IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Compressed and Secure Energy Efficient Routing Protocol for WBAN

R.Singla[1*], N.Kaur[2]

[1*, 2]Dept. of Computer Science, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India

Available online at: www.ijcseonline.org

Accepted: 20/July/2018, Published: 31/July/2018

Abstract- The increase in average lifespan, growing population and sedentary lifestyle has increased the need for ubiquitous healthcare services. Wireless Body Area Network (WBAN) is one such approach which serves as a promising health monitoring service. Several sensors are implanted in or attached to human body to monitor the health status of the patients. The obtained physiological information from patient is transmitted to the doctor so that the patient will be constantly and remotely monitored. Thus, WBAN provides location flexibility to the patients. Nevertheless, security and privacy issues are one of the downsides in adopting WBAN to its full advantage. The medical records are private and confidential. Hence for a patient to trust WBAN, physiological information captured by the sensors need to be reliably transmitted to the doctors. Another issue is the limited battery life of sensors. It is crucial for WBANs to have a longer network lifetime to avoid constant recharging and replacement of nodes attached to a patient. This is possible by proposing energy efficient routing protocols for lowering energy consumption. These protocols should also reduce the network traffic by reducing the size of the data before transmission. The current work proposes an energy efficient approach for secure transmission of patient data to higher medical personnel. The proposed work extends the work of Rel-AODV protocol by considering compression model and cost based function having parameters of delay and residual energy. The results show that the proposed methodology is energy efficient and improves the overall QoS of the system.

Keywords— WBAN, Wireless Body Area Networks, Routing Protocols, Cost Function, Energy efficiency, QoS.

I. INTRODUCTION

In this modern era, there are many causes that have led to an unhealthy lifestyle. As a result the rate of development of diseases has increased. The increased cost of healthcare services and the growing aged population has introduced enormous challenges for governments, healthcare industry and healthcare providers [1]. Moreover, millions of people die from asthma, cardiovascular disease, cancer, obesity, diabetes and many more chronic diseases every year. The common issue with all chronic or fatal diseases is that numerous individuals experience the symptoms and have illness finding when it is too late. The research demonstrates that numerous diseases can be avoided if they are diagnosed in their in their beginning stages [2]. The miniaturization of sensor devices revolutionized the health care services. In order to meet healthcare demands, Wireless Body Area Network (WBAN) evolves as a promising solution.

According to the definition of IEEE 802.15.6 “WBAN is a communication standard optimized for low power devices for their operation on, in or around the human body to serve a variety of applications including medical, consumer electronics or personal entertainment and other" [3].

WBAN consists of numerous miniature and lightweight sensors. These sensors positioned on the body as small patches either integrated in to garments or embedded under the skin. This technology brings reasonable and efficient medicinal services for individuals that will enhance their quality of life. Due to continual health monitoring, patients are not compelled to stay in the hospitals for frequent check-ups. Thus healthcare costs are reduced [4].

WBAN is a very useful technology for youth, aged persons as well as physically challenged people. Besides medical purposes, WBAN finds its applications in entertainment, real time streaming, lifestyle and fitness [5].

The architecture of WBAN is illustrated in Figure 1. It consists of three tiers. In Tier-1, bio-sensors worn on or implanted in human body collect the data viz. electrocardiography (ECG), electroencephalography (EEG), temperature, blood pressure etc and send to the body coordinator (BC) using ZigBee and Bluetooth wireless technology [6]. Tier1 is also known as Intra-WBAN. Tier-2 is also known as Inter-WBAN comprises of a BC that sends the aggregated data from the patient to the nearby access point or sink node. The patient data is transferred from Tier-1 to Tier-3 through this gateway. Tier-3 is also known as

Beyond WBAN where the sink nodes transmit the collected data to the remote medical centre or doctor through internet [3].

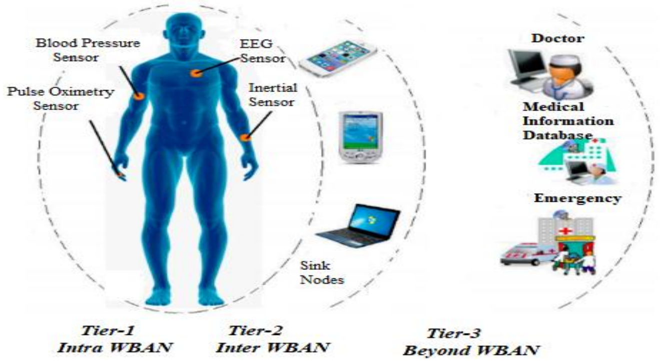

Figure 1 Architecture of WBAN

The physiological information of patients is strictly private and confidential. Therefore, communication of physiological information among sensors and over the Internet to servers needs to be secure. There is a need to encrypt the health related information to protect the privacy of patient [1]. Moreover, medical staff that gathers information should be sure that the information is not altered and actually generates from the patient. Furthermore, the physiological information of patients must not make available to unauthorized individuals. The malicious attacker can use the acquired information for illegal purposes. Therefore, security and privacy protection mechanisms are highly required in WBAN.

This paper proposes Compressed and Secure Energy Efficient Routing Protocol (CSEER) that enhances the energy efficiency as well as security by using RSA [7] and Arithmetic Data Compression Technique [8]. The performance of CSEER is evaluated and compared with Energy-aware Peering Routing Protocol (EPR) [9], Reliable Ad-hoc on-demand Distance Vector (Rel-AODV) [10] and conventional protocols such as AODV [11] and C-AODV [12] from literature.

Most of the secure routing protocols in existing literature were consists of single encryption mechanism that indirectly fails to maintain the security of the patient related information at a higher level. The main goal of proposed protocol is to achieve energy efficiency and high security. The proposed work uses a cost function to elect the next hop node on the basis of the amount of residual energy and delay. The proposed routing protocol has been evaluated using MATLAB in terms of energy consumption, throughput and packet delivery ratio**.** The results demonstrate that the proposed CSEER protocol is energy efficient as compared to existing routing protocols and slightly increased throughput.

The rest of the paper is organized as follows: Section II presents the review of related work from literature. Materials and methods used in proposed protocol are described in Section III. Section IV provides the working of proposed protocol. Results are discussed in Section V. Section VI finally concludes the paper.

II. RELATED WORK

Movassaghi et al. [1] reviewed the on-going research in the field of WBANs in terms of its architecture, routing of data packets, channel modelling and applicability to different applications. Characteristics inherent to WBANs have been explored with emphasis on topology, system architecture and types of WBAN nodes. The authors also presented the comparison of WBANs with Wireless Sensor Networks (WSNs) and other wireless technologies such as ZigBee, Bluetooth, Ultra Wideband, RuBee and many more. Data rates, power requirements and important issues associated with WBAN security has been described. Also, a list of existing bio-sensors, radio technologies and open issues in WBANs has been discussed.

Cherukuri et al. [13] proposed an approach in which biometrics derived from the human body are used to secure the key used in encryption processes. The biosensors collect information about vital body parameters from various parts of the body. The physiological information is of individual nature and is required to be secured. Lack of security may also lead to dangerous consequences. Distribution of keys is central to any security approach. This approach removes the need for costly computation and avoids unnecessary communications. The significant issues related with the utilization of biometrics include randomness and the error on measurement of the biometric. The authors also proposed solutions for problems raised by these two. Usage of error correcting codes and multiple biometrics are the key solutions for the problems of randomness and measurement errors.

Balasubramanyn et al. [14] proposed security solutions to prevent attacks on data freshness and maintain message integrity in WBAN. The authors utilize the measurement of permissible round trip time threshold as a feasible authentication solution to address the security threats in WBAN. For the detection of attacks on message integrity and data freshness, solutions are proposed. These solutions are suitable for the resource constrained WBAN because of less intensive computations and low memory space. A prototype framework in GloMoSim is implemented to evaluate the robustness of threat detection mechanism.

Raza et al. [15] proposed a new approach for security of information in wireless channel specifically during emergency conditions. Due to the area and resource constraints, security mechanism for biosensors should be lightweight. The authors proposed chaos based scrambling for communication of biosensors in case of emergency. Chaos based scrambling is lightweight with respect to AES. This method saves more than 99% processing time as compared to AES which is desired in emergencies. Thus this method provides immediate help to patient.

Perkins et al. [11] proposed an Ad hoc On-Demand Distance Vector (AODV) routing protocol for mobile nodes in an ad hoc network. This protocol offers low processing and memory overhead, quick adaptation to dynamic link conditions and low network utilization. AODV protocol facilitates self-starting, dynamic, multihop routing between participating mobile nodes to establish and maintain an ad hoc network. It ensured loop freedom by using destination sequence numbers at all times to avoid problems associated with classical distance vector protocols.

Manfredi et al. [12] introduced cooperative-based routing algorithm to guarantee a good performance trade-off between reliability and energy efficiency of WBAN. The authors proposed an enhanced cooperative AODV protocol (C-AODV) which distributes the traffic among nodes through a simple load balancing mechanism. C-AODV demonstrates the good performance in terms of scalability, reliability, packet losses, latency and energy efficiency.

Khan et al. [9] proposed a Body Area Network (BAN) network architecture for indoor hospital scenario and a new Energy aware Peering Routing protocol (EPR) that helps to reduce network traffic load, energy consumption, and improves BAN reliability. EPR consists of three parts (1) new Hello protocol, (2) neighbour table construction algorithm and (3) routing table construction algorithm. Both static and mobile patient scenarios are considered with fixed and variable number of packets to test the protocol. This protocol demonstrated better results by reducing the traffic load and energy consumption and simultaneously increasing the packet reception rate.

To improve the reliability and security of WBAN, **Raja et.al [10]** proposed a modified AODV protocol called Reliable AODV (RelAODV). The Secure and Reliable Data Transmission (SRDT) system addressed the security requirements of confidentiality and authentication. It enhanced the existing AODV routing protocol to obtain better reliability in routing packets. The classification of nodes as direct and relay nodes help in saving battery power and to reliably route packets to the destination. This protocol demonstrated better results in terms of packet drop ratio, packet delivery ratio and energy consumption.

III. MATERIALS AND METHODS

The proposed work has taken similar network model as RelAODV and introduces a multi-objective cost function to select the best next hop node. Based on this, secure and energy efficient routing mechanisms have been proposed for processing the vital information and similar scenarios as that of RelAODV are taken for the performance evaluation of proposed techniques.

A. Network model

Consider a hierarchical WBAN scenario comprising of thirty sensor nodes. These sensor nodes have equal power and communication capabilities. Sensor nodes forward the data to the Body Coordinator (BC) which is then sent to the doctor or physician. It is assumed that the position of sensor nodes is dynamic and has same transmission range. A wireless link can be established among the sensor nodes only if these nodes are present in the radio range.

B. Energy Model

The communication of among sensor nodes is at the expense of large amount of energy. The energy costs for data transmission, reception, aggregation and amplification is represented in equation 1 and 2.

$$E_{Tx\,(k,d,n)} = E_{Tx-elec}K + \left(E_{amp}\,nKd^{n}\right) \qquad (1)$$

$$E_{Rx\,(k)} = E_{Rx-elec}K \qquad (2)$$

where $E_{Tx-elec}$ is the energy dissipated per bit to run the transmitter circuit; $E_{Rx-elec}$ is the energy dissipated per bit to run the receiver circuit. K is the packet length and $E_{amp}$is the energy required for amplification of radio signals because the communication medium provides attenuation to radio signal in WBAN. n is the path loss coefficient in human body.

C. Compression model

The authors in [1] found that the energy consumption for data transmission is much greater than both encryption computations and encryption transmissions. If the transmitted data is compressed using arithmetic data compression technique then lesser number of bits needs to be transferred. This will result in reduced energy consumption for data transmission. Arithmetic data compression technique compresses as well as encrypts the data which enhances the security of WBAN.

D. Security model

RSA algorithm is used in Asymmetric Key Cryptography to encrypt the patient related data. This algorithm is proposed by Rivest, Shamir and Adleman and hence named RSA. Each sensor node has both private and public key to encrypt and decrypt data in order to implement high level of security in WBAN. Private Key is used for the encryption whereas public key of each sensor node is used for decryption process. As the public key is produced through the product of two prime numbers, it will be difficult for an intruder to decode the message without having the knowledge about the exact used prime numbers [16]. Thus RSA algorithm enhances the security of WBAN.

E. Delay Model

The value of path loss in human body is greater than its value in free space [3]. The delay in transmission of critical information may result in life threatening events. The physiological information of patients must be sent through a reliable connection and with minimum delay. The delay between source node (sn) to distance node (dn) can be calculated using equation 3.

$$Delay\ (sn, dn) = \frac{Distance\ (sn,dn)}{C} \tag{3}$$

where $Distance\ (sn, dn)$ is the distance between source node (sn) to destination node (dn) and C is speed of light.

Distance from source node (sn) to destination node (dn) is calculated using equation 4.

$$Distance\ _{(sn,dn)} = \sqrt{(x_{dn} - x_{sn})^2 - (y_{dn} - y_{sn})^2} \tag{4}$$

IV. PROPOSED PROTOCOL

The proposed CSEER protocol extends Rel-AODV protocol [10], by considering data compression technique to enforce security and reduce energy consumption. A cost function is used for selection of next hop node in multi hop data transmission environment. The methodology of CSEER protocol is discussed below:

A. Initialization Phase

The BC acts as sink node and has more energy as comparison to sensor nodes. Sink node broadcasts Hello Packets to construct a neighbour table. Hello packet contains short information about its ID, residual energy, location, and distance from sink node to recipient node.

B. Computation of cost function

In order to attain energy efficiency and minimize delay, CSEER protocol tries to select the best route followed by sensor nodes for transmission of data from source node to sink node. The proposed work uses a cost function to select the next hop node (i) in network as shown in equation 5.

$$cost\ function\ (i) = \frac{Delay\ (i)}{Residual\ Energy\ (i)} \tag{5}$$

where $Delay\ (i)$ is calculated using equation 4 and $Residual\ Energy\ (i)$ of node i is calculated as:

Residual Energy (i) =Initial Energy - Consumed Energy (i)

The next hop with minimum value of cost function is selected for data transmission. To balance energy consumption among sensor nodes, CSEER protocol elects new node in each round.

C. Scheduling and data transmission

The sink node assigns Time Division Multiple Access (TDMA) slots among the sensor nodes. All sensor nodes transmit the sensed data in their scheduled time slots to the next hop node that is selected on the basis of implied cost function. This selected node transmits the aggregated data to the sink node in its allocated time slot. If a sensor node has nothing for transmission, it switches to idle mode. Thus by using time scheduling, the energy dissipation of sensor nodes can be minimized.

D. Parameters Setting and Configuration

The various parameters used for the proposed work are listed below in Table 1.

Table 1. Simulation Parameters

Parameters	**Value**
Number of Nodes	30
Transmission Power	13.98 dBm
Initial energy	16 J
Threshold	3.2
Message Size	4000 Bits
No. of simulation rounds	6000
$\boldsymbol{E_{Tx}}$	16.7*0.000000001 (J)
$\boldsymbol{E_{Rx}}$	36.1*0.000000001 (J)
$\boldsymbol{E_{amp}}$	1.97*0.00000000 1 (J/bit)
Data aggregation energy ($\boldsymbol{E_{DA}}$)	5*0.000000001 (J)
Frequency	2.4 GHz
Sink Location	0.2m, 0.2m

V. RESULTS AND DISCUSSIONS

A comparison of CSEER is made with Rel-AODV [10], EPR [9], C-AODV [12] and AODV [11] using MATLAB simulator to show the effectiveness of CSEER in terms of energy consumption and throughput.

A. Number of Packets Dropped vs Number of Nodes

Figure 2 shows the comparison between packet dropping rate and number of nodes in the network. As the number of nodes increases, the number of packets dropped remain constant for proposing protocol where as the number dropped show an increasing trend in other protocols. Moreover, it is seen from the figure that CSEER has 17% least packet dropping rate as compared to 22.9% of Rel-AODV, 25% of EPR and 57% of conventional methods. This is owing to the use of compression technique while data transmission. The compression reduces the number of bits to be transmitted which will result in lower number of packets dropped as there will be no congestion in the network.

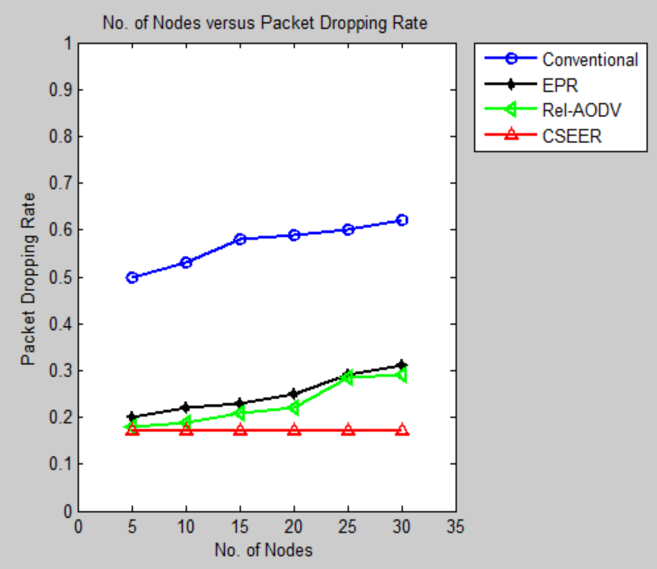

Figure 2 Packet Dropping Rate vs No. of nodes

B. Transmission power vs. Packet Dropping Rate

Figure 3 highlights the decrease in packet dropping rate with increase in transmission power. This is due to the fact that as the transmission power increases, the nodes will come in the range of the next hop node. In CSEER scheme, the node with minimum value of cost function based on delay and residual energy is chosen as the next hop node. This balances the energy consumption in the network and hence the packet dropping rate gets reduced. Moreover, it is seen from the figure that CSEER has 25.33% least packet dropping rate as compared to 33% of Rel-AODV, 41.1% of EPR and 46% of conventional methods with increase in transmission power.

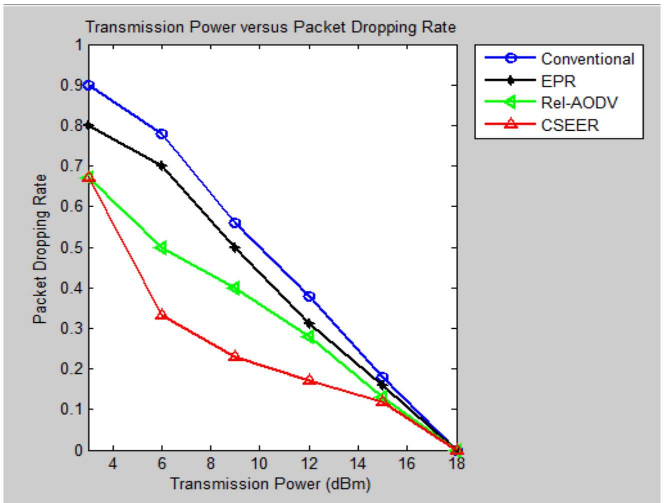

Figure 3 Transmission power vs. Packet Dropping Rate

C. Packet Delivery Ratio vs Nodes

Figure 4 shows the packet delivery ratio with increase in the number of nodes in the network. As the number of nodes in the network increases, packet delivery ratio decreases. More nodes in the network result in buffer overflow of sensor nodes as well as collision among transmitted data which will result in decrease in packet delivery ratio. Nevertheless, the throughput of the network is more than the compared approaches due to the compression technique employed as well as the proposed cost function.

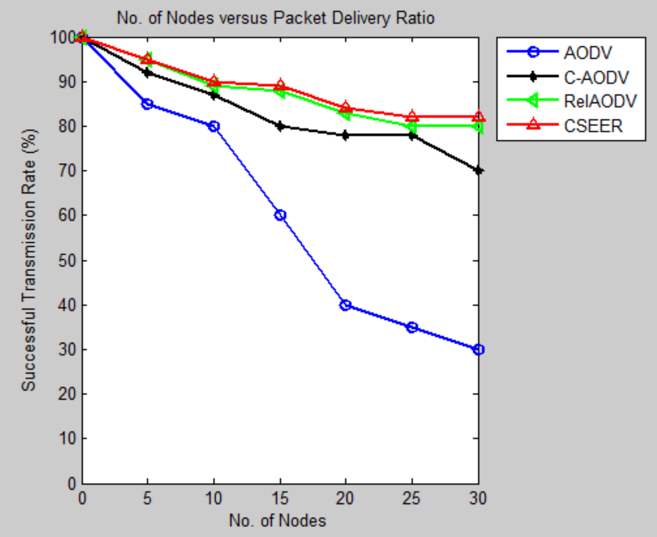

Figure 4 Packet Delivery Ratio vs Nodes

D. Throughput vs No. of Packets

It can be seen from Figure 5 that the proposed technique provides a throughput of 83% which is slightly greater than 80% of Rel-AODV but much remarkably than 60% of EPR and 49.2% of conventional protocols. This is owing to the use of compression technique while data transmission. The compression reduces the number of bits to be transmitted which will result in increase in throughput as there will be no congestion in the network. Moreover, the proposed cost function selects the next hop node on the basis of energy. More energy of nodes in the network result in lower number of packets dropped.

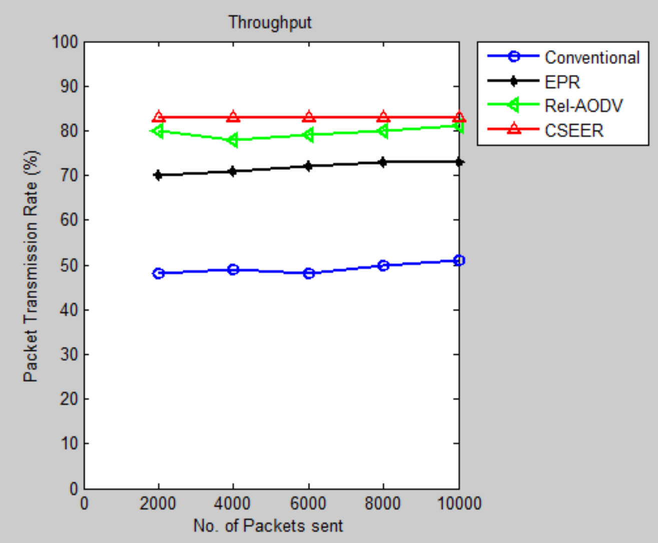

Figure 5 Throughput vs No. of Packets

E. Energy Consumption

The overall energy consumption of the network is shown in Figure 6. As CSEER scheme uses a cost function to select the neighbour node to achieve energy efficiency and to balance the residual energy among sensor nodes in the network, the overall energy consumption of CSEER is 30% lower than 40.3% of Rel-AODV, 48% of EPR and 75.5% of conventional protocols.

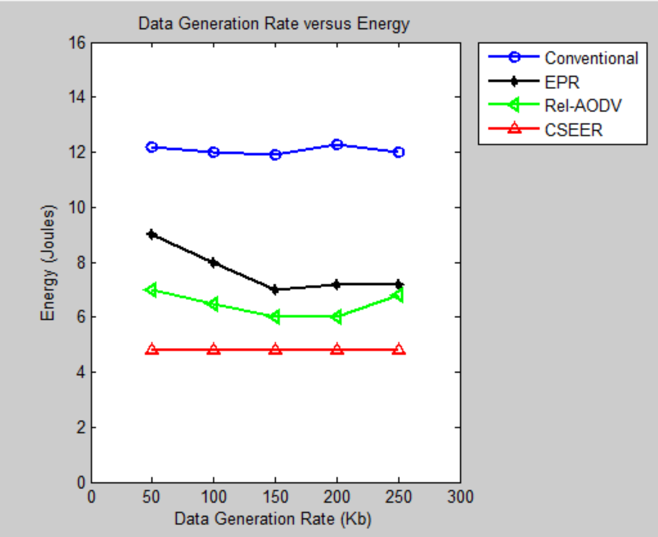

Figure 6 Energy Consumption

VI. CONCLUSION

This paper presents an energy efficient routing protocol (CSEER) for highly secure data transmission in WBAN. The proposed protocol utilizes two techniques. Firstly, an Arithmetic Data Compression technique for compression of patient data as well as to add a layer of encryption and secondly, RSA algorithm to provide more secure encryption to the crucial patient data. The proposed cost function selects the best next hop node for data transmission based on parameters such as delay and residual energy of node. The performance of CSEER is compared with Rel-AODV (SRDT), EPR and conventional protocols in terms of energy efficiency, throughput and packets dropping rate. The results demonstrate that CSEER protocol achieves 10-11 % more energy savings than Rel-AODV and is secure to use for medical purposes. Moreover, CSEER protocol achieves 3% more throughput than Rel-AODV and 10% low packet dropping rate with respect to transmission power. In the future, RSA algorithm used for encryption process can be replaced with its more appropriate variants such as Enhanced RSA, Elgamal or RSA-Elgamal.

REFERENCES

[1] S.Movassaghi, M. Abolhasan, J. Lipman, D. Smith, A. Jamalipour, " Wireless body area networks: A survey", IEEE Communications Surveys & Tutorials, Vol. 16, Issue.3, pp.1658-1686, 2014.

[2] D.Cypher, N.Chevrollier, N.Montavont, N.Golmie, "Prevailing over wires in healthcare environments: benefits and challenges", IEEE Communications Magazine, Vol. 44, Issue.4, pp.56-63, 2006.

[3] S.S. Javadi, M.A.Razzaque, "Security and privacy in wireless body area networks for health care applications", In Wireless networks and security, Springer, pp. 165-187, 2013.

[4] J.I.Bangash, A.H.Abdullah, M.H.Anisi, A.W.Khan, "A survey of routing protocols in wireless body sensor networks", Sensors, Vol. 14, Issue.1, pp.1322-1357, 2014.

[5] Pallvi, S.K.Gupta, R.K.Bedi, "An Improved Energy Efficient TDMA based MAC Protocol for WBAN", International Journal of Computer Sciences and Engineering, Vol.6, Issue.3, pp.34-39, 2018.

[6] S. Singla, K. Sharma, "A Review Paper on Wireless Body Area Network for Health Care Applications, International Journal of Computer Science and Mobile Computing, Vol.5, Issue.10, pp. 1-10, 2016.

[7] R. Kumar, A.K. Jain, "Simulation Survey of RSA and Its Variants", International Journal of Computer Sciences and Engineering, Vol. 5, Issue.7, pp.67-70, 2017.

[8] S. Boopathiraja, P. Kalavathi, , S. Chokkalingam, "A Hybrid Lossless Encoding Method for Compressing Multispectral Images using LZW and Arithmetic Coding", International Journal of Computer Sciences and Engineering, Vol. 6, Issue. 4, pp.313-318, 2018.

[9] Z.A.Khan, S.Sivakumar, W.Phillips, N.Aslam, "A new patient monitoring framework and Energy-aware Peering Routing Protocol (EPR) for Body Area Network communication", Journal of Ambient Intelligence and Humanized Computing, Vol. 5, Issue. 3, pp.409-423, 2014.

[10] K.S. Raja, U. Kiruthika, "An energy efficient method for secure and reliable data transmission in wireless body area networks using RelAODV", Wireless Personal Communications, Vol. 83, Issue. 4, pp.2975-2997, 2015.

[11] C. Perkins, E.Belding-Royer, S. Das, " Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561)", 2003.

[12] S. Manfredi, " Reliable and energy-efficient cooperative routing algorithm for wireless monitoring systems", IET Wireless Sensor Systems, Vol. 2, Issue. 2, pp.128-135, 2012.

[13] S. Cherukuri, K.K.Venkatasubramanian, S.K. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body", In Parallel Processing Workshops of the 2003 International Conference IEEE, Kaohsiung, pp. 432-439, 2003.

[14] V.B.Balasubramanyn, G.Thamilarasu, R. Sridhar, "Security solution for data integrity inwireless biosensor networks", In Distributed Computing Systems Workshops of the 27th International Conference on IEEE, Canada, pp. 79-79, 2007.

[15] S.F. Raza, C. Naveen, V.R. Satpute, A.G. Keskar, "A proficient chaos based security algorithm for emergency response in WBAN system", In Technology Symposium of 2016 IEEE Students', India, pp. 18-23, 2016.

[16] A.Negi, A.Goyal, "Optimizing Fully Homomorphic Encryption Algorithm using RSA and Diffie- Hellman Approach in Cloud Computing", International Journal of Computer Sciences and Engineering, Vol.6, Issue.5, pp.215-220, 2018.

Authors Profile

Ms. Ripty Singla obtained her B.Tech. (Computer Engg.) degree from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India in 2016. She is currently pursing Master of Technology in Cyber Security at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, India. Her current research interests include Wireless Body Area Networks.

Mrs. Navneet kaur obtained her B.Tech. (Computer Engg.) degree from Panjab Technical University, Jalandhar in 2000, M.E. (Computer Sc. & Engg.) Hons and Ph.D Degree from Panjab University, Chandigarh in 2007 and 2018 respectively. She is working as Assistant Professor in the department of Computer Science and Engineering in Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab. She is the Life Member of CSI and Member of ACM and IEEE. Her research interests include Wireless Sensor Networks, Wireless Body Area Networks and Wireless Adhoc Networks.