Biomedical Research 2016; Special Issue: S276-S282 *ISSN 0970-938X*
www.biomedres.info

Enhanced bio-trusted anonymous authentication routing technique of wireless body area network.

Sudha R[1*], Devapriya M[2]

[1]Department of Computer Science, PSG College of Arts and Science, Coimbatore, Tamil Nadu, India

[2]Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu, India

Abstract

In the current wireless era most of wireless body area networks are establishing Anonymous communications in adversary environments. This work aimed at preserving two factors unidentifiably and unlinkabilty as essential characteristic of this wireless body area network. Even though there are several existing researches focuses on anonymous secure routing protocols the requirement is not utterly satisfied. Previously existing protocols are susceptible to the attacks of counterfeit routing packets yet the node individualities are confined by pseudonyms. This paper devised a new biometric fusion based trusted anonymous secured routing protocol which assures prevention against such attacks. More specifically, the route request packets were authenticated by an iris fused with DNA coding to generate a dynamic complex group signature and to secure beside possible active attacks exclusive of presenting the node identities. In addition this work also prevented revealing real destination to intermediate nodes by adapting key-encrypted pairing onion. Simulation results confirmed the efficacy of the projected BFTASR protocol with enhanced performance as evaluated with the existing protocols.

Keywords: Wireless body area network, Biometric security, Healthcare, Anonymous routing, Authenticated routing.

Accepted on September 06, 2016

Introduction

There is a rapid growth in mobile health monitoring system due to the establishment of wireless body area network. It is very supportive to many of the medical oriented and no on-medical oriented applications by operating in close locality to, on or within a human body. With the help of wearable devices Wireless Body Area Network (WBAN) provides communication between humans and computers. It adapts the existing available techniques of wireless sensor network and adhoc networks to perform enhanced communication. Accurate sensing of the signal from the human body and processing the sensor signal are performed by a typical device node in WBAN. Finally it transmits wirelessly the processed signal to an area process unit [1].

Data security should be important concern in WBAN because without going to hospital it monitors patients at home and work space. Possibility of accessing healthcare information of patients by unauthorized users may happen. The failure of complex security features not only has an effect on the patient security and confidentiality but it compromises the patient safety [2].

In the earlier period, numerous researchers have been centering on building system architecture of health monitoring to progress the technological prerequisite purposely intended for WBAN. Few researches were initiated in offering the tough security method in anonymous authentication based secure routing. As component of communication means, WBAN faced assorted security problems such as failure of data, authentication and access control. Employing high security system directs to discrepancy in computational performance. It is suggested that the security system for WBAN must be deployed with small computational difficulty and elevated power effectiveness. None of prior researches effectively recognized elucidation to the above trouble. This proposed study investigates the use of biometric characteristics in anonymous authentication of trust based secure routing within WBAN in and reducing computational complexity as well as power efficiency.

Related Work

WBANs topology inherits many types of medical sensors which can be communicated to other control nodes like smart phones or medical sensors that can be interfaced with auxiliary types of networks like WiMAX/WiFi/VANET to distribute the composed information to the information hub [3]. Much enormous attempt has been dedicated to extend secure communication systems between the internet and control nodes [4]. Thus, this study centers on securing inter sensor communication in excess of the body area. In WBAN [5,6], key sharing is forever susceptible to man in the center attack. There are two types of threats namely active and passive

attacks. Dropping, reply to earlier messages and performing modification to the messages are the actions done by active attackers. Passive attackers are those who get tires to listen and observe the communication over WBAN unauthorized. An inclusive review on wireless body area networks is given in [7]. In addition the intermediary key sharing schemes, there are numerous enduring research works that employ the key distribution using biometric features. The fuzzy vault method was anticipated by Jules et al. [8]. This comes within reach of generating the polynomial that encodes the information. The security of vault lies on accumulating extra chaff points which brings the communication transparency. This technique uses fuzzy vault scheme to lock the key and unlock the vault to redevelop the key at receiver side. Studies has projected a hybridized security technique for secure messaging over WBAN [8,9]. Authors have employed asymmetric cryptography only for node organization process and to prevent link security symmetric cryptography was adapted [10,11]. The conventional asymmetric cryptography has serious exponential calculations and also size and calculation abilities. The authors have proposed a watermarking-based ECG signal tempering recognition approach [12,13]. A low frequency 15-digit chirp code is entrenched in wirelessly transmitted Electrocardiography (ECG) signal. That system can also entirely eliminate chirp code watermarks from rebuilded ECG signal to lessen ECG visualization deformation [14]. Sofia et al. has presented an impression of body area network and their associated issues prominence in security trouble [15]. They also study the dissimilarity between wireless body area network and Wireless Sensor Network (WSN). They tinted the security challenges that still require to be addressed to construct WBAN truthfully everywhere for an extensive assortment of applications. WBAN takes out a new set of confront in requisites of scalability, sensor consumption and density, energy effectiveness, security and privacy and wireless technology so WBAN necessitates an important safety measures system and element of it is validation. So there is a must to establish fusion based authentication protocol which will offer a well-built security scheme for WBAN. Ramesh et al. have surveyed the present improvement on wireless body area network and overwhelmed in security troubles encountered by this technology [16]. WBAN still lacks with various issues on varied security problems like information loss, endorsement and control of access. They summarized about WBAN and serious stress in secure communication, variations between wireless body area network and wireless sensor network. Ragesh et al. have presented an outline on the range of characteristic of WBAN with usage of sensors, applications used, efficiency of power, protocols used for communication, security necessities, obtainable projects in WBANs and confront met by wireless body area networks [17]. They put forth discussion on requirement of energy, security and issues in different layers of WBAN. At last social problems in relation with WBAN application are stated in this paper.

In paper [18] has delivered a summary of body area network and their associated concern prominence in security difficulty. Lastly, they tinted the security attacks and requirements in WBAN pursued by the security risk appraisal.

Gunasekharan et al. designed a key agreement scheme that permits neighbouring nodes in WBAN to issue the universal keys created by electrocardiogram signal [19]. The expected ECG-humming bird key agreement system makes possible the secure messaging over the WBAN.

John described Secure Onion Throat (SOT) protocol is proposed to offer absolute secrecy in a desirable environment [20]. The SOT protocol uses group signature permutation and to discover the route onion routing with ID-based encryption is implemented. The security investigation explains the performance of Sensory Organization Test (SOT) protocol beside all categories of attacks.

Biometric Based Public Key Infrastructure

Iris feature extraction

There are 400 distinguished characteristic are presented in iris which can be computed and used to identify an individual [21]. Among them only 260 of those are promising to captured for recognition. These particularized characteristics are striations, contraction furrows, pits, filaments, collagenous fibers, crypts, serpentine vasculature, freckles and rings. Due to these distinctive characteristics, the iris has six times additional distinct exclusive features compared to fingerprint

In this process an iris image of the individual is selected.

1. Convert RGB value of the input image to Gray scale image

$y=B \times 0.114+G \times 0.587+R \times 0.299+128$

$u=B \times 0.5-G \times 0.33126-R \times 0.16875+128$

$v=B \times (-0.08131) -G \times 0.41869+R \times 0.5+128$

2. Convert the Gray scale image into planar image

a. Setting the horizontal and vertical kernels respectively as follow:

$$\begin{bmatrix} 1.0 & 0.0 & -1.0 \\ 1.0 & 0.0 & -1.0 \\ 1.0 & 0.0 & -1.0 \end{bmatrix} \quad \begin{bmatrix} -1.0 & -1.0 & -1.0 \\ 1.0 & 0.0 & 0.0 \\ 1.0 & 1.0 & 1.0 \end{bmatrix}$$

b. Created planar image in step-2, is conceded through kernels created in step-a.

c. Customized fine-grained planar image is edge detection of iris image.

3. Edge detected iris raster data is examined and accumulated into a vector size matrix.

a) $v_{Size} = f_{size}- (54+ (4 \times 256))$

b) With the BMP edge detection of iris 8 × 12 Iris pattern is extracted using following logic:

For (x=0; x<=origlImage.rows-1; x^{++})

{

For (y=0; y<=origImage.cols-1; y^{++})

{

if (y<30 && x=((origImage.rows/2) +4) && GryValue==255)

{

for (i=0; i<8; i^{++})

{

for (j=0; j<12; j^{++})

{

(edgImage.data + (i × edgImage.cols) +j) = (origImage.data +

(x × origImage.cols) - (i × origImage.cols) + (y + j));

Write down to new BMP image file

}}}}

Where

v_{Size}-vector Size, f_{size} is File size, origImage-Original Image, edgImage-Edge detected Image, GryValue-Gray value of the given iris image

Proposed private key extraction on iris by converting into DNA representation

The proposed step converts the extracted features of iris which in the representation of binary data to a DNA based representation string. There are numerous advances in this field to translate binary data to a DNA string and these are identified as DNA coding technology.

We propose a new DNA coding technology to convert binary data to DNA strings. The rule for coding DNA Representation String is shown in Table 1.

Table 1. *The rule for coding DNA representation string.*

Binary data	DNA data
00	AA
01	T
10	C
11	GG
0	A
1	G

The concept of the DNA conversion is if the iris binary string is '00' then it is converted to AA or if it is '11' then it is transformed to 'GG'. This process continues to convert all the binary information of iris feature extracted into a DNA sequence. In case if the length of the iris binary data is not even, the last two rows help us to convert correctly.

For example, if the value of binary string is:

00101001001001001001001001001001001011010100101
00100100101001001010111011010000010010101001101010101
01001001001001010010111111001011101011001001001001010
10010010100010010000010111101001001010

The value of iris binary string, which is based on the proposed DNA coding technology, is as follows

AACCTAACTAACTAACTAACTAACGGTTAACCTAACTT
ACCGGCGGTAAAATAACCAAGGTTTTCTAACTAACCTT
GGGGCTTGGTTCTAACTAACCTAACCAACTAAAATTG
GGGTAACTA

This work chooses a DNA secret key with a key length of 256 randomly from the resultant DNA code based iris feature extraction.

Public key generation

Most of the existing work uses RSA for public key generation this proposed work adapts Elgamal algorithm because security of the Elgamal depends on the difficulty of computing discrete logs into a large prime modulus and it has the advantage that the same plaintext gives a different cipher text each time it is encrypted. The secret key is individual's bio-cryptographic key generation as discussed in the previous section.

Where,

- pm be a large prime such that computing discrete logarithms modulo pm is difficult.
- μ<pm be a randomly chosen generator of the multiplicative group of integers modulo pm.
- β be secret key generated by iris-DNA representation based b bio-cryptographic private key generation

Compute public key $\tau=\mu\ \beta \bmod pm$.

These steps are performed once by the signer.

Group signature management

Let the WBAN network be considered as a group WG in this each node has its own private and public key. Each node sends untraceably one public key to a public list maintained in a trusted public directory as blinded public keys. This scheme overcomes the risk of maintaining trusted authority and to prevent secret key revealed through group manager. If a node N1 (for N1 ε WG) can sign its message using its private key denoted as GW_{N1-}, and this message can be decrypted by the public key GW_{WG+} by other nodes in the same group.

To sign a message m the signer N1 performs the following process

- A random number rk is chosen such that $1<tk<pm^{-1}$ and gcd (k, pm^{-1}) =1.
- Compute $v=\mu^{rk}$ (mod pm)
- Compute st=(Hash (m)-β v) rk^{-1} (mod pm^{-1})
- If st=0 start over again.

Then the pair (v, st) is the digital signature of m. The signer N1 repeats these steps for every signature.

During the signature verification process the signature (v, st) of a message m is verified as by the receiving node as follows.

0<v<pm and 0<st<p-1

$\mu^{Hash\ (m)}=\tau^{v}v^{st}$ (mod p)

The verifier accepts a signature if all conditions are satisfied and rejects it otherwise.

Onion routing

Three essential components of The Onion Routing (TOR) network are the entry nodes, exit nodes and other nodes. Entry nodes carry out the most vital and the most imperative duty in a TOR network; formalizing the intensity of encryption. Packets sent through a TOR network needs diverse levels of encryption based on their consequence. The progression of encrypting the packets depending on the prerequisite is done at the entry level nodes. These nodes receive packets in their true form devoid of any encryptions; therefore the entry nodes are high concert and extremely secure nodes that cannot be compromised simply. In the final layer of encryption exit nodes are strip off therefore they are also prepared reliable and protected. The residual nodes carry out the mediatory process of stripping off the encryption layers and promote\the packet to the subsequent node.

Process of route selection

During the initial step up phase of TOR network the bio-secure method of route selection process begins. With the help of corresponding routers in the network the identification of nodes and their distances are recorded. Generally TOR system performs the process of selecting next node it won't perform selection of route. This routing algorithm is circulated to all the routers in the network.

Algorithm:

1. Initial process starts with setting up the network node and then builds the graph accordingly

2. For each node determine the neighbour node set N

3. For each incoming packet do the following

a. If the curr_node ≠ exit _node then

i. Weighted sum of each node in the network is determined by calculating success rate, failure rate and other QoS parameters using the Equation 1

$$Wtsum_{route} = \sum_{i=1}^{X} wt_i * Norm_{route}$$

where,

$wtsum_{route}$-weighted sum of each router

W_{ti}-weight of the property i

$Norm_{routei}$ represents the normalized value of the i^{th} attribute for the router r.

ii. Find out the probability of choice of selecting each node by Equation 2

Prob (2)

where probroute – Probability of selecting route

iii. Find the destination router Dest_route using Cumulative Distribution Function as represented in the equation (3)

Funx (x) =Prob (X□x) (3)

iv. Repeat (iii) until the extinction condition is reached

v. Add Dest_route to Exploitation List if it is not in it.

b. If the current node=exit node then

Final layer encryption is strip off and packet is forwarded to the destination

If the node is an entry node while a packet is come across, it generate route selection process. In this method selecting route relies not only on the basis of distance between current and destination node; it includes the factor of QoS parameters which is related to transmission. The QoS parameters used in this work are jitter, delay and the level of network traffic presently encountered in the network circumference. In addition it also examines success and failure rates of the current. Because diverse networks are created with dissimilar functionalities a hard coded value will not be a suitable alternative. Therefore this method is done by the network administrator previous to deployment. All the routers in the network work with the identical constraint weights, thus this is a onetime course of action. To assign weight Analytic based Hierarchy Processing is performed.

Algorithm:

1. Initialization of node

a. Key server which shares the key at initial time

b. Normal node in WBAN

2. Initially the leader node will send the group ID key to all the nodes in WBAN

3. Once it is received by normal node it stores the ID into memory

4. If the node containing group ID

a. Generate private key using its multimodal biometric authentication for encryption

5. If not a. Can't access the request

6. If node (i) wants to communicates with another node then

a. If session available

i. Begin the communication with Lower Back (LB) Key

b. If no secure session then

i. Send the session request to its neighbour with digital sign 1.

A neighbour verifies the sign and establishes the session key to requester

ii. Session key is received from number of available neighbours and stay for small interval

iii. Launch local broad-cast key and send to protected neighbours

7. Subsequent to verification is ended sender digitally signs on Route Request (RREQ) packet and broadcast it

8. Receiver verifies sign and checks for destination

a. If it matches then Sends Route Reply (RREP) to node i

b. else matches forward to next node

9. If node i receives RREP then send data through found route

10. If node i not acknowledged within convinced time then resend RREQ

Experimental Result

Simulation result

In this proposed work Network Simulator version 2 (NS-2) has been used to simulate the results. In this section, the performance metric and implementation outcome of the proposed protocol is shown. This proposed work undergoes two different kinds of simulation results. In the first kind performance is compared based on their behaviours under the packet dropping, throughput and end to end delays in the presence of attacks with different levels. The second is to evaluate the routing performances of proposed TAASR with existing protocols namely Ad hoc On-Demand Distance Vector (AODV), Anonymous On-Demand Routing (ANODR), and Anonymous Secure Routing(AASR) under different mobility scenarios.

Performance metric

a. Packet Lost is measured by the total number of packets dropped during the simulation.

Packet lost=No.of packet send-No.of packet received

b. Throughput is calculated by the ratio of successful packet received at the receiver to number of packet generated

Throughput=successful packet received/no.of packets generated

c. End-to-end delay is determined by finding the average time taken by a data packet to reach the destination. In addition both delay time of route discovery process and the queue size in data packet transmission is also included. The data packets that successfully delivered to destinations alone are counted.

E-E delay=Sum (arrive time-send time) /Sum (Number of connections)

Performance evaluation under the effects of malicious attacks

To perform this scenario this work configured the mobile network with an average speed of 4 ms. The number of malicious nodes varies from 0 to 9. The results are recorded and plotted in the following Figures 1-6.

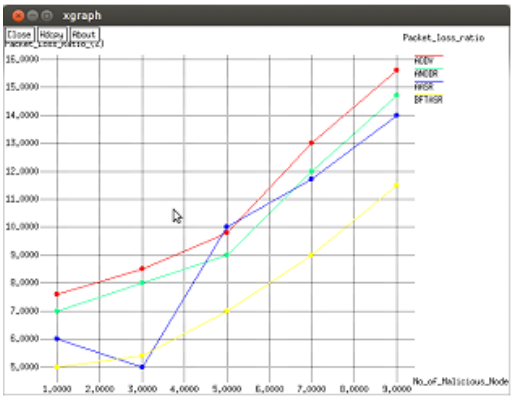

Figure 1. *Comparison based on packet loss ratio.*

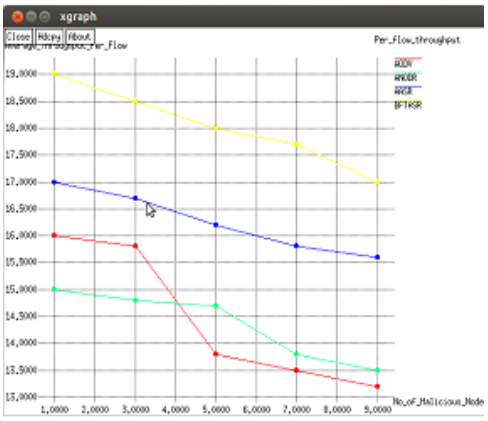

Figure 2. *The comparison based on throughput.*

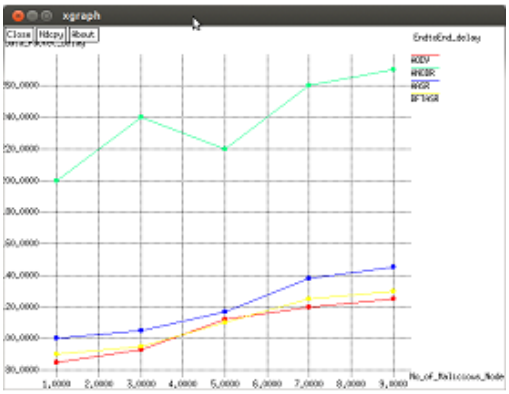

Figure 3. *The comparison based on end to end delay.*

As shown in the Figure 1 the proposed BFTASR has highest ability to identify packet dropping attack with the help of its trust management approach and it outperforms the existing techniques AODV, ANDOR and AASR. The more packet loss is examined on AODV while comparing the other protocols. AASR achieves 5% greater loss ratio than Trust model Authenticated Anonymous Secure Routing (TAASR) in average.

As shown in Figure 2, while there is increase in number of malicious nodes the average throughput of four protocols decreases obviously. Throughput of the proposed BFTASR is higher than the remaining existing protocols. Next to that AASR produces better throughput than ANODR and AODV.

The end-to-end delays are shown in Figure 3. It is observed that ANODR spends more time in route discovery while AODV is blind to the malicious attacks and takes no additional actions; its delay does not vary in the presence of different numbers of malicious nodes. Since TAASR spend time in the security processing in their route discovery, its delay is higher than AODV. If ANODR is under a heavy attack, it will launch new route discoveries for the broken routes, which introduce more delays in average. Compared to the attacked ANODR, AASR and AODV the proposed TAASR reduces the need of re-routing due to its trust based authentication and onion routing which results in 20 ms less of delay in average.

Performance evaluation of mobile scenario under adversarial environment

To simulate the adversarial environments, we set 20% of the total nodes, i.e., 9 nodes, as malicious nodes. The network mobility varied from 1 to 5 ms and records the performance results of the four protocols.

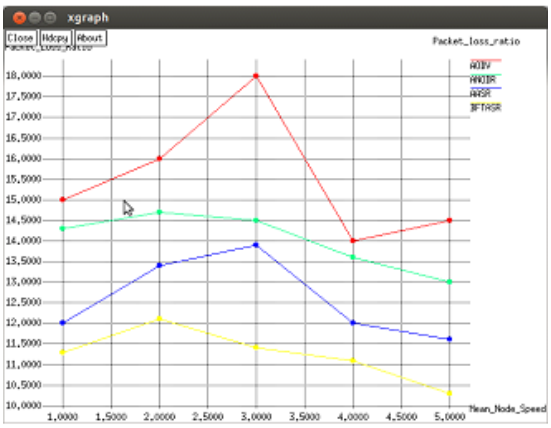

Figure 4. *The comparison based on packet loss ratio.*

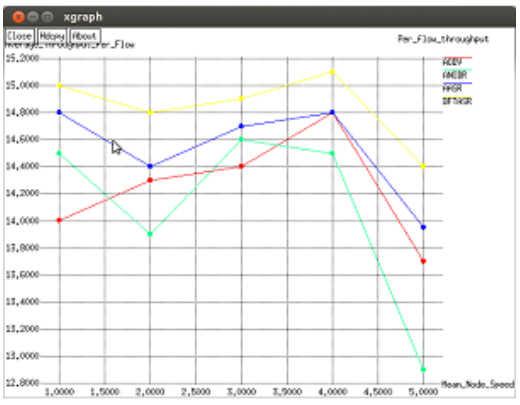

Figure 5. *The comparison based on throughput.*

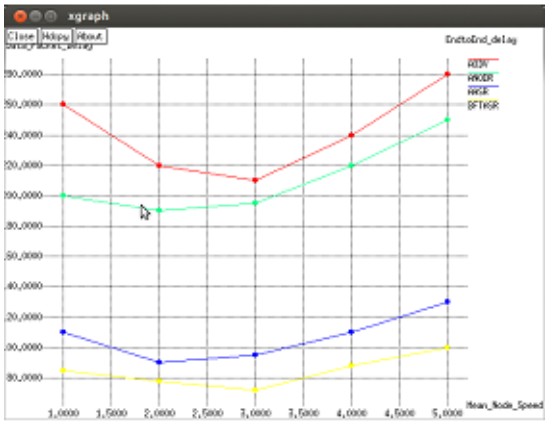

Figure 6. *The comparison based on end to end delay.*

As shown in Figure 4, while the mean node speed increases, the packet loss ratio of four protocols varies. Because the nodes move randomly and depending the defending property of each protocol the BFTASR performs better than the other three protocols. The worst case is AODV which is not capable of handling attacks in the adversarial environment.

The throughput of low connections may be improved or upgraded in different mobile topologies. Despite the performance variation, TAASR always achieves the highest throughput due to its trust based handling nature. This can be explained by its ability in defending the packet dropping attack. Observing Figure 5, it can be observed that the throughput and loss ratio achieved by ANODR and AODV are similar. Once being attacked, ANODR requires more cryptographic processing delays than the normal AODV protocol. As a result, sometimes ANODR performs worse than AODV, e.g., in the “slow” movement scenarios.

The curves of the end-to-end delay are shown in Figure 6. Due to the additional security processing time in RREQ flooding, AODV, ANODR and AASR have longer delays than TAASR, while AASR has 20 ms less of delay than BFTASR in average.

Results

In this section, the results have been analysed using the three performances metric are Packet delivery Ratio (PDR), throughput and number of dropped packets. In all graphs x-axis represents the number of nodes and y-axis represents the value of performance parameter. Throughput results show that the throughput of BFTASR is better as compared to AODV. Generally, by increasing the number of nodes, throughput also increases. Number of drop packets in the graph shows that the number of drop packet using AODV is increasing by varying the number of nodes but using BFTASR, least number of packets has been dropped. The Simulation result of packet delivery ratio shows that the PDR of AODV has some ups and downs at some point due to variation in the number of nodes but BFTASR is giving better result as compared to AODV.

Conclusion

The Biometric and cryptography relationship among nodes can be represented, calculated and combined using an item opinion. In our BFTASR routing protocol, each nodes can assist mutually to achieve an objective opinion about another node's trustworthiness. They are also capable of performing trusted routing behaviours according to the trust relationship among them. With an opinion threshold, nodes can flexibly choose whether and how to perform cryptographic operations. Therefore, the computational overheads are reduced devoid of the necessity of demanding and validating certificates at each operation of routing. Our BFTASR routing protocol is a more feasible and reliable by providing more flexible security elucidation than other cryptography and authentication design. It uses fused biometric key values to support packet forwarding by sustaining a trust counter for each node. If the trust counter value falls below a threshold, the corresponding intermediate node is malicious node. In this proposed scheme, high throughput and packet delivery ratio is provided by authorized node of WBAN and significantly decreases the average end to end delay.

References

1. Omer A, Benny L, Ara D, Guang ZY. Body sensor network. EBook Springer 2006.
2. Ethala K, Seshadri R, Renganathan NG, Saravanan MS. Secret handshake issue and validate authority based authentication system for wireless sensor network. J Comput Sci 2013; 9: 1174-1180.
3. Ab-Rahman MS, Hadiguna, Supian LS. Power analysis on same filter different sources for selection of spectral filters in optical demultiplexer. J Comput Sci 2013; 9: 866-874.
4. Bao SD, Zhang YT, Shen LF. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. Proc Int Conf Eng Med Biol Soc IEEE Xplore Press 2005; 2455-2458.
5. Barni M, Failla P, Lazzeretti R, Sadeghi AR, Schneider T. Privacy-preserving ECG classification with branching programs and neural networks. IEEE Trans Inform Forens Sec 2011; 6: 452-468.
6. Miao F, Jiang L, Li Y, Zhang YT. Biometrics based novel key distribution solution for body sensor networks. Proc Int Conf Eng Med Biol Soc IEEE Xplore Press 2009; 2458-2461.
7. Chen M, Gonzalez S, Vasilakos A, Cao H, Leung VC. Body area networks: A survey. Mob Netw Appl 2011; 16: 171-193.
8. Liu J, Kwak KS. Hybrid security mechanisms for wireless body area networks. Proc Int Conf Ubiq Fut Netw IEEE Xplore Press 2010; 98-103.
9. Babu AM, Singh KJ. Performance evaluation of chaotic encryption technique. Am J Applied Sci 2013; 10: 35-41.
10. Poon C, Zhang YT, Bao SD. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Commun Mag 2006; 44: 73-81.
11. Raghini M, Maheswari NU, Venkatesh R. Overview on key distribution primitives in wireless sensor network. J Comput Sci 2013; 9: 543-550.
12. Kaur S, Farooq O, Singhal R, Ahuja BS. Digital watermarking of ECG data for secure wireless Communication. Proc Int Conf Telecommun Comp Rec Trend Info IEEE Xplore Press 2010; 140- 144.
13. Duraisamy K, Ragavendran U. Low power analog multiplier using MIFGMOS. J Comput Sci 2013; 9: 514-520.
14. Jayanthiladevi K. Cluster based key management authentication in wireless bio sensor network. Int J Pharm Bio Sci 2016; 7: 89-94.
15. Ramesh K, Rajeswari M. State of the art: Security in wireless body area networks. Int J Comp Sci Eng Technol 2013; 4: 622-630.
16. Ragesh GK, Baskaran K. An overview of applications, standards and challenges in futuristic wireless body area networks. IJCSI Int J Comp Sci Issues 2012; 9: 180- 186.
17. Shikha P, Naveen B. Security issues in Wireless Body area network. Inte J Comp Sci Mob Comp 2014; 3: 1171-1178.
18. Sangari S, Martin LM. A light-weight cryptography analysis for wireless based healthcare applications. J Comp Sci 2014; 10: 2088-2094.
19. Gunasekaran M, Premalatha K. An anonymity-based secure on-demand routing for mobile ad hoc networks. W Acad Sci Eng Technol Int J Comp Electr Autom Contr Info Eng 2014; 8: 98-107.
20. John GD. High confidence visual recognition of persons by a test of statistical independence. IEEE Trans Patt Anal Mac Intel 1993; 15: 1148-1161.

*Correspondence to

Sudha R

Department of Computer Science

PSG College of Arts and Science

India