Level based Fault Monitoring and Security for Long Range Transmission in WBAN

S. Kanaga Suba Raja
Assistant Professor, Department of Information Technology, Easwari Engineering College, Chennai, Tamilnadu, India

T. Jebarajan
Principal, Kings Engineering College, Chennai, Tamilnadu, India

ABSTRACT

In Wireless Body Area Network (WBAN), detection of fault node improves reliability and security for long range transmission. In this paper, we propose a combined approach for reliable and secured data transmission in WBAN. The proposed architecture consists of sensor nodes, relay nodes, the intermediate processing nodes and body area network (BAN) coordinator where the nodes are modeled to have direct and relay mode. The secured communication is ensured among the node and BAN coordinator by following simple protocol. The secure data transmission is proposed through authentication check, duplication check and faulty node detection. The proposed method is applicable to long ranges of transmission. It is also supporting a retransmission concept. Advancement of work to secure level checking provides a prohibition unwanted responses of WBAN and retransmission improves the probability of sending all most all data. Faulty node detection powers our security checking methodology further. By simulation results we prove that the proposed approach reduces the packet drop, energy consumption and the delay.

Keywords

level ID, body area network, node header, retransmission, authentication check

1. INTRODUCTION

Wireless sensor devices with ubiquitous dependent network connections granted several new applications in many fields. Among many, health care application is considered as the prominent one. [1] [2]

1.1 Wireless Body Area Networks (WBANs)

Wireless Body Area (WBAN) network includes a group of tiny sensor nodes capable of residing in human body. These sensors accumulate health data namely heart rate, body movement, ECG, pressure and body temperature. The accumulated informations are forwarded to the central device called base station or medical hub. This transmission may be done directly or by relying intermediate nodes. [3]

Each WBAN consists of exclusive medical hub; it works as gateway between WBAN and the internet. When compare with normal sensor nodes, a medical hub is embedded with more computation power. Hence, it is possible for a medical hub to process medical data and produce alarms. The interconnection between gateway and sensor node makes data transmission possible and this communication channel must be defended with appropriate security mechanisms. Any network can be an external network to associate medical hub and the back end server. Mostly, this communication network is wireless in nature. The back end server is a secure device that processes and maintains massive number of medical information of all patients. This processed information can only be accessed by authorized person such as doctor or medical staff. [4] [5]

In recent times WBAN is extensively used for monitoring human body. To achieve significant efficiency, IEEE 802.15.6 TG has introduced the standard for WBAN. In which, WBAN contains numerous sensors, actuators for pumping medicine, relay node and sink or gateway node. All the mentioned components are equipped with wireless radio interfaces and configured using star or multihop tree topology to compensate stringent power constraints. [6]

1.2 Applications of WBANs

WBAN is widely useful when a patient requires prolonged monitoring and treatment. By using WBAN this could be possible even at home. [7] [8] It offers reduced health care costs by shortening hospital stays, reducing hospital readmission rates, lessening frequent visits of medical professionals and by promoting health education. [9] [10] It makes possible of real time monitoring, early diagnosis and treatment for potential risky diseases from remote sites. [11] [12]Monitoring cardio vascular diseases, asthma, consulting doctors through tele-medicine or health care systems and monitoring diabetes will be the future applications of WBAN. [13] [14]

1.3 Security Threats in WBANs

The vulnerable nature of wireless channel results in security risks which interrupts the progress of WBANs. The various risks are described below. [6] [2]

- **Eavesdropping**

As WBANs uses the exposed nature of the wireless channel, the attacker can interrupt the radio communications between the nodes without difficulty. Hence the attacker eavesdrop packets in hop-by-hop manner and investigates the packet to get all important information.

- **Data Modification**

A section or whole of the eavesdropped information is either removed or restored by the attacker and send to the original receiver to attain illegal activities.

- **Impersonation Attack**

In case the attacker eavesdrops the legal data's of the BNC's and BN's, the obtained data's will be utilized to mislead BNs or BNC.

- **Replaying**

There is a possibility that an attacker can eavesdrop private information and again send it back to the original receiver after some period for the same reason of misleading the nodes in diverse cases.

- **Denial of Service**

During overflow of the network above the system capacity, the DoS attack occurs. This is related to effects caused by the activities of malicious or compromised attacks.

1.4 Fundamental Security Requirements in a WBAN

This section presents the fundamental security requirements of WBANs: [4] [2]

- **Data Confidentiality:** This property is needed to prevent the exposure of data. During medical use, the BNs forward the sensitive information such as health status of the patients. To make this transmission more confidential the data's are encrypted using the secret key which is shared among BN and BNC.

- **Data Authentication:** For both medical as well as non-medical applications, data authentication is essential. It is very much necessary for every BN and BNC to investigate whether the sensor nodes those send the data is trusted and not affected by any adversary. The data authentication is attained using the symmetric techniques in WBANs.

- **Data Integrity:** The information about the patient can be changed by an opponent while transmitting through insecure WBAN. When the network is short of the data integrity the attacker can change the patient information prior to reaching the BNC. The data authentication protocols help in attaining the data integrity.

- **Data Freshness:** This property guarantees the freshness of the data. This means ensuring whether data frames are well organized and not used again. The data freshness is categorized into two types namely weak freshness and strong freshness. Weak freshness ensures limited ordering of data frames and necessitates low-duty cycle BNs like blood pressure (BP). Strong freshness ensures complete data frame ordering and needs freshness during synchronization.

- **Security Management:** At the BNC, secure management is desired as it offers key distribution to BNs for permitting the process of encryption and decryption. The BNC securely inserts or eliminates the BNs during association or disassociation.

- **Availability:** This guarantees that the information about the patients is available to the physician all times. By either arresting or disabling ECG node, the attacker targets the WBAN's availability that results in loss of life. Hence it is better to sustain the BNs operation and during the availability loss, the operation should be shifted to other BN.

2 RELATED WORKS

The Sriram Sankaran et al. [15] have considered publisher-subscriber driven body sensor networks, a key enabler for the design and development of CodeBlue system. They proposed a key management scheme, IDKEYMAN, for this communication model using Identity-Based Encryption (IBE). IBE facilitates faster key set up in addition to incurring low overhead. They have used IBE to set up pairwise symmetric keys between publishers and subscribers. Their scheme preserves the confidentiality, authenticity and integrity of safety critical medical data while also being energy-efficient.

Their method has provided security and privacy support for publisher-subscriber driven wireless ad hoc body area networks, by presenting IDKEYMAN, a key management scheme using IBE.

Benoˆıt Latre et al [11] have presented a lightweight modular framework for body area networks (MOFBAN). In this framework, a modular structure is used which allows for a higher flexibility and improved energy efficiency. The authors investigated the challenges and requirements needed for sending messages in a WBAN and then discussd about using the framework while designing new protocols by defining the different components of the framework

Shrirang Mare et al [16] have proposed an adaptive security model in which nodes change the size of packet overhead dynamically when a node detects a possible forgery attack, thereby providing strong security and privacy in the presence of an adversary, but otherwise using a low overhead to minimize the energy consumption of the network.

The authors have demonstrated how to apply the adaptive security model to a class of privacy-preserving protocols to reduce their transmission overhead while preserving the security and privacy properties of those protocols, so that these protocols can be used in low-power m Health sensors.

3. LEVEL BASED FAULT MONITORING AND SECURITY FOR LONG RANGE TRANSMISSION IN WBAN

3.1 System Design

In our previous work [6], We have proposed a reliable and secure data transmission technique for wireless body area network. The work has been extended to a long range transmission. Still some security threat is coming as some unauthorized nodes are accessing the data send by another node. For that purpose we have designed a level id based transmission in our proposed method. We have focused on two steps. The first step is an authentication check of all the intermediate nodes and the second step checks whether duplicate node ID is present or not. There is an additional step present which is deciding which the faulty node is. The faulty node detection is important because it can prohibit the further error in the data transmission.

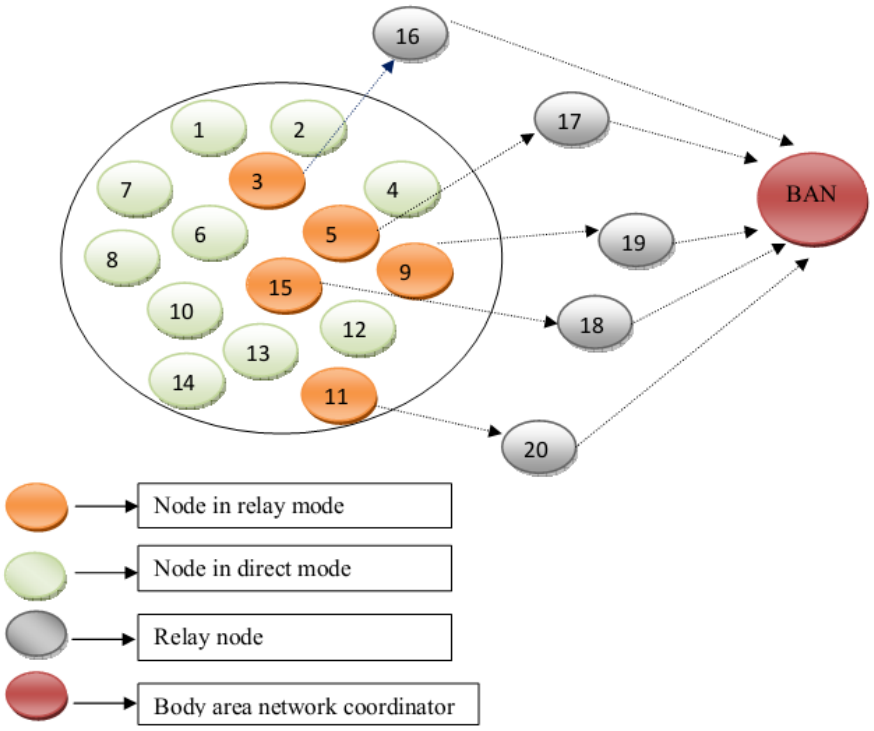

Fig. 1: showing the architecture of the wireless body sensor network

The Fig.1 can be represented based on the levels in the Fig.2.

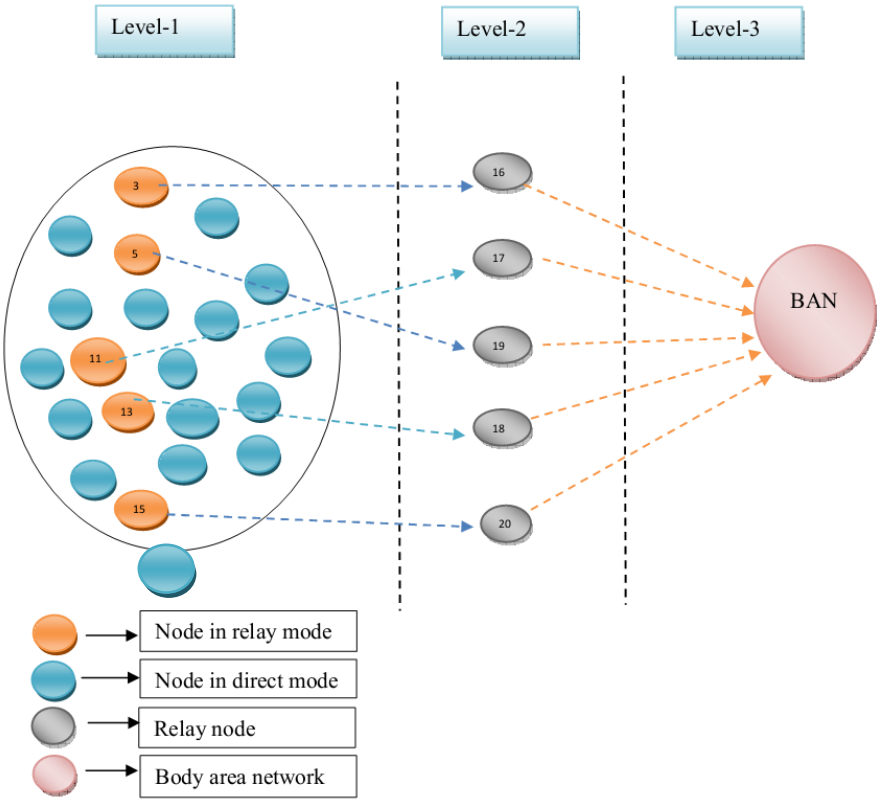

Fig. 2: showing Level Based architecture of WBAN

Here the structure can be divided into three levels. First level consists of nodes in relay mode or direct mode. Second one is relayed node and the third one is body area network. Here we have taken the first level nodes which are working as sensors. It can be taken as high level. Its importance is more valuable in the network. So we are giving the level Id is AAA. As single node is responsible for the entire range of operation; so the sender node should only carry the level id. The relay nodes are

the intermediate nodes. This level can be taken as B16, B17, B18, B19, and B20. At this level or level 2 there may be a single interference of relay node or the number of relay nodes extends to a number. The base paper is assigning the relay nodes on the basis of SNR ratio. The relay nodes are unable to send the message to WBN as it presents so far from the WBN.

Every node that may be a relay node or sensor nodes in direct mode or relay mode creates their unique id with the combination of level id and node ID. At the time of data transmission the sensor nodes have to transmit the data keeping the unique ids in their related field. During a certain time the relay nodes are able to transmit only one signal. The central control system of BAN (it may be the coordinator or any other device which can take the decision) maintains a data table to find the correct set of data transmission. All the relay nodes and the nodes participate in data transmission are priory authenticated by the central system of BAN. Every node has to add their unique id in the data packet. Two or more sensor nodes should not transmit the data packet through a single relay node. When a relay node is in transmission mode it shows a signal 1. If a relay node is in idle mode it shows signal 0. When the signal is 0 the sensor nodes are able to transmit the data packet through the relay node. One relay node is responsible for only data packet transmission. A body area network has different nodes as well as for the different jobs. The aim of data transmission is only for data transfer from the sensor node to the central system of the body area network. The body area network can refresh its data table after a certain difference of time. There is a relay node head present. This relay node is responsible for detecting the faulty node and informing all other nodes. The node head is generated by the decision maker of body area network at the time initialization of network

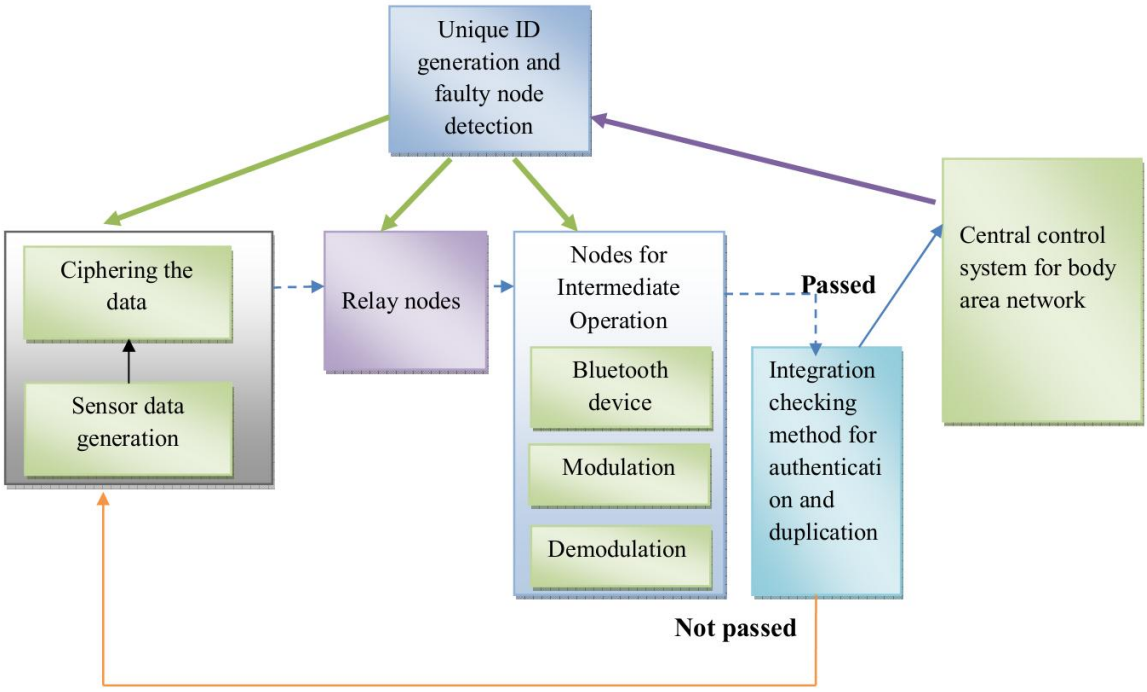

Fig 3. showing the architectural view of the security checking

3.2 Authentication of Intermediate Nodes

Two types of tables are present at a node in BAN who can take decision. The first table just keeps the node id in it. The table is given below. At the time of getting of the data all nodes id present had to go through it.

Table 1: showing authentication check of nodes

NODE ID	AAA12, AAA32, B15, B16, B18, B20 …

When a central system of body area network gets a data packet, it extracts the sender node ID and the intermediate node field IDs from the data packet. All the IDs are matched with the authentication table mentioned above. If it matches with the any one of the IDs then the message is further proceed. If any match is not found the message is simply discarded. The id should contain only the level one id. If so the body area network accepts the message packet.

3.3 Duplicate Checking

For the long range data transmission we have used the following data packet configuration. In the described case when a node wants to transmit its data packet to a distant node it changes its data packet configuration. The data packet at the sender is given below

Table 2: showing A data packet carrying different type of information

Sender ID/ signature	Destination	Data	Other info	Reserved	Flag

The sender sends the data-packet to the end points with the above described method. At the sender node the flag field is set to one (on). Here flag on indicates that the data can be modified by the end node and can be retransmitted. The end nodes abstracts the data from the data packet makes a new data packet. First the end node looks at the destination address. If the destination is in the range of the end node then the intermediate node set the flag to 0 and adds its id at the reserved place. Then

it is transmitted to the destination. If it is unable to find the destination then it adds it's id in the reserved field and keeps the flag on. Then it has to transmit the data packet to its maximum possible node except the sender. The second node also abstracts the data finds the destination address and checks its availability in the transmission range. If it is present makes the flag off and transmits the data. If the second node is also unable to locate the destination then in the regeneration of data packet it keeps the flag on and adds its id with the exiting ids and transmits it to the end nodes except the sender and all those nodes who's IDs are present in the reserved field.

The data packet model is given below

Table 3: showing the structure of data packets at intermediate nodes

Sender ID/ signature	Destination	Data	Other info	<Node id1/signature><Node id2/signature> …….	Flag

Table 4: showing the duplication checker table present at central control of body area network

Sender	**Intermediate node**	**Status**
AAA12	B12, B15, B45	Send acknowledgement
AAA34	B56, B87, B12	Send acknowledgement
AAA54	B47, B21, B65	Accept
…….	…….	……

The second kind of table which is used for sender and duplication check at wireless body area network is given above. The above table consists of three columns the first one is the sender field, the second one is intermediate relay node fields and the third field is the status field. The third field decides the response of that data packet. Duplication of ID in the second level

3.4 Detection of Faulty Node

Table 5: showing the retransmission data packet type sends by the sensor nodes

Sender ID/ signature (only having level 1 id i.e. AAA)	Destination (the last level id)	Data	Other info	<Node id1/signature added with level id > <Node id2/signature added with level id> …….	Flag	Retransmission flag

After sending the first data packet the sensor node starts a timer. The timer is fixed before the time of the installation of the network. If the sensor node is not getting any reply message from the central system before the timer becomes zero it retransmits the same message to the central system by adding a retransmission status. The sensor node has to send the data to the central system as every data has its importance in the body area network. Sensor network is also informing to the central system about the fault.

When the central system of body area network gets a data packet, the body area network deciphers it. If the central system of body area network finds a retransmission flag present then it generates a set of nodes ID which should be verified for the faulty node which is dropping any message. The set of ID is generated subtracting all the set of node ID present at the duplication checking table from the set of all the nodes that is present at authentication check table. The formula is given below.

Checking set=set of all nodes- set of nodes present duplication check table (1)

The set is transferred to the relay node head to find out the faulty node which is dropping the message.

When the node head gets the order to identify the faulty node with a set of node from which the node head has to identify the faulty node; the node head generates a message and transmits it to all nodes present in the set of the node IDs. It waits a certain time to receive the message from the entire nodes. If it is not getting any message from any node then the node is taken is the faulty node. It informs to the central system of the body area network the ID of the faulty node.

3.5 Overall Algorithm

Steps to follow

1. A sensor node generates the specific type of the data packet. The data packet is sent according to long range transmission. The sender node starts the timer.
2. Before the timer becoming zero if the sensor node is not getting an acknowledgement then it regenerates the same data packet. The sensor node sends the data packet with a retransmission flag.
3. When a relay node gets a message from a sensor node it accepts only if it is free that means at that time it is not transmitting any message.
4. When the central system of body area network gets a data packet it first checks its sender id. The id should contain only the level one id. If so the body area network accepts the message packet.
5. If the data packet contains two or more senders' ids then the central control system does not accept the data packet and sends request to both the data packets to resend it.
6. Then the body area network checks the intermediate fields. It gets the intermediate level fields and gets the level ids.
7. If there is any level 1 or sensor node IDs are present in the packet then it discards the data packet sends request to both nodes having sender node ids.
8. It checks the entire set of node authentication. The entire set node consists of nodes from relay nodes to last level modulation modes.
9. If the entire relay node involved in the data transmission process passes the authentication then it processed to the next step or it rejects the data packet and sends request to the sender node to retransmit it if the sender is an authenticated one.
10. Then the body area network keeps the sender node id and the intermediate node ids in a data table maintained with it.
11. Then it finds the duplicate values present in the data tables.
12. If there is any duplicate value for the relay node to the common PC; the central control system of the body area network discards the data packets which contain the id.
13. It sends a request packet to the sensor node to retransmit the data again.

14. If there is no second value present in the data table the data packet is accepted by the central system of the body area network.
15. The central system of the body area network looks at the data packet and finds if there is retransmission flag present. If the retransmission flag is present the central system orders to the node head to check the correctness of the all the relay nodes.
16. For checking the correctness of the node the central control system of body area network sends a set of node id which should be verified. The set of node IDs contains the node ID which is not present in the duplication check table.
17. The node head (this is generated by the decision maker of body area network at the time initialization of network) generates a random message and sends to the every node present in the set send by the central control system.
18. If the node head is not getting any message from any node then the node is chosen as faulty node. The node head informs to central control system.
19. The central system orders all other nodes not to deal with the faulty nodes.
20. In a certain time interval the above method should take place. The time period should be of Nano Seconds. So that other transmissions from the sensor nodes takes place.
21. After all the above operations the central system of the body area network refreshes the data table.

Algorithm

{Where n is the maximum no of node used in the data transmission}

1. For(int i=0 to n)
   Unique ID=ID +level ID;
2. Sensor nodes generate the data and cipher it.
3. The nodes pass the data through the relay nodes or in long transmission mode.
4. If the (relay nodes are in idle mode)
   a. Accept
5. Else
   a. Do not accept.
6. When the central system of body area network receives the message extract the sender id
7. If (sender ID € set to (sender id))
   {
   a. If (sender level ID==any level ID)
   {
   b. Call step-x;
   Exit (0);
   }
8. If (all other ids € set of (authentication IDs))
   {
   For node id: level 1 to level n-1
   If (any duplication)
   {
   Call step x;
   Exit (0);
   }
   Else
   Send an acknowledgement packet to the sensor nodes;
9. Get the data packet and check whether any retransmission data packet is present or not
10. If {the data packet contains any retransmission flag}
    Checking set=set of all nodes- set of nodes present duplication check table;
    Call error checking (checking set);

Step-x
{
Count the no of level-1 IDs;
For (int i=0; I<=count; i++)
Generate request packet ()
{
Destination= unique id (level id) [I];
Other information;
}
}

3.6 A Complete Example

A wireless body area network consists of a larger amount of sensor data. They are communicating to the required station through a number of intermediate stages. The first stage consists of the sensor nodes. The second stage is relay nodes. The third stage may contain Bluetooth devices or cell phones. The next stage is home PC which may be a part of the large group area which is connected to the hospital or research through the internet. A simple architecture is given below.

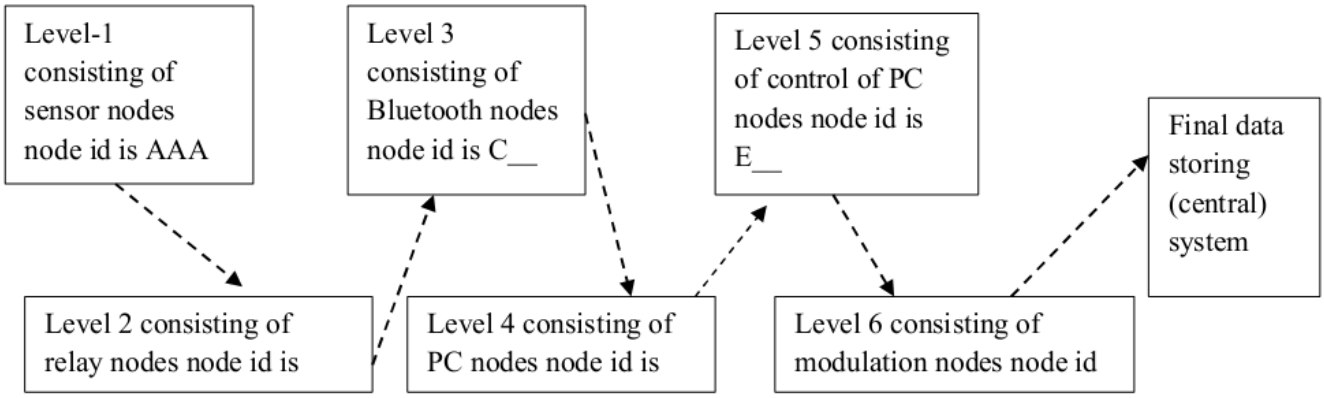

Fig. 4: showing data flow through different to reach at the central system

There are many methods present for the authentication of a new node enters in the network at the central system. Ciphering the data at the sensor node and deciphering the data on the central system increase the probability of the error control. For this

solution the function used in the central system is just the inverse of the function used at the sensor node for cipher the data. There are few methods present [17] for key generation and cipher the data. The nodes present at the intermediate level should not have the quality to decipher the data. Here level 1 is for the sensor nodes. So it needs a large value of id in it. Every data packet received by the central node should have only one level 1 id that is in here AAA. It should be at sender field only. If the id is present at the intermediate field then it simply discards the message and sends the acknowledgement packet to the sensor node to resend the data. The second level consists of the relay nodes. Many relay nodes can be present for long range of data transmission. These all nodes should be registered with the central system. Many relay nodes IDs can present at the intermediate nodes. Only one single Bluetooth devices are required for one data packet data transmission. So one id should present having C__ field in the data packet. Only one PC can be is able to work as intermediate between the Bluetooth device and the modulation device. The modulation device can carry its own technique to send the data in the group. It has its own security checking method. So the modulation device id can have multiple copies in receiver field. When we are having data packet given below

Table 6: showing in color the field needed to verify at central control system

Sender ID/ signature (only having level 1 id i.e. AAA)	Destination (the last level id)	Data	Other info	<Node id1/signature added with level id > <Node id2/signature added with level id> ……	Flag

For the security verification we have used the following table.

Table 7: showing the authentication checking table present at central system

Sender	**Intermediate node**	**Status**
AAA12	B12,B15,B45,C14,D23	Send acknowledgement
AAA34	B56,B87,B12,C15,D39	Send acknowledgement
AAA54	B47,B21,B65,C6,D23	Accept
……	……	……

Here the sender node cannot have multiple level ids. If any duplicate id is present the central systems just discard the data packet and send to all the entire set of nodes having node id AAA. All the nodes having the level ids AAA to F__ should be verified for the authentication phase. Nodes from B__ to D__ nodes should also pass through the duplication field. If any duplicate field is available the central system does not accept both the message and sends request to sender node to resend the message.

4 STIMULATION RESULTS

4.1. Simulation Setup

The performance of the proposed Level Based Fault Monitoting and Security (LBFMS) technique is evaluated using NS-2 [18] simulation. A network area of 50 X 50 m is considered. The IEEE 802.15.4 MAC layer is used for a reliable and single hop communication among the devices, providing access to the physical channel for all types of transmissions and appropriate security mechanisms. The IEEE 802.15.4 specification supports two PHY options based on direct sequence spread spectrum (DSSS), which allows the use of low-cost digital IC realizations. The PHY adopts the same basic frame structure for low-duty-cycle low-power operation, except that the two PHYs adopt different frequency bands: low-band (868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length.

The simulated traffic is exponential with UDP source and sink. Table 4 summarizes the simulation parameters used

Table 8: Simulation Parameters

No. of Nodes	22
Area Size	50 X 50
Mac	IEEE 802.15.4
Transmission Range	25m
Routing Protocol	LSA
Traffic Source	Exponential
Packet Size	512
Rate	50,100,150,200 and 250Kb.
Simulation Time	30,50,70 and 90 sec.

4.2. Performance Metrics

The performance of LBFMS is compared with the SBAN scheme. The performance is evaluated mainly, according to the following metrics.

Average end-to-end Delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.
Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.
Packet Drop: It is the number of packets dropped during the data transmission.
Energy Consumption: It is the average energy consumption of nodes during the transmission.

The simulation results are presented in the next section.

A. Based on Rate

In our first experiment we vary the transmission rate as 50,100,150,200 and 250kb.

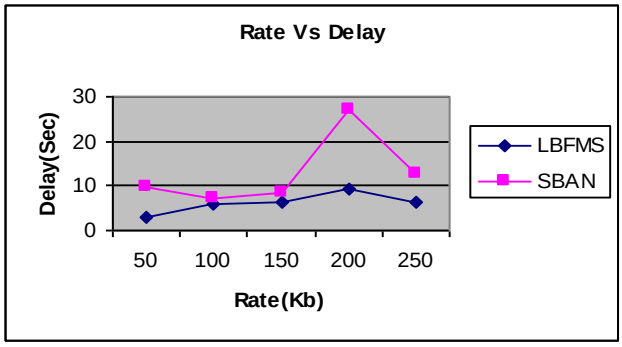

Fig 5: Rate Vs Delay

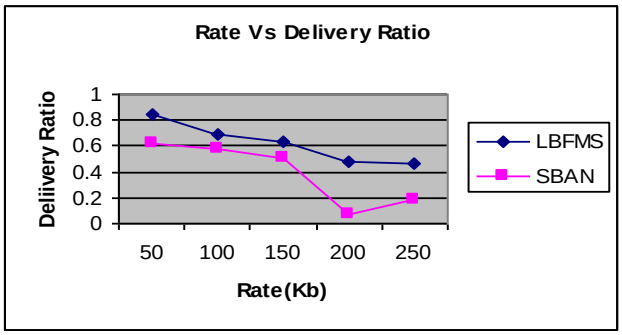

Fig 6: Rate Vs Delivery Ratio

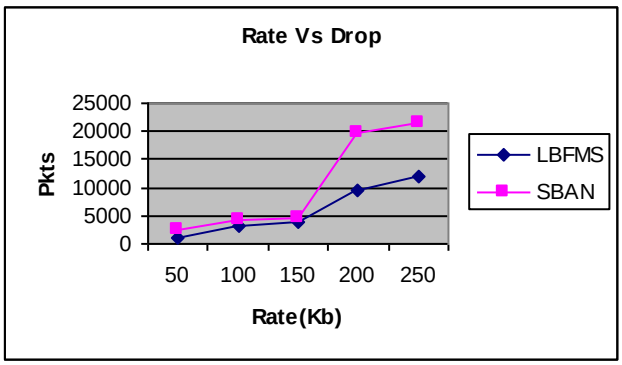

Fig 7: Rate Vs Drop

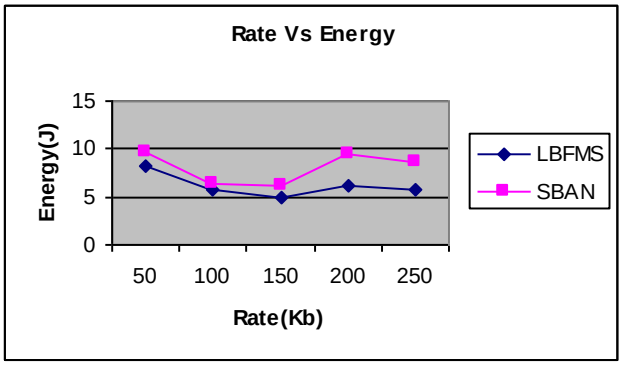

Fig 8: Rate Vs Energy

From fig. 5, we can see that the delay of our proposed LBFMS is less than the existing SBAN protocol.

From fig. 6, we can see that the delivery ratio of our proposed LBFMS is higher than the existing SBAN protocol.

From fig. 7,we can see that the packet drop of our proposed LBFMS is less than the existing SBAN protocol.

From fig. 8, we can see that the energy consumption of proposed LBFMS is less than the existing SBAN protocol.

B. Based on Time

In our second experiment we vary the time as 30, 50, 70 and 90sec.

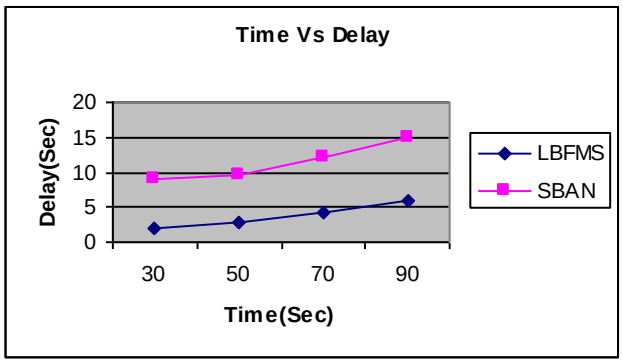

Fig 9: Time Vs Delay

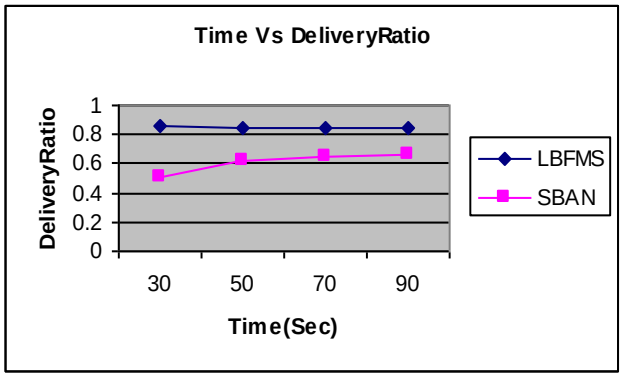

Fig 10: Time Vs Delivery Ratio

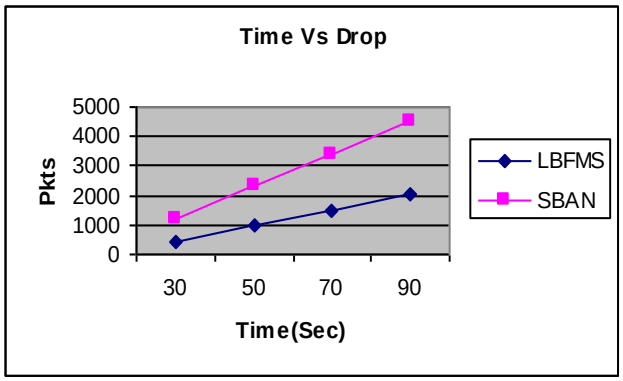

Fig 11: Time Vs Drop

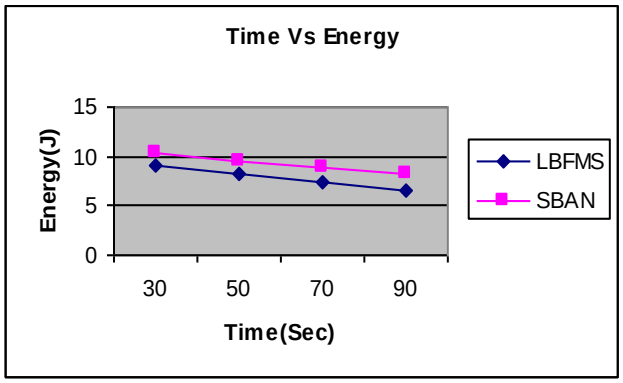

Fig 12: Time Vs Energy

From fig. 9, we can see that the delay of our proposed LBFMS is less than the existing SBAN protocol.

From fig. 10, we can see that the delivery ratio of our proposed LBFMS is higher than the existing SBAN protocol.

From fig.11,we can see that the packet drop of our proposed LBFMS is less than the existing SBAN protocol.

From fig. 12, we can see that the energy consumption of proposed LBFMS is less than the existing SBAN protocol.

5 CONCLUSION

This method shows a better way to find the correct packet to be processed. Many intermediate nodes can be involved in the current data packet transmission with the security checking. No duplication of data present. We can add up multiple levels in the transmission path to have more functionality. The relay node involved in the data transmission can process the data being in a different level. Interference in data is decreased at node level and duplicate data is eliminated at body area network level. This method is refreshed at a time interval of Nano second. Continuous data transmission of data packets can be possible in body area sensor networks. Here security is checked in two phases. In the first phase the nodes are passed through authentication stage and in the second stage the data packet pass through duplication check phase. This method is powered by adding level ids for different type of operations are done at the intermediate level. This method is introducing another step which is finding out the faulty node which is involved in dropping the message and prohibits further dealing with the node. By simulation results we have proven that the proposed approach reduces the packet drop, energy consumption and the delay.

The future work can include further clarification of faulty node at relay node level. This work can be implemented through some automation software.

6. REFERENCES

[1] Eliasz Kańtoch, Magdalena Smoleń, Piotr Augustyniak, Paweł Kowalski," Wireless Body Area Network System based on ECG and Accelerometer Pattern", IEEE International Conference on Computing in Cardiology, pp- 245 – 248, 2011

[2] Mohammed Mana1, Mohammed Feham2, and Boucif Amar Bensaber3, "SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network)" International Journal of Advanced Science and Technology Vol. 12, November, 2009

[3] Garth V. Crosby1, Tirthankar Ghosh2, Renita Murimi3, Craig A. Chin," Wireless Body Area Networks for Healthcare: A Survey" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012

[4] Song Wang, Jong-Tae Park," Modeling and Analysis of Multi-type Failures in Wireless Body Area Networks with Semi-Markov Model", IEEE Communications Letters, Volume 14 Issue 1, pp- Pages 6-8, January 2010

[5] Arie Reichman," Standardization of Body Area Networks", IEEE International Conference on Microwaves, Communications, Antennas and Electronics Systems, (COMCAS'09), 2009

[6] S. Kanaga Suba Raja and T. Jebarajan, "Reliable and Secured Data Transmission in Wireless Body Area Networks (WBAN)", European Journal of Scientific Research, ISSN 1450-216X ,Vol.82 No.2 (2012), pp.173-184 © EuroJournals Publishing, Inc. 2012

[7] Joonyoung Jung, Kiryong Ha, Jeonwoo Lee, Youngsung Kim and Daeyoung Kim," Wireless Body Area Network in a Ubiquitous Healthcare System for Physiological Signal Monitoring and Health Consulting", International Journal of Signal Processing, Image Processing and Pattern Recognition, 2008

[8] Vladimir Oleshchuk and Rune Fensli," Remote Patient Monitoring Within a Future 5G Infrastructure", Springer Science Business Media, LLC. 2010Springer Science Business Media, LLC. 2010

[9] M. Somasundaram and R. Sivakumar," Security in Wireless Body Area Networks: A survey", International Conference on Advancements in Information Technology With workshop of ICBMG 2011

[10] Cory Cornelius, David Kotz" On Usable Authentication for Wireless Body Area Networks", In USENIX Workshop on Health Security (HealthSec), August 2010.

[11] Benoˆıt Latr´e, Eli De Poorter, Ingrid Moerman and Piet Demeester," MOFBAN: a Lightweight Modular Framework for Body Area Networks", Proceedings of the 2007 international conference on Embedded and ubiquitous computing (EUC'07), pp- 610-622, 2007

[12] Muhammad Ahsan Habib, Aslam Khan, Mian Muhammad Omair, Junaid Imtiaz, Ahsan Jamal Khan," Ensuring Authentication and Freshness in Wireless Body Area Sensor Networks", International Conference on Circuits, System and Simulation,2011

[13] Paul Honeine, Farah Mourad, Maya Kallas, Hichem Snoussi, Hassan Amoud and Clovis Francis," Wireless Sensor Networks in Biomedical: Body Area Networks", IEEE 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 2011

[14] Cristina Tarin, Lara Traver, Narsic Cardona"Wireless Body Area Network for Telemedicine", ISSN 1889-8297, Waves, 2009

[15] Sriram Sankaran, Mohammad Iftekhar Husain, and Ramalingam Sridhar," IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks", 2008

[16] Shrirang Mare, Jacob Sorber, Minho Shin, Cory Cornelius, and David Kotz," Adaptive security and privacy for mHealth sensing" HealthSec, August 2011.

[17] Mohammed Mana1, Mohammed Feham1, and Boucif Amar Bensabe,"A Light Weight Protocol to Provide Location Privacy in Wireless Body Area Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011

[18] Network Simulator: http:///www.isi.edu/nsnam/ns