynomial is generated by ECG signals feature detection. The ECG signals changed in time and frequency domain feature selection. After quantization detect peak points which changed into binary form. The higher order of polynomial generated using feature selection of ECG signals. This is a lightweight method to secure BAN.

Yao et al. [18] proposed an interpulse-intervals based key agreement protocol which can uses randomness, variance, uniqueness and distinct features of electrocardiograms (EKG) signals. It is using Bloom filter to recover problems provider set the public and private key with each other. In authentication part the client node and application provider authenticate each other. This approach fulfil the in physiological signals like uncertainty or inconsistency. By using bloom filter, the high security is gain with low cost. Here the bio features of EKG signals are shared among nodes.

The traditional method of healthcare system data are stores in a central database. When the central databases are compromised then the whole network is compromised. So, Wang et al [19] proposed a security framework based on blockchain called eHealthcare system. It is following the distributed storage structure of data. All participants on medical system can add data as a ledger which append only and distributed. Modifying records needs tendering a modification transaction which are nonrepudiation assets of the blockchain, means each transaction is cryptographically signed and protected. All the transactions will be added by ensuring that it will follow rules and policies of medical system. Introducing the blockchain in WBAN security can enhance the protection, reduce the resource utilization and improve the performance.

Sayed Ashraf Mamun [20] proposed a protocol based on Bluetooth low energy which provide lightweight anonymous authentication and mutual authentication. It is energy efficient scheme for internet integrated healthcare system. This method can add 3.8% power overhead from basic protocol.

Another physiological signal and biometric features and fuzzy algorithm based key agreement and distribution protocols are proposed by Reshan et al [16]. In this method, first the sender node initiates communication by generating random secret key by using prestored biometric and fuzzy algorithm. After that features of physiological signals uses to protect secret key by using fuzzy vault scheme. The secure secret key with authenticator is send by sender node to receiver node. Where authenticator contains ID of sender and receiver node, timestamp value and lifetime of key. After receiving this message, receiver node opens the fuzzy vault by using their own physiological signals and biometric to unlock the key. After that receiver can authenticates messages and user and establishes secure session between sender and receiver. In summary, this scheme provides high security, reliability, flexibility in key management scheme.

Ostad-Sharif et al. [21] proposed a lightweight method for authentication and key management protocol to protect WBAN. In this method, there are three phases initialization, registration and verification. In the verification phase the sensor node authenticate user by using information of hub node. In this paper the author review Li et al's protocol and points out some limitations. In their proposed method limitations are overcome by author. This method guaranteed the privacy of user and secure against various attacks such as session hijack attacks, man in middle attack, replay attack, eavesdropping and modification attack.

Kasyokaa et al. [22] has proposed a key management and secure method in WBAN. This method using ECC and provide pairing free authentication in healthcare management. This method has three part initialize, register and authenticate. In first part, network manager initializes the parameters of system and cryptographic hash function to generate public and secret key. In register part a smartphone controls all sensors used in WBAN. The client node and the application requirement of resource constraint environment of WSN.

4. System Model

4.1. WBAN Model

A WBAN is collection of smart body sensors and environment sensors which are implanted, attached or worn in human body. These biosensors are collected bio signals generated from body in real time. These information's are collected by the body sensors and send to the access points through wireless medium. The access points are that node who have more resources like energy, collect data from different body sensors and send to the local servers. The physiological signals are analysed and monitored by medical staff, doctors or specialist. Any problem diagnosed by medical specialist according to data collected then immediately treatment can start. It is depicted in Figure 4.

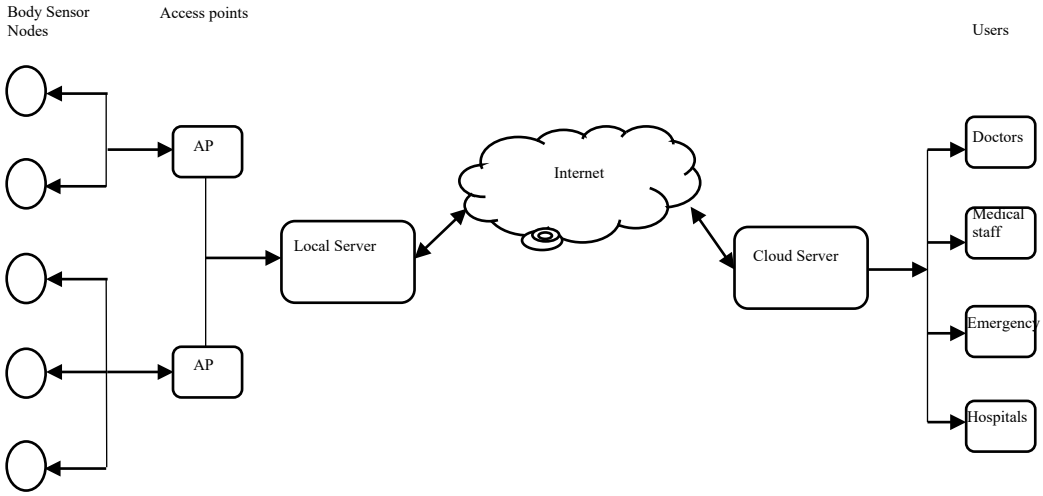

Figure 4. WBAN model

Our scheme uses network model 802.15.6 standard which was proposed by IEEE for body area networks in 2012. It is mainly using two hop central architecture [23][24]. In our scheme mainly three types of nodes, ie, body sensor node (N_S), access point (N_{AP}) and head node/local server (N_H). NS are the resource constraint sensors which are attached to body and receive physiological signals and transmitted to N_{AP}. N_{AP} and N_H are more resource efficient than N_S. All the data collected by N_{AP} send to the N_H which works as a local server and have rich resources. Figure 4 depicted the network model of our scheme.

4.2. Threat model

We assume that adversary is able to get data which are exchanged. He can insert malicious script or data, update the data and delete data and replace new data from old. In this threat model we assume that two parties or sensors want to communicate in insecure medium. Therefore, the sensors are not trusted, and medium is not secure. When any sensor node is compromised then adversary can extract all information from sensor node. Consider the following assumption in our approach are as follows.

- The head node and access points are trusted and will not be captured by any adversary.
- All the new body sensor nodes are not trusted.
- The malicious node measured to be a probabilistic polynomial time which are given in previous cryptographic mechanisms. The adversary wants to generate multiple fake identification (ID) to perform various attack on sensor network.
- The node is physically access by an attacker. The aim of attacker to recover keys and other cryptographic material which had used for Encryption/Decryption.
- Some of adversaries might observe the traffic of communication. This threats main aim to observe the factors (routing information, frequency etc.) of traffic, communication contents and finding the information's about the nodes.

4. Proposed approach

WBAN is the essential part of any healthcare network. We want that any node joins the network securely and it is not dangerous for the network. Therefore, the basic idea behind proposed method is that any new node joins a WBAN with the help of any access point. The access point forwarded the join request of new node to head node/ local server. The head node generates a new ID for newly join sensor node which can securely communicates in WBAN. Figure 5 shows the schematic diagram of the proposed approach.

5.1 Specification

When any new node joins WBAN then our approach produces a secure node ID for newly joining node (N_S) with the help of a access point node (N_{AP}) and head node/local server (N_H). The approach mainly works in three phases; initial phase, joining request phase and the endorsement phase. Table 2 explain the symbol used in our scheme.

Table 2. Symbol used

Notations	Meaning
PU_x	Public key of node X
PR_x	Private key of node X
IP_x	Initial unique identification of node X
T_S	Timestamp value
α, β and γ	Parameters generated during operation
X .Y	Point multiplication of X to Y
X || Y	Concatenation of the X and Y
H(.)	Hash operation
T_{AP}	Time taken during communication with access poimt node
T_{SH}	Time taken during communication with head node
T_H	Hash function computation cost
T_{mul}	Computation cost for scalar point multiplication
T_{add}	Computation cost for addition
T_{inv}	Computation cost for inverse operation
T_{PU}	Computation cost for public key generation
T_{PR}	Computation cost for private key generation

5.2. Initialization phase

Assume that there is a group (G_P) of large prime number of order P where G is a primitive element of G_P. The parameters G and G_P are available for all the nodes in the network. When any N_{AP} and N_H which already exist in the WBAN, then both N_{AP} and N_H select PR_{AP} and PR_H as their private key respectively which belongs to G_P. The public keys of AP and N_H are calculated as follows:
$PU_{AP} = PR_{AP} . G$ and $PU_H = PR_H . G$

Request phase

A new joining node N_S which wants to join the cluster, it must have the public parameters and the ID of at least one known node. The public parameters should be known by installing the overlay code.
Here the new node selects a random number PR_S which is the private key. And the public key of new node N_S is calculated as:

$PU_S = PR_S . G$
Then, N_S request by following steps.

Step 1

N_S request to N_{AP} for joining the cluster by sending their public key and unique ID by encrypting public key of known node.
PU_{AP} {IP_S|| PU_S}

Step 2

The access point node N_{AP} receives the joining node request from N_S. After extracting IP_S and PU_S, the N_{AP} calculates $\alpha = PR_{AP} . PU_S$
then N_{AP} sends the following message to head node N_H. The message is encrypted with the public key of N_H .
PU_H{IP_S||PU_S|| α }

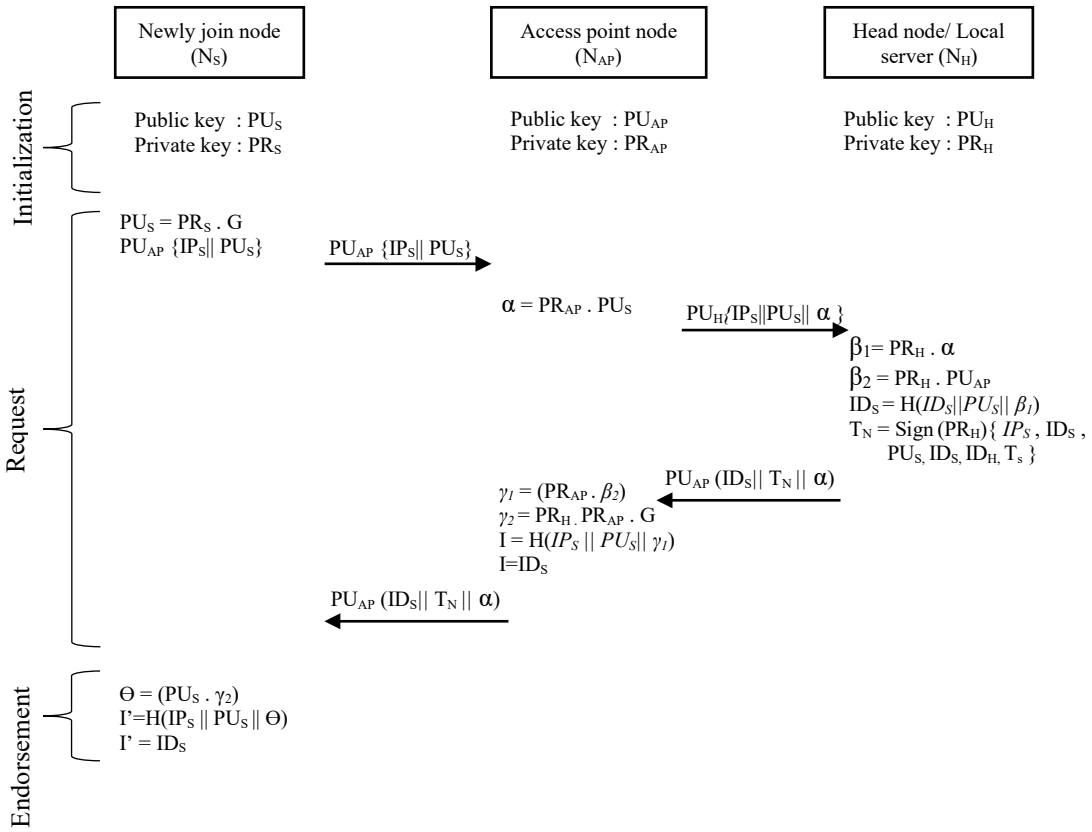

Figure 5. Schematic diagram of our prposed approach

Step 3

The N_H receives the message from N_{AP} for joining of node N_S. After, extracting the content of the message, N_H computes the following:

$\beta_1 = PR_H . \alpha$ and $\beta_2 = PR_H . PU_{AP}$

After that the N_H computes the ID of the new node N_S.

$ID_S = H(ID_S||PU_S|| \beta_1)$ where H represents the standard hash function like SHA1.

After that N_H generates a token by including unique ID of N_S public key of new node (PU_S), ID of the known node (IDS), ID of the N_H (ID_H) and the timestamp value. The N_H returns the signed token to N_K which is signed by private key of N_H.

$T_N = Sign (PR_H)\{ IP_S , ID_S , PU_S, ID_S, ID_H, T_s \}$

Step 4

The node N_K verifies the ID_S by using private key and compute following.

$\gamma_1 = (PR_{AP} . \beta_2)$ and $\gamma_2 = PR_H . PR_{AP} . G$

After that, known node N_{AP} calculates the following

$I = H(IP_S || PU_S|| \gamma_1)$

After that N_{AP} verifies

$I=ID_S$

If the verification is successful, then N_k sends (ID_S $||T_N || \gamma_2$) the following message to node N_S.

5.4. Endorsement phase

The N_S receive the message from N_{AP} the N_S calculates the following

$\Theta = (PU_{new} . \gamma_2)$ and

$I'=H(IP_S || PU_S || \Theta)$

After that it checks

$I' = ID_S$ then

It checks the token T_N to use it for further communication inside the network.

5. Result and Analysis

This segment represent the theoretical and analytical analysis to evaluate performance of proposed secure new node joining scheme. The design requirement analysis, computation complexity analysis, storage overhead analysis, and communication overhead analysis also present.

6.1 Design requirement analysis

There are mainly two types of attacks that an adversary node can perform, e.g., active and passive attacks. In passive attack, an adversary analyzes the traffic by overhearing and get some information about the key without any physical access to the node. However, in active attack, an adversary

obtains some information of key that leaked through the physical access of a node. The proposed scheme can provide defense against node various attacks.

Security against eavesdropping attack

The adversary can get messages from transmitted medium. It means that the adversary can get the content of transmitted information which are transferred from sensor node to access node and access node to the sensor node. These messages are following.

NK to NB : $PU_b\{IP_{new}||PU_{new}||\ \alpha\ \}$

And N_B returns the signed token to N_K which is signed by private key of N_b.

$T_N = Sign\ (PR_B)\{\ IP_{new}\ ,\ ID_{new}\ ,\ PU_{new}, ID_k, ID_b, T_s\ \}$

First of all, in both cases all messages are encrypted with public key of receiving node. The public key of node is calculated from large prime number. Secondly, the adversary not able to get parameters α, β and γ and ID_{new} because it is encrypted with strong public keys.

Sensor node anonymity

The generated ID of newly join sensor node never transmitted directly to sensor by access node. It has always wrapped by public key of sensor node. An adversary will not get the ID by eavesdropping attack. And the parameters such as T_N, α, β and γ are refreshed each time. These variables are also random and not guessable by any adversaries. The generated ID is hashed with the strong hash function. So, it is not possible to get ID of the new node. And guaranteed for sensor node anonymity.

Impersonation attack

It is assume that any adversary obtain the information $ID_{new} = H(IP_{new}||PU_{new}||\ \beta_1)$ by capturing the message then it also not get the ID of new node. Each message is encrypted with one way hash function therefore, adversary hijack the message but not get the useful information. Also, the token (TN) is produced and confirmed by the base node.

Traceability

Our proposed method tracks any node by all the parameters of the token T_N. The T_N which is defined as $T_N = Sign\ (PR_B)\{\ IP_{new}\ ,\ ID_{new}\ ,\ PU_{new}, ID_k, ID_b, T_s\ \}$. In the protocol specification steps, the verification of real identity which are collaborated by node ID and validity checks with the issuing time.

Unique

In our proposed approach, initially we have assigned temporary ID of each sensor which want to join the network. With the help of access node, the permanent node ID assigned to sensor node. This ID is unique and not same as another node ID because every time the node ID is assign with the help of public key cryptography. Every ID is wrapped with its temporary ID and the token generated by access node. Each token can be verified by corresponding pair node. So, the generate ID is assumed to be unique.

Secure Joining

The access point node can generate hash value of public key of new node and permanent ID of new node with the help of strong hash function like SHA1.

Scalability

Our proposed approach is easily applied on any size of network. It will support either static or dynamic structure of sensor network.

Stability

Our proposed approach collaborates the cluster head and any previously existing node to offer stability. So, no other node can change the ID of node.

DoS attack

Our proposed scheme offers unique node ID assignment where every node gets their ID by using secure public key cryptographic approach. So, by this approach we protect body sensor from message injection in network.

6.2. Communication cost analysis

Below we analyze the efficiency, attack model, re-keying for a member leaving and safety of nodes of the proposed scheme.

Storage cost analysis

Initially each sensor node N_{new} need to store temporary id of 16bits. The access point node wants to store $PU_b\{IP_{new}||PU_{new}||\ \alpha\ \}$ and $ID_{new} = H(IP_{new}||PU_{new}||\ \beta_1)$ which takes 192 (64 +64+ 64) and 256 bits because the SHA-256 takes 256 bits. The base node needs to store all the id generated for sensor node which can take 256 + 448n bits where n is the number of sensor nodes. Therefore, every sensor nodes store 16 bit id and 64 bits of key. The tuple transfer from N_{new} to N_K is $PU_{sn}\ \{IP_{new}||\ PU_{new}\ \}$ and it takes 64 +64 +64 =192 bits. The tuple transfer from N_K to N_B is $PU_B\{IP_{new}||PU_{new}||X1\}$ and it takes 64 +64 +64 =192 bits. Finally, the token $T_N = Sign\ (PR_{CH})\{\ IP_{new}\ ,\ ID_{new}\ ,\ PU_{new}, ID_k, ID_{ch}, T_s\ \}$ and $I = H(IP_{new}\ ||\ PU_{new}||\ X_2)$ then it will take 64+64+64+16+16+16=240 bits and 256 bits.

Energy utilization analysis

The energy constrained sensor nodes consume more energy during transmission of data packet rather than node process or generating data packets. This work analyses consumption of energy during joining of new node in the network. The energy consumption mainly calculated with the number of packets transferred and received among nodes. In our proposed approach, the total energy consumed during previous approach. Our proposed scheme can aggregate of energy consumed by single node, cluster head node and known node.

$E`_{Total} = E_N + E_{CH} + E_K$

So, no need to new node communication with the base station. So, our approach takes lesser energy than previous approach.

6.3. Communication cost analysis

The computation cost analysis mainly focuses on cryptographic operations such as scalar point multiplication, hash operations, key generation, addition and inverse operation performed by our approach and various other cryptographic approach. The computations complexity of hash function is lesser than the public and private key calculation time which means that $T_{PU} > T_H$ and $T_{PR} > T_H$. The computation time of T_H takes linear and at worst case it takes quadratic time.

Computation cost $T_{SN,}$ when any sensor node wants to join the WBAN with the help of access node.

$T_{SN} = T_{PR}+T_{PU}$

Computation cost $T_{KN,}$ when any sensor node request to known node.

$T_{KN} = 3\ T_{add} + 4\ T_{mul} + T_{inv} + T_{PR} + T_{PU} + T_H$

Computation cost $T_{BN,}$ at base node level.

$T_{BN} = 6\ T_{add} + 6\ T_{mul} + T_{inv} + T_{PR} + T_{PU} + T_H$

For a 32-bit Cortex-M3 microcontroller with 72 MHz, SHA-1 hash function takes 0.06 ms. During the request of ID for newly join node with the help of known node and communications with base node it will take $T_{KN} = 37.479$ms and $T_{BN} = 75.54$ ms. The following Table 3 shows the result analysis our proposed approach.

Table 3. Summary of result analysis

Ressiliance against	Eavesdropping attack	Scalability	Traceability	Impersonation attack	Sensor node anonymity	DoS attack
Storage cost	New node take 16bits, Access point node takes 256 bits, Head node takes 256+448n					
Energy utilization analysis	$E`_{Total} = E_N + E_{CH} + E_K$					
Communication cost analysis	$T_{KN} = 37.479$ms and $T_{BN} = 75.54$ ms.					

6. Conclusion and future direction

The acceptance of internet integrated wearable medical devices is trending in the field of healthcare. WBAN can monitor real-time data collected from patient and provide immediate prescription from medical service providers. It also reduces burden from the medical service providers. Due to the wireless and broadcast nature of communication in healthcare services, it is always vulnerable to privacy breach, eavesdropping, DoS, malicious data injection, node compromised, and many attacks made by adversary. For securing the healthcare networks, we proposed a public key cryptography based new node joining approach to provide unique node ID for newly join node.

Acknowledgment.

This paper is funded by University Grant Commission (UGC), India under Junior Research Fellowship (UGC NET-JRF) vide letter no. 3331/(SC)(NET-JUNE2015). Authors are also thankful to Director, IMS engineering college, Ghaziabad for his constant encouragement and motivation.

References

[1] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: a survey," Mobile Networks and Applications, vol. 16, no. 2, pp. 171–193, 2011.

[2] A. Rghioui, A. L'aarje ,F. Elouaai and M. Bouhorma, "The internet of things for healthcare monitoring: security review and proposed solution," In proceeding of Third IEEE International Colloquium in Information Science and Technology (CIST), pp. 384-389, 2014. IEEE.

[3] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system, " Future Generation Computer Systems. Vol. 1, no. 82, pp 375-87, 2018.

[4] A. K. Gautam and R. Kumar, "A comparative study of recently proposed key management schemes in wireless sensor network, " In proceeding of International Conference on Computing, Power and Communication Technologies (GUCON), pp. 512-517, 2018, IEEE.

[5] N. Paul and T. Kohno, "Security risks, low-tech user interfaces, and implantable medical devices: a case study with insulin pump infusion systems," in Proceedings of the 3rd USENIX conference on Health Security and Privacy, p. 8, USENIX Association, 2012.

[6] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar and S. Shamshirband, " Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, " Egyptian Informatics Journal, vol 18, no 2, pp. 113-122, 2017.

[7] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application, " Procedia computer science. Vol 1, no. 132, pp. 1243-1252, 2018.

[8] White paper Cisco External, Healthcare security,

[9] https://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/healthcare-security-white-paper.pdf.

[10] S. Chatterjee, A. K. Das, and J. K. Singh, "A novel and efficient user access control scheme for wireless body area sensor networks," Journal of King Saud University-Computer and Information Sciences, vol. 26, no.2, pp. 181-201, 2014.

[11] R. Kumar and R. Mukesh, "State of the art: Security in wireless body area networks, " International Journal of Computer Science & Engineering Technology (IJCSET) , vol. 4, pp. 622–630, 2013.

[12] J. White, "White paper: Top types of cyberattacks on hospital, healthcare networks, "http://www.healthcarebusinesstech.com/top-cyberattacks-hospitals/

[13] S. Cherukuri, K. K. Venkatasubramanian and S. K. Gupta, "Biosec: A biometric based approach for securing

communication in wireless networks of biosensors implanted in the human body, “ In proceeding of International Conference on Parallel Processing Workshops, 2003, pp. 432-439, 2013, IEEE.

[14] T. G. Zimmerman, “Personal area networks: Near-field intrabody communication,” IBM Systems Journal, vol. 35, no. 3-4, pp. 609–617, 1996.

[15] Z. Xu, C. Xu, H. Chen H and F. Yang, “A lightweight anonymous mutual authentication and key agreement scheme for WBAN, “ Concurrency and Computation: Practice and Experience, vol. 31, no, 14, pp 5295, 2019.

[16] Z. Zhang, H. Wang, A. V. Vasilakos and H. Fang, “ECG-cryptography and authentication in body area networks, “ IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, pp. 1070-8, 2012.

[17] M. Al Reshan, H. Liu, C. Hu and J. Yu, "MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks," IEEE Access, vol. 7, pp. 78484-78502, 2019.

[18] R. Shanthapriya and V. Vaithianathan, “Secured healthcare monitoring system in wireless body area network using polynomial based technique. “ Polish Journal of Medical Physics and Engineering, vol. 25, no. 3, pp. 171-177, 2019.

[19] X. Yao, W. Liao, X. Du, X. Cheng X and Guizani M, “Using Bloom Filter to Generate a Physiological Signal-Based Key for Wireless Body Area Networks, “ IEEE Internet of Things Journal, vol. 6, no. 6, pp. 396-407, 2019.

[20] J. Wang, H. Kaining, A. Anastasios, C. Zhiyu, Z. Zeljko, P. Yu, J. Gwanggil and F. Piccialli, "A blockchain-based eHealthcare system interoperating with WBANs," Future Generation Computer Systems 2019.

[21] S. A. Mamun, "Sensor Networks in Healthcare: Ensuring Confidentiality and User Anonymity in WBAN.", 2019, arXiv preprint arXiv:1910.00991

[22] A. Ostad-Sharif, M. Nikooghadam and D. Abbasinezhad-Mood, “Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks, “International Journal of Communication Systems. vol. 32, no.12, pp. 3974, 2019.

[23] P. Kasyoka, K. Michael and S. M. Angolo, "Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system." Journal of Medical Engineering & Technology, pp. 1-8, 2020.

[24] M. Kompara and M. Hölbl, ``Survey on security in intra-body area network communication," Ad Hoc Netw., vol. 70, pp. 2343, 2018.

[25] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. D. Zeeuw, ``Enhancing heart-beat-based security for mHealth applications," IEEE J. Biomed. Health Inform., vol. 21, no. 1, pp. 254262, 2017.

[26] N. Jamali and L. C. Fourati, “SKEP: A secret key exchange protocol using physiological signals in wireless body area networks,” In Proceeding of Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), pp. 1–7, 2015.

[27] A. S. Sangari and J. M. L. Manickam, “Public key cryptosystem based security in wireless body area network,” In Proceeding of Circuit Power Computing Technology (ICCPCT), pp. 1609–1612, 2014.

[28] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks,” Comput. Network, vol. 129, pp. 429–443, 2017.

[29] Z. Xu, C. Xu, W. Liang, J. Xu and H. Chen, “ Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things”.