Cost Effective Energy Efficient and Secure Routing Protocol (CESR) for WBAN

Gurbeer Kaur, Navneet Kaur
Department of Computer Science
Baba Banda Singh Bahadur Engineering College
Fatehgarh Sahib, Punjab

ABSTRACT
With the increase in lifespan and sedentary lifestyle of people, there is an increase in demand for remote healthcare. Wireless body area network (WBAN) is a health monitoring technology in which sensors are attached to or implanted in various parts of the human for remote monitoring of different body parameters. The patient data thus obtained is private and confidential. The Cost effective Energy efficient and Secure Routing protocol (CESR) is an enhancement of Reliable Adhoc on-demand Distance Vector (RelAODV) protocol from literature, where the data is encrypted using RSA encryption scheme, thus enhancing its security. A cost function is formulates to select the minimum cost value forwarder node to enhance energy efficiency. Performance of the CESR is analyzed using MATLAB and the results show increase in reliability and security of the enhanced approach.

General Terms
Wireless Body Area Network (WBAN) is a wireless network of various sensing devices which could be implanted and embedded inside the body (Implants), could be placed on the body (Wearable Technology) or could be escorted devices that patients can carry in different positions as in clothes, pockets and many more.

Security is the detection and prevention of information against internal and external malicious and threats.

RSA algorithm is based on message encryption which is done through taking two prime numbers. Then product of these values has performed and generating number is treated as public key and private key used for encryption and decryption purposes.

Keywords
Wireless Body Area Networks Security, Cost Function.

1. INTRODUCTION
Wireless Body Area Network (WBAN) is a wireless network of various sensing devices which could be implanted and embedded inside the body (Implants), could be placed on the body (Wearable Technology) or could be escorted devices that patients can carry in different positions as in clothes pockets etc. Different types of sensors could be used for detection of several medical problems. These sensors collect different biological information of the body and inform the medical personnel without regard to the actual location of the patient. This provides location elasticity for patient [1].

The lifetime of WBAN is a major anxiety for these wireless networks. Most of the research is concentrated on increasing the longevity of network by minimizing the energy consumption.

WBAN is a growing technology; there are many challenges to meet before it is widely accepted. WBAN systems will have to approve unified data transmission between devices such as Bluetooth, Zigbee, etc. to support data exchange and device association [2]. Moreover, the networks will have to be accessible, guarantee effective route across networks and propose endless connectivity. The sensors comprised in WBAN should of light weight, less complex, power efficient, easy usage and can be reconfigured.

Moreover, the storage devices must assist remote storing and screening of patient data as well as access to external processing and analysis tools via the internet. If security is not accurately maintained, then it may be difficult for individuals to preserve privacy which is quite important for most of the patients as it contains personal data of patients [3]. The wireless connection used for body sensors have to reduce the interference of sensor node devices with other network devices present in the situation. WBAN applications are necessarily cost effective so that they could be widely used [4].

The WBAN should be wearable, light weighted as well as non-invasive. WBAN should not alter or delay the person's routine activities. The technology should be transparent to the consumer, i.e. it should execute its monitoring jobs without the user recognizing it [5]. The performance of a WBAN should be reliable. The data measured by several sensors should be accurate and remain unaltered even if the WBAN is turned off and on again. The wireless links should be determined and activate under different situations.

Security is one of the major challenges that need immediate attention. It is very important to make sure that the patient's crucial data is protected. WBANs is resource-constrained in terms of battery power, memory storage, communication ratio and computational ability, security keys advised for other networks may not be effective to WBANs. Freshness, validation, integration, and confidentiality of data along with accessibility and secure organization are the security requirements in WBAN. Medical records are very sensitive data and hereafter for a patient to trust the system, data needs to be sent privately and securely. Moreover, every detail captured by the sensors needs to be reliably transmitted to the concerned medical authorities. Another issue is the restricted battery power of the sensors. A sensor should not be overloaded with calculations as that will drastically drain the battery.

Reliable Ad hoc On-Demand Distance Vector (RelAODV) [6] is a power efficient methodology for secure transmission of patient data to the medical authorities and improves the reliability of the system.

This paper proposes a CESR protocol for enhancing the security of RelAODV by encrypting and decrypting information for transmitting the messages from the sensor nodes to the medical server to be observed by medical personnel using RSA algorithm. A minimum cost function based on distance and energy as parameters is proposed and the forwarder node is chosen based on the minimum value of the proposed cost function.

1.1. WBAN Architecture

A Wireless Body Area Network consists of a number of sensors to sense the biomedical conditions of human body and to transfer the collected information to the server which is deployed at the hospital. The data transmission is done by using Bluetooth or ZigBee technologies. The data is forwarded to the health care system at the server side.

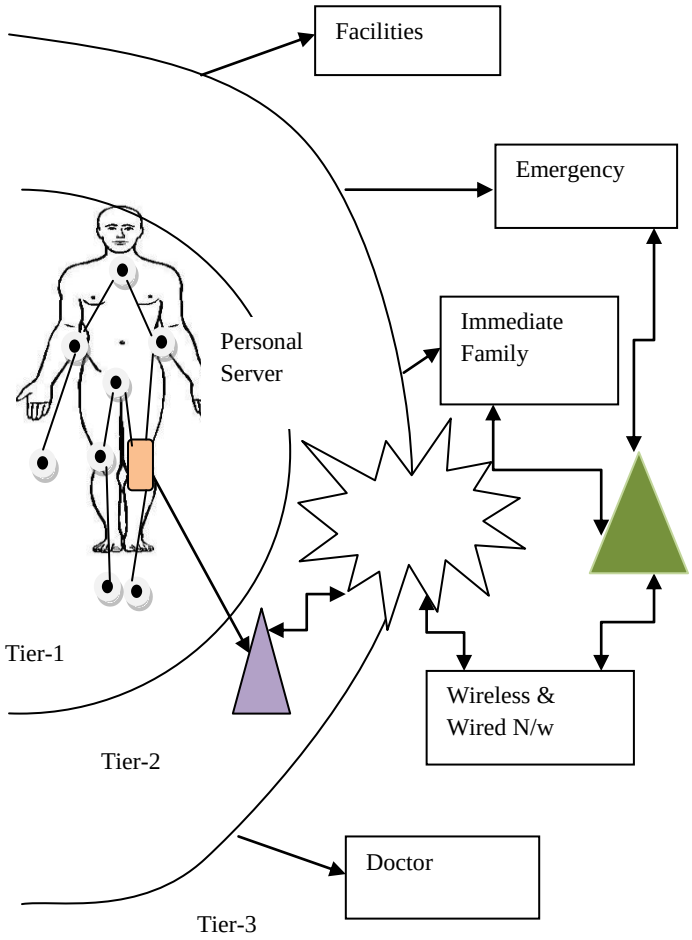

Fig.1: WBAN architecture

Fig.1 explains the architecture of wireless body area networks. The architecture of WBAN consists of three tiers as follows:

1. Tier-1:Intra-Body
2. Tier-2:Inter-Body
3. Tier-3:Extra-Body

1. **Tier-1:** In Intra-body Tier, the sensor nodes are embedded on the human body. Tier-1 depicts the network interaction of nodes and their respective transmission ranges (∼ 2 meters) in and around the human body. Each sensor node transmits this information to the BAN coordinator (BANC).In Tier-1, variable sensors are used to transfer body signals to a Personal Server (PS) which is located in Tier-1. The data is then transmitted to an access point in Tier-2.
2. **Tier-2**: In Inter-Body Tier, the BAN coordinator in the network is responsible for transmitting of data from the node to the server in Tier 2. Tier-2 communication aims to interconnect WBANs with various networks, which can easily be accessed in daily life as well as cellular networks and the Internet.
3. **Tier-3:** In Extra-Body Tier, the retrieved data has sent to the database or the medical server to take preferable actions by the corresponding physician relied in Tier 3. The sensor nodes are connected to the medical server through the internet which resides in the top of the hierarchy and responsible for monitoring the health of the wearer.

1.2 Classification of Messages

WBAN has been used for various applications, in particular for medical areas where sensors have embedded on the body of the patient that continuously monitors signals coming from the patient's body. Most of the information requires constant directions of the medical professionals, any abnormal variations in the signal should be considered rapidly. Thus, embedded sensors information can be derived into two categories as critical and non-critical types of messages.

1.2.1 Non-critical messages

Those messages which carry regularly monitored information such as body temperature, ECG, Pulse rate etc. are considered in this category. In comparison with critical messages, they sent to the network very frequently. In case of the consideration, the data is monitored by the professionals. For instance, if the temperature of the body is sent as 400 degree Celsius, then doctor will doubt on the system rather than doubting on the health of the patient. For this reason, these messages and type of information is categorized as non-critical messages.

1.2.2 Critical messages

Messages which require sudden attention of medical professionals comes in this category. These messages carry impulsive alarming data such as high and low variation in blood pressure, changes in heart rate etc. So, this type of data should be transmitted to the upper level of hierarchy. As compared to the non-critical messages, critical messages are not as frequent.

2. RELATED WORK

Amjad et.al [1] provides an overview of WBAN, its applications, challenges and security issues. WBANs are the facility of suitable security and privacy protection of the wireless communication intermediate. The data transmission between the sensor nodes should be kept confidential and integrity protected. WBAN is a system that provides smooth less expensive and ambulatory inspection during routine function works in close association with wireless body area network. It also provides better and cheap substitutions for achieving good health conditions. These systems reduce the huge costs associated with patients in hospitals as monitoring can take place in real-time even at home and over a longer period. Thus a great benefit goes to patients, physicians as well as the whole society.

Tuteja et.al [2] emphasized the need and importance of WBAN in several fields. Moreover the challenges that

WBANs are facing are also highlights here. WBANs will help in continuous monitoring of patients in medical fields, and early detection of anomalous conditions. Also, measurement of elementary signs like heart rate and blood pressure will enable patients to involve in outdoor activities instead of being entrapped at home or near medical services.

Movassaghi et.al [3] reviewed the on-going research in WBANs in terms of system architecture, address allocation, routing, channel modeling, PHY layer, MAC layer, security and applications. A comparison of WBANs with respect to WSNs and other wireless technologies is given. Additionally, a list of existing and applicable sensors, radio technologies and current research projects, open issues, and future work in WBANs is also presented. WBANs will allow for continuous monitoring of patients in medical applications, capable of early detection of abnormal conditions resulting in major improvements in the quality of life. Importantly, even basic vital signs monitoring (e.g. heart rate) can enable patients to engage in normal activities as opposed to being homebound or nearby specialized medical services.

Wang et.al [4] proposed a MAC protocol which is involved in the wireless body area network for conflict detection, priority control, timeslot assignment and order of transmission etc. Therefore design of MAC protocol plays vital role in WBAN for the reliability and efficiency of the network. In this paper a new MAC protocol has been proposed named as protocol-AD-MAC protocol which ensures energy efficiency and reliability of WBAN. This protocol helps in adopting dynamic nature i.e. dynamic priority control, dynamic time slot allocation mechanism and dynamic length allocation mechanism so that transmission reliability retains at the time of low latency and low power consumption. Simulation has been performed on the proposed protocol and results shows that AD-MAC protocol is better in terms of power consumption, delay and throughput in comparison with IEEE802.15.6 MAC and CA-MAC.

Dey et.al [5] proposed two key management schemes focusing on the independent generation of keys at the sender and the receiver. The need for the removal of exchange of keys in security mechanisms is fueled by the fact that if the security association, or the initial phase of exchange of keys or exchange of numbers used to generate the keys, is compromised, the whole communication becomes susceptible. In the proposed key generation / management schemes, the need for key exchanges is removed by using mechanisms that enable the sender and the receiver to generate the keys at their end. This ensures that the susceptibility of the communication at the security association phase does not apply when such a system is used.

Kamble et.al [6] proposed that security concerns while using WSN network with medical or health care systems. The success and reliability of such WBAN networks is depending on use of efficient and effective network security solution for protecting the patient's sensitive information. There are four core different types of security solutions discussed in this paper. They summarized their performances in terms of FRR, FAR, advantages and disadvantages and security requirements.

Raja et.al [7] proposed the Reliable Ad-hoc on-demand Distance vector (Rel-AODV) protocol to improve the reliability in the WBAN network. Patient-related data stored in the WBAN play a critical role in medical diagnosis and treatment. Hence it is essential to ensure the security of these data. The Secure and Reliable Data Transmission (SRDT) system addresses the most important security requirements of confidentiality and authentication and also improves upon transmission reliability compared to the existing protocols. This paper proposes the classification of nodes as direct and relay nodes to help in saving battery power and to reliably route packets to the coordinator. The paper also classifies the messages into critical and non-critical information to bestow more intelligence to the sensor nodes. It enhances the AODV routing protocol and proposed Rel-AODV for better reliability in routing packets. SRDT yielded better results in terms of packet drop ratio, packet delivery ratio and better management of transmission power, hence improving the overall reliability of the system. But one of the issues in adopting WBAN is the security and privacy of data. Medical records have sensitive information and hence for a patient, data needs to be sent securely. Moreover, every detail captured by the sensors need to be reliably transmitted to the medical authorities concerned. Another issue is the limited battery power of the sensors. A sensor should not be taxed to do so many computations as that will drastically drain the battery. In this work, authors also proposed a power efficient methodology for secure transmission of patient data to the medical authorities.

Chukwunonyerem et.al [14] investigates security and inter-node transmission energy for biosensors in a wireless body area sensor network (WBASN) system. Existing security solutions in WBASN have been observed to employ the pre-deployment of static authentication keys, which are unsecured and energy intensive. Electrocardiogram (ECG) biometric-based security scheme was developed using the peak location index (PLI) and inter-pulse-interval (IPI) of the heartbeat. The fast Fourier transform method was used to process individually selected ECG datasets of diabetic patients and the differential equation method was used to extract the ECG biometric features (PLI and IPI). Energy model of Chipcon CC2420 specification was used to evaluate inter-node energy consumption performance. The research results show that different PLI and IPI features were extracted from the ECG datasets and unpredictable authentication keys were generated. Node energy consumption performance evaluation showed a 25% reduction in energy consumption for successful inter-node transmission. The ECG feature keys generated were different and unpredictable at every instant, providing for inter-node communication security. Non-additional node energy for processing the authentication acknowledgment packets provided for inter-node energy consumption reduction.

Zhou et.al [15] proposed practical situation of cloud-assisted WBANs in m-healthcare social networks where patients traverse among blocks outdoors and WBANs are more vulnerable to sophisticated attacks including even node compromise attack. To solve the problem, a secure and privacy-preserving key management scheme resilient to both time-based and location-based mobile attacks is proposed by the cooperation of the mobile patients in the same social group for both hierarchical and distributed environment. It also protects patient's identity privacy, sensor deployment privacy and location privacy by exploiting the blinding technique and embedding human body's symmetric structure into Blom's symmetric key mechanism with modified proactive secret sharing. Especially, the computationally-intensive privacy-preserving key material updating is outsourced to the cloud server and the unchanged pairwise keys after key material updating dramatically saves the resources for energy-constrained WBANs.

Ibrahim et.al [16] proposed a protocol which is a lightweight anonymous mutually authentication protocol to mutually authenticate the sensor nodes with the controller node (hub) in a star two-tier WBAN topology. The protocol proved efficiency and achieved the necessary security requirements for a secure anonymous mutual authentication scheme.

Han et.al [17] proposed the Multi-valued and Ambiguous Scheme to capture data confidentiality in the Cloud-assisted Wireless Body Area Networks since it is the most important issue. The approach combining the scheme with existing encryption schemes provides a general paradigm for deploying applications. The obtained results show that secure data communications between the cloud and Wireless Body Area Networks can be achieved.

Table 1: Review of the related work proposed by different researchers

Author	Contribution	Limitations
Saurabh Dey et.al [5]	Key management scheme for the enhancement of security in WBAN	Limited to a single encryption algorithm
J. Chukwunonyerem et.al [14]	Fast fourier transform method is used to provide secure and energy intensive data	Extracted limited features of the heartbeat
Jun Zhou et.al[15]	Key management scheme which is durable to both time based and location based mobile attacks.	Excluded the method of dealing with patient's selfishness in corporation in order to defy mobile compromise attacks.
Maged Hamada Ibrahim et.al [16]	Secure protocol for star topology two tier wireless body area network	Cannot be implemented in multitier WBAN.
Nguyen Dinh Han et.al [17]	Multi-valued and ambiguous scheme which provides capturing of data confidentially in WBAN.	Focused on a single security parameter

After analyzing the literature survey, it has been concluded that the security of data in WBAN has been focus of many researchers. Several techniques have been proposed till date to resolve the problem of corruption of data. Most of the researchers focused only on the single encryption but in this paper, for the encryption RSA encryption algorithm has used which ensures the security and authentication of the data. In CESR technique critical and non-critical messages are encrypted using RSA algorithm which increases security and a cost function is used to select the best next hope node with the minimum value of cost which results in energy efficiency and reliability.

3. MOTIVATION

3.1 Need of Security

With the advancements of technology, WBAN has evolved. The crucial patient data is collected by various sensor devices and sent to the doctor remotely. This communication of health related information between sensor in a WBAN and over the internet to server is private and confidential and should be encrypted to protect the patient's privacy. Therefore, security becomes an important part in any such communication. Furthermore, medical staffs that collect data must ensure that the data is not corrupted by and indeed initiates from that patient. Security and privacy protection mechanisms use a considerable part of the available energy and should therefore be energy efficient and lightweight.

3.1.1 RSA Algorithm

RSA algorithm is used in Public Key Cryptography to encrypt the data to conserve its privacy. This algorithm is based on the mathematical fact proposed by Rivest, Shamir and Adleman and hence named RSA. Two private and public key are used to encrypt and decrypt the data for high level of security. Private Key is used for the encryption whereas public key is used for decryption. As the public key is generated through the product of two prime numbers so it will be difficult for the attacker to decode the message without having knowledge about the exact used prime numbers. RSA algorithm can be applied on WBAN for enhancing its security [18]. Security requirements of the WBANs are:

- Confidentiality
- Integrity
- Authentication

Algorithm of RSA for the proposed work is given below.

Algo 1: RSA Encryption and Decryption (Random Data)

Calculate p & q prime numbers

if p &q = isprime();

cal_e();

cal_d();

end

Perform Encryption

encdata(j)=RSAen(M(j), pk, e);

end

Perform Decryption

Decdata(j)=RSAdec(encdata(j), pk, d);

end

Where,M(j)= message need to be sent

pk,e= public key for encryption

pk, d= private key for decryption

3.2 Energy Model

In order to perform transmission of data between the nodes, firstly network has initialized where area of the network, no. of nodes in the network, initial energy and threshold are identified. After the initialization or setup phase, transmission phase starts where initially energy values of each node has

evaluated and will be updated after each transmission round. Residual energy has calculated after each transmission round to evaluate whether the cluster node can continue the transmission in the next round or not. With the aim of simulating the consumption of energy in the system, energy model has used.

The equations of the model are shown as:

ETx is transmission energy in Joules

ERx is energy consumed by the receiver in Joules

Eamp is the energy required by the amplifier circuit in J/bit.

EDa is the energy used in data aggregation in Joules.

$$E_{Tx}(k,d) = E_{Tx\text{-}elec}k+(E_{amp}kd) \ldots\ldots \ldots (1)$$

$$E_{Rx}(k) =E_{Rx\text{-}elec}k \ldots. \ldots. \ldots. (2)$$

Where d= distance between transmitter and receiver

E_{Tx} = Energy consumption per packet costs by Transmitter

E_{Rx} = Energy consumption per packet costs by Receiver

$E_{Tx\text{-}elec}$ = the per bit Energy Consumption Values for Transmitter

$E_{Rx\text{-}elec}$ = per bit Energy Consumption Values for Receiver

E_{amp} = The Amplifier type

K = Packet Length

4. MATERIALS AND METHODS

4.1 Network Description

The various parameters used for the simulation of CESR are listed below in Table 2.

TABLE 2: NETWORK PARAMETERS

S.No.	Network Parameters	Values
1.	No. of nodes	30
2.	Transmission power (dBm)	13.98
3.	Initial energy (joules)	16
4.	Threshold	3.2
5.	No. of simulation Round	100
6.	ETX(Transmission) (joules)	16.7*0.000000001
7.	ERX(Receiving) (joules)	36.1*0.000000001
8.	Emp(amplification) (joules/bit)	1.97*0.000000001
9.	EDA (joules)	5*0.000000001

Note: Transmission power should not exceed 13.98 dBm (decibel-milliwatt) [7] in real life but it is a simulation work so in this the transmission power is 18dBm.

4.2 Cost Effective Energy Efficient Secure Network Model

A network model for routing of important data from sensor nodes to destination node in a secure manner is required. The goal is to minimize the overall energy consumption of the network while not compromising its security. The cost function is used in the proposed work to define or select the forwarder node. The node which has minimum cost function will be chosen as forwarder node for the transmission of data packets from source to destination. The cost function has been calculated with respect to distance as shown in Eq.3

$$Cost\_fun\ (i) = distance(i)\ \frac{i}{(info\_sensor\ (i).E)}; \ldots\ldots\ldots (3)$$

Where distance (i) is calculated using Eq.2

$$distance\ (i) = sqrt\ \Big(\big(info\_Sensor(i).xd - (Sink.x)\big)^2 + \big(Info\_Sensor\ (i).yd - (Sink.y)\big)^2\Big); \ldots\ldots\ldots (4)$$

Where info_sensor- no. of nodes

Sink.x= x-axis of sink node

Sink.y= y-axis of sink node

Info_sensor(i).xd= x-axis of sensor node

Info_sensor(i).yd=y-axis of sensor node

Pseudo code for evaluation of cost function:

```
for 1:length(critical flag)
        ifinfo_sensor(i).E>0
        calculate cost function();
        end
end
ifcost_function=minimum
        choose forwarder node
end
```

EXAMPLE SCENARIO

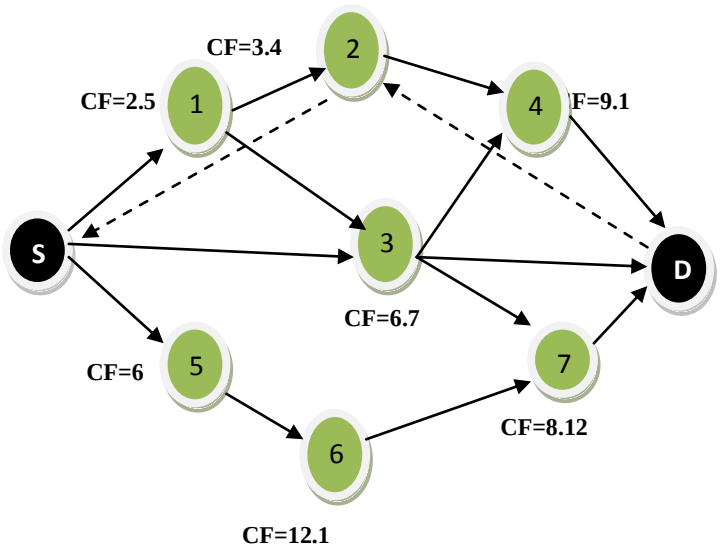

Fig.2: Proposed Routing Model

Sensor Node as Relay Nodes

Node Behaving as Source and Destination

Requested Nodes

Communication Nodes

Cf Value of Cost Function

Let us take a scenario of total 9 nodes as shown in fig.2 in which node S is a source node, D is a destination node and rest all the nodes as relay nodes. The routing algorithm chooses the sensor node with least value of communication cost from many relay nodes for the same destination. Before each data transmission once in 5 minute RSA algorithm is applied for encryption of data to enhance security.

Firstly, source node is sending request to node 1, 3 and 5. Node 1 has least value of communication cost, so it has to be chosen as next hope. Next nodes are 1, 2 and 3 for sending request. Node 2 has least value, so it is chosen as next hope. So the final path for sending request is node S, 1, 2, 4 and D.

5. RESULTS AND DISCUSSION

The proposed work aims to secure critical data nodes from the alterations during transmission by applying RSA algorithm on the critical data nodes in the network and chosing the next hope node by using the proposed cost function. The results are then observed and compared.

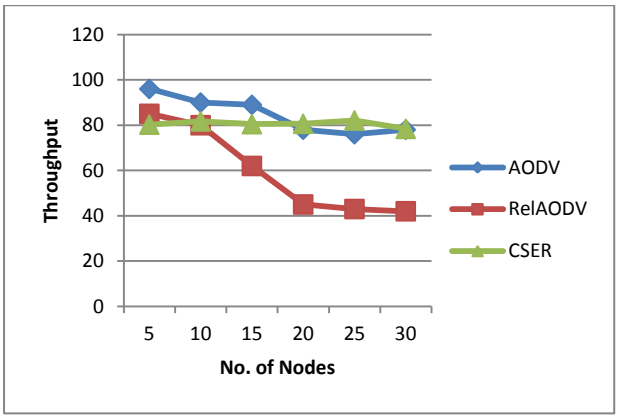

Fig.3: Throughput vs No. of Nodes

Fig.3 represents the successful transmission rate with respect to the increase in number of nodes. As the number of nodes increases in the network, the options to choose the next hope node using the cost function in the CESR also increases. There is a lesser probability of packets being dropped due to non-availability of forwarder node; hence the successful rate of transmission is higher throughput.

In case of AODV and RelAODV,as there is no mechanism that selects the best next hope, the increase in number of nodes, increases congestion and hence throughput decreases.

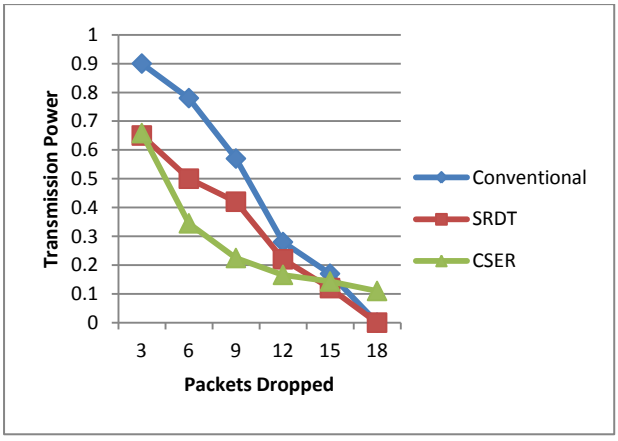

Fig.4: Transmission Power vs Packets Dropped

Fig.4 shows that number of packets dropped depends on the transmission power of the nodes. The more the transmission power, the lesser the number of packets dropped and hence more reliability. The proposed technique has fewer packets dropped as compared to SRDT with the same transmission power. Hence, the proposed technique is more energy efficient and more reliable as compared to SRDT as lesser the number of packets dropped, lesser is the requirement of retransmission of packets and lesser energy consumption takes place. Moreover, more successful transmission will result in more reliability.

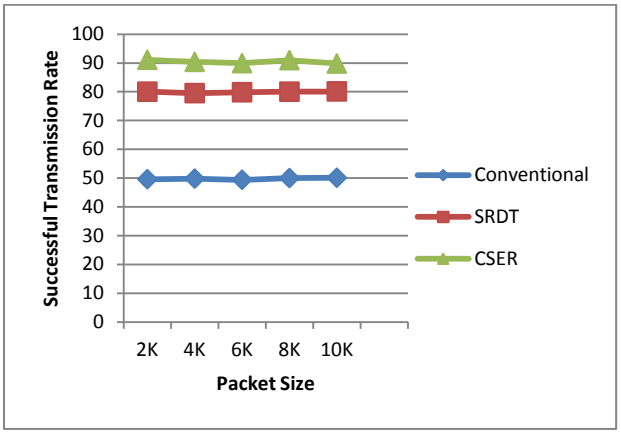

Fig. 5: Successful Transmissions vs Packet Size

The above fig.5 represents the transmission power in decibel-mill watts with respect to the packet size. The representation of the graph shows the performance of the proposed work is having more transmission rate as nodes which are chosen for the data transmission are much efficient that data is not dropping as much with respect to traditional approaches during transmission from source to the sink. In figure 5 throughput of the system is analyzed, the percentage of packets successfully transmitted against the total number of packets sent through the network is compared for the four schemes. A high throughput of above 80%is observed when proposed scheme is implemented.

6. CONCLUSION AND FUTURE SCOPE

Patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment. Hence it is essential to ensure the security of these data. RSA encryption algorithm has used for this work which ensures the security and authentication of the data. In the proposed technique critical and noncritical messages are encrypted using RSA algorithm which increases security and a cost function is proposed to select the best next hope node with the minimum value of cost which results in energy efficiency and reliability.

In future more features of WBAN can exploit by providing intelligence to the sensor nodes. To enhance the security level of patient data RSA algorithm will be used to encrypt the data as well as Run Length Encoding (RLE) will be used to reduce the size of data for more energy efficiency. This will be done by proposing a cost function which depends on delay, energy and distance of nodes.

7. ACKNOWLEDGMENTS

I would like to thank Baba Banda Singh Bahadur Engineering College for providing me best infrastructure for preceding my research work.

8. REFERENCES

[1] Syed Furqan Qadri;Salman Afsar Awan; Muhammad Amjad; Masood Anwar; Suneel Shehzad. Applications, Challenges, Security of Wireless Body Area Networks (WBANs) and functionality of IEEE 802.15.4/Zigbee. Sci.Int.(Lahore). 2013, 25(4), 697-702.

[2] Er. Shikha Tuteja, Rajandeep Kaur, Er. Ravinder Tonk. Need of WBAN: A Survey. International Journal of Engineering Research & Technology (IJERT). April-2015,Vol. 4 Issue 04, 1063-1065.

[3] Movassaghi, S.; Abolhasan, M.; Lipman, J.; Smith, D.; Jamalipour, A. Wireless Body Area Networks: A Survey. IEEE Commun. Surv. Tutor. 2014, 1–29. [Google Scholar]

[4] Savita Sindhu et.al. A Review on Wireless Body Area Network (WBAN) for Health Monitoring System: Implementation Protocols. Communications on Applied Electronics (CAE). March 2016, Volume 4– No.7.

[5] Raghav V. Sampangi, Saurabh Dey, Shalini R. Urs and Srinivas Sampalli. A Security Suite For Wireless Body Area Networks, International Journal of Network Security & Its Applications (IJNSA). January 2012, Vol.4, No.1, 97-116.

[6] Jyoti S. Kamble, Amarsinh V. Vidhate. Wireless Body Area Network Security, International Journal of Advanced Research in Computer Science and Software Engineering. December 2015, Vol. 5 Issue 12, 269-273.

[7] Kanaga Suba Raja, Usha Kiruthika. An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV. Wireless Personal Communications. 2015, 83.4, 2975-2997.

[8] Aashima Arya et.al. A Review: Wireless Body Area Networks for Health Care. International Journal of Innovative Research in Computer and Communication Engineering. April 2014, Vol. 2, Issue 4.

[9] Sapna Singla et.al. A Review Paper on Wireless Body Area Network for Health Care Applications. IJCSMC. October 2016, Vol. 5 Issue 10, 1 – 11.

[10] Pervez Khan et.al. Performance Analysis of WBAN MAC Protocol under Different Access Period. International Journal of Distributed Sensor Networks. October 2015, Vol. 11-No. 10 .

[11] Xin Qi et.al. MAC Protocol in Wireless Body Area Network for Mobile Health: A Survey and an Architecture Design. International Journal of Distributed Sensor Networks. October 2015, Vol. 11, No. 10.

[12] Jun Wang et.al. An all dynamic MAC protocol for Wireless Body Area Network. 11th International Conference on Wireless Communications. September 2015, 1 – 6.

[13] Luis Filipe et.al. Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review. International Journal of Distributed Sensor Networks. October 2015, Vol. 11- No. 10.

[14] J. Chukwunonyerem et.al. Development of key generation algorithmusing ECG biometrics for node security in wireless body area sensor network. European Research in Telemedicine. September 2016, 1-8.

[15] Jun Zhou et.al. 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks.

[16] Information Sciences. September 2015, Vol. 314, 255-276.

[17] Maged Hamada Ibrahim et.al. Secure anonymous mutual authentication for star two-tier wireless body area networks. Computer Methods and Programs in Biomedicine, October 2016, Vol. 135, 37-50.

[18] Nguyen Dinh Han et.al. A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks. Information Sciences. November 2014, Vol. 284, 157-166.

[19] Nitin Jirwan et.al. Review and Analysis of Cryptography Techniques. International Journal of Scientific & Engineering Research, March 2013, Vol. 4, No. 3, 1-6.