NOVEL TRUST BASED AUNTHENTICATION APPROACH IN WIRELESS BODY AREA NETWORK

Dr.R.Sudha

Associate Professor, Department of Computer Science
PSG College of Arts & Science, Coimbatore, India

Abstract

Recent advances in wireless technology leads to WBAN which promises inconspicuous ambulatory health observing for an elongated period of time and afford real-time apprises of the patient's position to the doctor. The leakage of privacy is one of the main issues in WBAN. Authentication is the primary step towards security. Enhanced authentication scheme inhibits the networks from pretenders and annoying users meritoriously. This paper proposes a trust based authentication protocol and its simulation result demonstrates that they outperform the existing systems in terms of improved trade-off between anticipated security possessions and computational complication.

Keywords: Trust Management, Authentication, Security, Onion Routing, Digital Signature and WBAN.

I. Introduction

Security in any wireless technology especially in wireless body area networks is highly needed. Authentication process is solitary of the preliminary steps for security employed to put off from the unconstitutional users and pretender.s Authentication schemes vary as per the nature of wireless body area network. For such networks, there is a need of specific light weight authentication schemes. Security starts with a negotiation of desired security suite between the two communicating the parties, node and hub. The security selection sets off a security association between the two parties. To activate a pre-shared or generating a new shared master key. Security association protocols are done based on the key exchange policies.

The process region of a WSN is extremely huge and can be used in ecological observing, manage temperature and moisture, vehicle transfer control, checking of human body organs, among others. Figure 1 exemplifies a situation of WBANs in the medical area where patients that are being observed can be in a hospital, at home, or anyplace besides performing an goings-on routine. Sensing data are send to health experts in the course of the Inter.net.

The fundamental security requirements in WBAN are described below, [8].

1. Data Confidentiality To protect the data from a revelation, the system necessitate data discretion
2. Data Authentication Applications together with mutually medical and non-medical relevance demands data authentication. Symmetric technique can be used in a WBAN to attain data authentication. This method shares the secret key to work out Message Authentication Code for all data.
3. Data Integrity This is compulsory as an rival can modify the data that is broadcasted over an anxious channel. Deficiency of data integrity system paves a way to the opponent to amend the information before it reaches the destiny.

II. Related Work

Numerous research factions have been emerging the implantable or wearable devices for health observation in WBAN communications. However, these researches in the main specialize in building system design and in lesser extent on developing networking protocols. Besides, it's tough to get solutions providing security for WBAN and security has typically been lined individually. Some researches show the security for sensor nodes in or on the human body in WBAN. They show that the sensors have to be compelled to build use of cryptographic algorithms to encrypt the data they send to regulate node and consequently the haphazard assortment that is engaged in security protocols will be produced by biometrics [1][18]. Biometrics advance uses relate degree essential trait of the individual body as the verification uniqueness or the means that of securing the allotment of a cipher key to protected inter-WBAN communications[17]. At early stage, lots of security scheme of WBAN are recognized by the symmetric cryptosystem due to limited resources, nevertheless have problems like impediment the illuminating of the symmetric keys and providing weak security comparatively since it's not durable against corporeal negotiation [2]. Besides the complexness of sensing element node's key managements in WBAN offer every part excess. On the divergent, some research exploit the asymmetric cryptosystem in mobile and ad hoc networks even have been intended, and tried to seem at the idiosyncratic uniqueness of WBAN [3][4]. One distress about the asymmetric cryptosystem is a source constraint trouble but current work has shown that performing ECC consumes a lot a lesser amount of of memory and computing power [4]. These researches addressed a reach of controlled WBAN though they exclude the embedded sensor networks. The objective of WBAN is in addition

the execution of body area network that may get in touch with with anywhere in, on, and out the human body. Otto et al. [5] and Jovanov et al. [6] presented a system design that each holds the contact inside the WBAN and among the WBANs and a medical server in an exceptionally multi-tier telemedicine scheme. The communiqué amid the sensors and also the sink is single-hop, holed and use ZigBee or Bluetooth. The slots are synchronous utilization inspiration at irregular intervals send by the sink. They use of the shelf wireless sensors to aim a prototype WBAN like the Tmote sky policy from at one time Moteiv [7], currently sentilla [8]. The European MobiHealth project [9] provides a whole end-to-end mHealth platform for ambulant patient observing organized over UMTS and GPRS networks. The MobiHealth patient/user is prepared with diverse sensors that continuously observe very important signals, e.g. blood pressure, heart rate and electrocardiogram (ECG). Communication between the sensors and the special device is Bluetooth or ZigBee based and is singlehop. The main issues considered are protection, reliability of communication resources and Quality of Service guarantees. The French project BANET [10] intends to construct a structure, replicas and tools to mode optimized wireless communication systems intending the widest contrast of WBAN-based applications, contained by the shopper usual philosophy, medical and sport fields. They focus in the study of the WBAN proliferation channel, MAC protocols and survival of WBANs and substitute wireless networks. The German BASUMA-project [11] focuses at developing a complete platform for WBANs. As communication system, a UWB-front-end is used and a MAC etiquette based on IEEE 802.15.3. This protocol also uses time frames divided into contention free periods (with time slots) and contention access periods (CSMA/CA).

A bendable and inexpensive WBASN respond suitable for a large vary of applications is urbanized in [12]. The major goal falsehood on attitude and movement detection applications by means that of sensible implementation and on-the-field testing. The sensors are WiMoCA-nodes, anywhere sensors are defined by tri-axial incorporated MEMS accelerometers. The IBBT IM3 centers on the research and completion of a wearable scheme for health monitoring [13]. Patient data is composed using a WBAN and examined at the medical center wear by the patient. If an incident (e.g. heart pulse problems) is sensed, a signal is sent to a health care practitioner who can observe and investigate the patient data tenuously. By assessment, every approach has numerous problems to be notion of in terms of the security services in WBAN. Further, there's a transaction between recital and security. Associated with these, another examination cluster has forced these two assorted cryptosystems in their analysis that offers security and privacy to WBAN. In [14], they believe that these two cryptosystems may be applied within the authentication of WBAN depleting every liability of them quickly. They primarily focus on the authentication within the overall coverage of WBAN together with in-, on- and out body to produce the robust and adequate security for WBAN.

1. Trust and Security Issues

Information security is mainly based on two factors trust and security. In WBAN each node involved in the packet transfer should assure that their neighboring nodes are trustful and secure. The mechanism which authenticate that the information about the source is actually who it claims to be. The Signatures and encryption mechanisms should need a provision to check by any nodes the sources of that information. Security and trust is strongly mutually dependent entity that cannot be alienated.

2. Proposed Methodology

We denote a WBAN by **B** and make the following assumptions.

A. Group Signature

Group Signature is a method for allowing members of a group to sign anonymously in a WBAN routing protocol. Group Signatures can be viewed as traditional public key signatures with additional privacy features. This approach is to run a group key agreement protocol at the beginning of every time slot and use the resulting group key as the common parameter and scalable. The more efficient approach is to use a group key agreement protocol in order to agree on the common parameter and group manager to generate and distribute this starting value. Group Signature scheme has group manager, who is response for adding new members and revoking signature of individual nodes in anonymity are given to a group manager.

Public Key G_{B+}: key this is common to all the nodes of a group B.

Private Key G_{N1-}: key which gives privacy for the data of individual node N1 in a group B where $N1 \in B$

Node *N1* may sign a message with its private key G_{N1-}, and this message can be decrypted via the public key $G_{B+}$by the other nodes in **B**, which keeps the anonymity of N1 [15].

B. Onion Routing

The main work of Onion routing protocol is establishment of connection and allowing for unidentified communication. During Route request the messages are repetitively encrypted the information whilst sent source to destination nodes of onion routers [16]. While in Route-Request has each intermediate nodes known as onion routers confiscates a layer of encryption and expose routing information when propels the message from destination to the source node. This technique preserves these intermediary nodes about knowing the origin, destination and content of the message. To pass a text message the routing onion is a data structure which forms hidden layer by encryption for forwarding a text message with consecutive layers of encryption. At the same time while back warding a text message it decrypts their corresponding layer and the original plaintext message viewable only to sender and recipient. It is end to end encryption and decryption process between the source and the destination in adversarial environment.

III.Proposed Work

Many trust management schemes have been proposed to evaluate trust values and most of the trust-based protocols for secure routing calculated trust values based on the characteristics of nodes behaving properly at the network layer. Trust measurement can be application dependent and will be different based on the design goals of proposed schemes. The trust management metrics include

overhead (e.g., control packet overheads), throughput, packet delivery ratio, packet dropping rate, and delay

Parameter	
CURVE	the elliptic curve field and equation used
G	elliptic curve base point, a generator of the elliptic curve with large prime order *n*
N	integer order of *G*, means that $n \times G = O$

1.Public key Cryptography

For onion routing the messages are encrypted and decrypted using PKC. In this paper we have used Elliptic Curve Diffie Hellman Key exchange algorithm.

2.Public Key Encryption

The goal of Public Key Encryption (PKE) is to ensure that the communication being sent is kept confidential during transit.

To send a message using PKE, the sender of the message uses the public key of the receiver to encrypt the contents of the message. The encrypted message is then transmitted electronically to the receiver and the receiver can then use their own matching private key to decrypt the message.

The encryption process of using the receivers public key is useful for preserving the confidentiality of the message as only the receiver has the matching private key to decrypt the message. Therefore, the sender of the message cannot decrypt the message once it has been encrypted using the receivers public key. However, PKE does not address the problem of non-repudiation, as the message could have been sent by anyone that has access to the receivers public key.

3. Elliptic Curve Diffie Hellman Key exchange algorithm

ECDH is used for the purposes of key agreement. Suppose two nodes, n1 and n2, wish to exchange a secret key with each other. N1 will generate a private key d_A and a public key $Q_A=d_AG$ (where G is the generator for the curve). Similarly n2 has his private key d_B and a public key $Q_B=d_BG$. If n2 sends its public key to n1 then able to calculate $d_AQ_B=d_Ad_BG$. Similarly if n1 sends its public key to n2, then he can calculate $d_bQ_A=d_Ad_BG$. The shared secret is the x co-ordinate of the calculated point d_Ad_BG. Any eavesdropper would only know Q_A and Q_B, and would be unable to calculate the shared secret

4. Digital Signature

The goal of a digital signature scheme is to ensure that the sender of the communication that is being sent is known to the receiver and that the sender of the message cannot repudiate a message that they sent. Therefore, the purpose of digital signatures is to ensure the non-repudiation of the message being sent. This is useful in a practical setting where a sender wishes to make an electronic purchase of shares and the receiver wants to be able to prove who requested the purchase. Digital signatures do not provide confidentiality for the message being sent. The message is signed using the sender's private signing key. The digitally signed message is then sent to the receiver, who can then use the sender's public key to verify the signature.

5. Signature generation algorithm

Suppose ***N1*** wants to send a signed message to N2. Initially, they must agree on the curve parameters (CURVE, G, n). In addition to the field and equation of the curve, we need G, a base point of prime order on the curve; n is the multiplicative order of the point G.

N1 creates a key pair, consisting of a private key integer d_A, randomly selected in the interval $[1, n-1]$; and a public key curve point $Q_A = d_A \times G$. We use $\times$ to denote elliptic curve point multiplication by a scalar.

For N1 to sign a message m, follows these steps:

1. Calculate $e = \mathrm{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-2.
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Select a cryptographically secure random integer k from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + rd_A) \bmod n$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s).

When computing s, the string z resulting from $\mathrm{HASH}(m)$ shall be converted to an integer. Note that z can be *greater* than n but not *longer*.

As the standard notes, it is crucial to select different k for different signatures, otherwise the equation in step 6 can be solved for d_A, the private key: Given two signatures (r, s) and (r, s'), employing the same unknown k for different known messages m and m', an attacker can calculate z and z', and since $s - s' = k^{-1}(z - z')$ (all operations in this paragraph are done modulo n) the attacker can find $k = \dfrac{z - z'}{s - s'}$. Since $s = k^{-1}(z + rd_A)$, the attacker can now calculate the private key $d_A = \dfrac{sk - z}{r}$.

6. Signature Verification Algorithm

For N2 to authenticate N1's signature, it must have a copy of its public-key curve point Q_A. N2 can verify Q_A is a valid curve point as follows:

1. Check that Q_A is not equal to the identity element O, and its coordinates are otherwise valid

2. Check that Q_A lies on the curve
3. Check that $n \times Q_A = O$

After that, N2 follows these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \mathrm{HASH}(m)$, where HASH is the same function used in the signature generation.
3. Let z be the L_n leftmost bits of e.
4. Calculate $w = s^{-1} \bmod n$.
5. Calculate $u_1 = zw \bmod n$ and $u_2 = rw \bmod n$.
6. Calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$.
7. The signature is valid if $r \equiv x_1 \pmod n$, invalid otherwise.

7. Protocol Design

To prevent the attack by malicious node, the identity information like IP address and Trust factor value has been used. This identity information is assigned to each node in initialization phase or when the node will be configured.

8. Trusted Anonymous Route Request

In the proposed scheme, a mechanism to check the next node whether it is trusted or not have been deployed where each node will be configured with the constant trust factor value, that value will be known to each and every node. The trust value is initiated in the route discovery phase. Each node keeps a constant trust value that will change in the RREP phase. Initially each node will be configured with the constant trust value 50 using node trust function. Source node broadcasts RREQ to neighboring nodes until a destination node or node having a route to destination determines, during this process hop count is initialized. If the current node is final destination it will check the trust value of the previous hop and if it is not the destination then it will forward the request to all its neighbouring nodes. If the current node is destination then it will evaluate the shortest path from destination to source. The proposed protocol can select the better path (trusted and shortest) using trust value and the number of hops. When the RREQ and RREP message are generated in the network, each node append its own trust value to the trust accumulator on these route discovery phase. Each node also updates its own routing table. The following formula can be used to evaluate the trusted and shortest path.)

$$\frac{sum.of.tursted\_values * \sqrt{no.of.hops}}{no.of.hops}$$

Sum of trust values Where, Sum of trust value = ∑ trustvalue (i)

1) Source Node: We assume that S initially knows the information about D, including its pseudonym, public key, and destination string. The destination string dest is a binary string, which means “You are the destination” and can be recognized by D. If there is no session key, S will generate a new session key KSD for the association between S and D. The following entry will be updated in S’s destination table:

Dest.Nym. Dest.Str Dest. Pub_Key Session Key ND dest KD+ KSD

Then, S will assemble and broadcast an RREQ packet in the format of (1). To simplify the notation, we ignore the timestamp information in the RREQ packet, i.e.,

$S \rightarrow *$: [*RREQ,Nsq, VD, VSD,Onion*(*S*)]*GS*− (1)

where RREQ is the packet-type identifier, Nsq is a sequence number randomly generated by S for this route request, VD is an encrypted message for the request validation at the destination

node, VSD is an encrypted message for the route validation at the intermediate nodes, and

Onion(S) is a key-encrypted onion created by S. The whole RREQ packet is finally signed by S with its group private key GS− here digital signature generation is done using elliptic Curve Digital Signature. The combination of VD and VSD works similarly to the

global trapdoor used in ANODR. We introduce VSD as

VSD = (Nv)Kv (2)

where Nv and Kv are two parameters created by S and sent to D for future route verification, Nv is a one-time nonce for theroute discovery, and Kv is a symmetric key.

The secret message VD is defined as

VD = _Nv,Kv, dest_KSD, {KSD}KD+. (3)

If D is the receiver of the message, D can decrypt the second part of VD by its private key KD− and then decrypt the first part by the obtained KSD. Otherwise, the receiver knows that it is

not the intended destination.

If S and D have already established KSD in a previous communication, the costly public encryption in the second part of VD can be eliminated, and then, VD is defined as

VD = _Nv,Kv, dest_KSD, pad (4)

where pad is a predefined bit-string that pads the message to a constant length. VSD and VD are separated in the RREQ format (1). For a non-destination node, it can use VSD as a unique identity for the route request. Now, we describe the encrypted onion Onion(S). S creates the onion core as follows:

Onion(S) = OKv (NS) (5)

where NS is a one-time nonce generated by S to indicate itself. The core is encrypted with the symmetric key of Kv and can only be decrypted by D via Kv.

After sending the RREQ, S creates a new entry in its routing table, which looks similar to the following:

Req.Nym. Dest.Nym. Ver.Msg. Next_hop Status Nsq ND VSD N/A Pending

Intermediate node: Intermediate nodes which receive the message from source node A and the further encryption, before send the message to the destination node E (2).

$I \rightarrow [P_B^-, G_B^-, O_B^-]$

Destination node: Destination node E receives the message from intermediate node and performs signature verification using Elliptic curve digital signature, which uses shared key generated by elliptic Diffie Hellman key exchange to access the secret message. The node E ready to route reply after receive the packet and reply to node A.

Route-Reply

The destination node makes sure to the source node the route is clear for transferring packet.

Destination node: Destination node D can send the route reply to the source node S in its original path

D ⟶ (RREP, Nr, ;⟨Kv,Onion (J)⟩KJD)

where RREP is the packet type identifier; Nrt is the route pseudonym generated by D; Kv and Onion(J) are obtained from the original RREQ and encrypted by the shared key KJD. The intended receiver of the RREP is J.

Intermediate node: Intermediate node J which receives the reply from destination node D and make decrypt the message to another neighbor intermediate node.

J ⟶Decrypt*⟨Kv,Onion(J)⟩,KJD)*

If J receives the RREP from D, J will navigate the shared keys KJD in its neighbourhood table, and try to use them to decrypt In case of a successful decryption, J knows the RREP is valid and from ND, and J also obtains the validation key Kv. Then J continues to decrypt the onion part Onion(J). J knows the next hop for the RREP.

Source node: S validates the packet in a similar process to the intermediate nodes. If the decrypted onion core NS equals to one of S's issued nonce, S is the original RREQ source. Then the Source node after receiving the trusted route reply from intermediate node for successfully packet transmission and ready to discover new packet in same path. This packet transfer is updated in routing table.

Anonymous Trusted Data Transmission

Now S can transmit the data to D. The format of the data packet is defined as follows:

S → D: (DATA; Nrt; ⟨Pdata⟩KSD)

where DATA is the packet type; Nrt is the route pseudonym that can be recognized by downstream nodes; the data payload is denoted by Pdata, which is encrypted by the session key KSD.

9.Trusted Routing Procedure

The routing algorithm can be implemented based on the existing on-demand ad hoc routing protocol like AODV. The main routing procedures can be summarized as follows:

1. During route discovery, two phases are performed
    1) First Before sending the RREQ the trust value of each neighbouring node is initialized to 50
    2) Second source node broadcasts an RREQ packet in the format to discover trusted neighbours.
2. If an intermediate node receives the RREQ packet, it verifies the RREQ by using its group public key, and adds one layer on top of the key-encrypted onion. It checks the trust value of the neighbor node and based on the trust factor the node decides its ne]xt neighbouring node for RREQ packet transfer. This process is repeated until the RREQ packet reaches the destination or expired.
3. Once the RREQ is received and verified by the destination node, the destination node assembles an RREP packet in the format, and broadcasts it back to the source node.
4. On the reverse path back to the source, each intermediate node validates the RREP packet and updates its routing and forwarding tables.
5. Then it removes one layer on the top of the key-encrypted onion, and continues broadcasting the updated RREP in the format.
6. When the source node receives the RREP packet, it verifiesthe packet, and updates its routing and forwardingtables. The route discovery phase is completed.
    1) The source node starts data transmissions in the established route in the format. Every intermediatenode forwards the data packets
7. by using the routepseudonym

IV. Experimental Result

A.Simulation Results An NS-2 simulator has been used to simulate the results. This proposed work undergoes two different types of simulation results. In the first type performance is compared based on their behaviors 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 AODV, ANODR, and AASR under different mobility scenarios.

Performance Metrics:

- Packet lost = Number of packet send – Number of packet received
- Throughput = successful packet received/number of packets erated
- End-to-end Delay=∑ (arrive time – send time) / ∑ Number of connections

2. Implementation

The Random Way Point Mobility Model describes the movement of nodes. In this simulation, files are categorized by number of nodes such as 10,30,50 and 70. The pause time is set to 10 sec. and maximum speed set to 5 m/s. The simulation time is set to 100 sec. and nodes are equally distributed in 800x800 m area. The comparison between AODV, ANDOR, AASR and TAASR are evaluated.

3. Results

In this section, the results have been analyzed using the three performances metric are Packet lost,throughput and end-end delay. To perform this scenario this work configured the mobile network with an average speed of 4ms. The number of malicious nodes varies from 0 to 9. The proposed TAASR 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 TAASR in average.While there is increase in number of malicious nodes the average throughput of four protocols decreases obviously. Throughput of the proposed TAASR is higher than the remaining existing protocols. Next to that AASR produces better throughput than ANODR and AODV.

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 record the performance results of the four protocols. 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 TAASR 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. 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.

V Conclusion

The trust and trust relationship among nodes can be represented, calculated and combined using an item *opinion.* In our TAASR routing protocol, nodes can cooperate together to obtain an objective opinion about another node’s trustworthiness. They can also perform trusted routing behaviors 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 without the need of requesting and verifying certificates at every routing operation. Our TAASR routing protocol is a more light-weighted but more flexible security solution than other cryptography and authentication design. It uses trust values to favor packet forwarding by maintaining 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, authorized node has high throughput and packet delivery ratio can be improved significantly with decreasing average end to end delay by increasing trust value.

References

[1] Poon, C. C. Y., Zhang, Y. T., & Bao, S.-D.. ”A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health,” Communications Magazine IEEE, IEEE, vol. 44, 2006, pp. 73-81, and doi: 0.1109/MCOM.2006.1632652.

[2] William, C., Tan, C. C., & Wang, H.. “Body Sensor Network Security: An Identity-Based Cryptography Approach,” Proc. ACM Conference on Wireless Network Security (WiSec ’08), ACM Press,2008, pp. 148-153, doi: 10.1145/1352533.1352557.

[3] Lim, S., Oh, T. H., Choi, Y. B., & Lakshman, T.. “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring,” 2010 IEEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing, 2010, pp. 327-332, doi: 10.1109/STUC.2010.61.

[4] Sharmilee, K. M., Mukesh, R., Damodaram, A., & Subbiah Bharathi,V.. “Secure WBAN Using Rule-Based IDS With Biometrics And MAC Authentication,” 2008 10th IEEE International Conference On EHealth Networking Applications and Services, EEE, 2008, pp.102-107, doi: 10.1109/HEALTH.2008.4600119.

[5] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, “System architecture of a wireless body area sensor network for ubiquitous health monitoring," Journal of Mobile Multimedia, vol. 1, no. 4, pp. 307-326, 2006.

[6] E. Jovanov, A. Milenkovic, C. Otto, and P. C. de Groen,\A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," Journal of NeuroEngineering and Rehabilitation, vol. 2, no. 1, pp. 16-23, March 2005.
[7] Moteiv [online] http://www.moteiv.com.
[8] Sentilla [online] http://www.sentilla.com.
[9] A. T. van Halteren, R. G. A. Bults, K. E. Wac, D. Konstantas,I. A. Widya, N. T. Dokovski, G. T. Koprinkov, V. M.Jones, and R. Herzog, "Mobile patient monitoring: The mobihealth system," The Journal on Information Technology in Healthcare, vol. 2, no. 5, pp. 365-373, October 2004.
[10] BANET project website [online] http://www.banet.fr.
[11] T. Falck, J. Espina, J. P. Ebert, and D. Dietterle, BASUMA - the sixth sense for chronically ill patients," in Wearable and Implantable Body Sensor Networks, 2006. BSN 2006. International Workshop on, Cambridge, MA,USA, 3-5 April 2006, pp. 57-60.
[12] E. Farella, A. Pieracci, L. Benini, L. Rocchi, and A. Acquaviva,"Interfacing human and computer with wireless body area sensor networks: the wimoca solution," Multimedia Tools and Applications, vol. 38, no. 3, pp. 337- 363,2008.
[13] IBBT IM3-project [online] http://projects.ibbt.be/im3.
[14] Jang, C. S., Lee, D. G., Han, J.-W., & Park, J. H.. "Hybrid security protocol for wireless body area networks," Wireless Communications and Mobile Computing, vol. 11, 2011, pp. 277-288, doi:10.1002/wcm.884.
[15] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. CRYPTO, Aug. 2004, pp. 41–55.
[16] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, " MASK:Anonymous On-Demand Routing in Mobile Ad hoc Networks, " IEEE Journal on Wireless Communications, vol. 5, no. 9, pp. 2376-2385, Sep.2006.
[17] R. Sudha, Dr. M. Devapriya, "Enhanced bio-trusted anonymous authentication routing technique of wireless body area network" in the Biomedical Research 2016 in Special Issue: S276 - S282, September 2016.
[18] R. Sudha, Dr. M. Devapriya, "A Survey on Wireless Body Sensor Networks for Health Care Monitoring" in International Journal of Science and Research (IJSR) in Volume 3, Issue 9, Page No. 1574 - 1578, September, 2014 .