IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 16, 2021, accepted August 9, 2021, date of publication August 17, 2021, date of current version August 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3105600

Optimized Energy Efficient Secure Routing Protocol for Wireless Body Area Network

RIPTY SINGLA[1], NAVNEET KAUR[2], (Member, IEEE), DEEPIKA KOUNDAL[3], SAIMA ANWAR LASHARI[4], SURBHI BHATIA[5], AND MOHAMMAD KHALID IMAM RAHMANI[4], (Senior Member, IEEE)

[1]Department of Computer Science Engineering, Chandigarh University, Mohali, Punjab 140413, India
[2]Department of Computer Science Engineering, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab 140407, India
[3]Department of Virtualization, School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[4]College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia
[5]Department of Information Systems, College of Computer Science and Information Technology, King Faisal University, Hofuf 36362, Saudi Arabia

Corresponding authors: Navneet Kaur (navneet.sehgal@bbsbec.ac.in), Deepika Koundal (dkoundal@ddn.upes.ac.in), and Surbhi Bhatia(sbhatia@kfu.edu.sa)

ABSTRACT Fast growing age demographics, sedentary lifestyle, increasing chronic diseases, shortage of medical facilities and huge costs for healthcare treatment have arisen the need for ubiquitous as well as inexpensive healthcare services. A huge part of the cost in providing healthcare is utilized in frequent patient's visits and continual monitoring of the chronically ill patients. Wireless Body Area Network (WBAN) has offered promising outcomes for Quality of Service (QoS) in the healthcare system. Nevertheless, it is constrained with restricted battery power of sensors, security and privacy issues for its complete adoption. Henceforth, security, privacy and energy efficiency issues need to be addressed well with optimal solutions. The current work proposes an Optimized Energy Efficient Secure Routing Protocol (OEESR) that minimizes network congestion, provides secure data transmission and selects the most optimal route in the network. The performance of OEESR protocol is contrasted with other state-of-art protocols. The results show that OEESR is highly secure and achieves 90% throughput with 8.8% of overall energy consumption. It is having only 13% of packet dropping rate with respect to transmission power.

INDEX TERMS Compression, energy efficient, routing protocol, security, wireless body area network.

I. INTRODUCTION

In today's era, people are leading an unhealthy lifestyle due to bad lifestyle choices, lack of physical activity and inadequate relief of chronic stress, which further leads to the development and progression of chronic diseases. Thus, the need for healthcare systems and disease management is more than ever. According to the World Health Statistics 2020, the worldwide epidemic of COVID-19 will have an unknown consequence towards a healthier world [1]. The majority of human deaths were caused due to Non Communicable diseases (NCDs), accounting for 71% (40.3 million) of the overall deaths. In the last 15 years, these diseases have been the key causes of deaths worldwide as symptoms are not acknowledged or experienced in earlier stages by patients. There is need of a ubiquitous and cost effective healthcare system that could diagnose the diseases in their initial stages [2].

Wireless Body Area Network (WBAN) evolves as a cost efficient solution due to the miniaturization of sensor devices that revolutionized the healthcare services [3], [4]. WBAN consists of numerous minute, low powered and lightweight sensors having wireless communication capability. These types of sensors are located on the body, which are affixed either to the garments or at the skin or implanted under the skin (biosensors) [5]. The WBANs are employed to quantify the physiological factors of the humans such as heart rate, respiratory rate, Electromyography (EMG), blood pressure, pulse, body temperature, blood flow, electroencephalogram (EEG), oxygen saturation (SO_2), Electrocardiogram (ECG), glucose metabolism, metabolism rate and detect falls [6]–[11]. The sensors transmit this data to the base station termed as Body Coordinator (BC) for further processing and analysis. The BC send message to one or more access points such as cellular networks and further this data can be forwarded anywhere in the world through Internet Protocol (IP) [12]. Due to continual and remote health monitoring, patients are not compelled to stay in the hospitals for frequent

The associate editor coordinating the review of this manuscript and approving it for publication was Pietro Savazzi.

check-ups. Thus, WBAN provides location flexibility to its users with reduced healthcare costs [13], [14]. For ubiquitous and cost effective healthcare solutions, WBAN technology faces several challenges in terms of restricted battery power of sensors, dynamic network topology, stringent QoS requirements, varying data generation rate and size, and low transmission power. Therefore, there is a strong requirement to address these challenges to implement the WBAN effectively.

Energy management plays an important task to enhance the network lifetime of WBAN as battery power of sensors is limited [15]–[18]. Multi-hop communication is preferred for routing the data via intermediary nodes that goes offline early due to more communication [19]. Although, there are numerous mechanisms reported in the literature for increasing the energy efficiency of Wireless Sensor Networks (WSNs) but cannot be employed directly in WBAN due to its distinctive challenges and requirements [20]–[24].

The human vital signs are strictly private and confidential. Therefore, security and privacy protection mechanisms must have great importance in WBAN [25]. The security and privacy protection mechanisms need to be integrated with routing protocols in order to achieve confidentiality and authenticity of data packets. Therefore, the need for a new approach of route selection that is energy efficient, secure, reliable and maximizes the throughput of the network is highly recommended.

The contributions of the proposed work are as follow:

i. Categorization of WBAN routing protocols based on different characteristics. In each category, detailed discussion of prevailing research on WBAN environment has been carried out.
ii. Proposed an OEESR protocol to transmit data packets in a reliable and secure way
iii. Utilisation of optimized cost function based on Particle Swarm Optimization (PSO) technique for the selection of next hop node in an energy efficient way.
iv. Critical analysis of OEESR protocol with other state-of-art techniques present in literature.

OEESR protocol has been assessed and the performance is evaluated in comparison with Energy aware Peering Routing (EPR) [26], Reliable Adhoc On-Demand Distance Vector (Rel-AODV) [27], Compressed and Secure Energy Efficient Routing Protocol for (CSEER) [28] other conventional protocols such as Adhoc On-Demand Distance Vector (AODV) [29] and Co-operative Adhoc On-Demand Distance Vector (C-AODV) [30] in terms of throughput, packet dropping rate, energy efficiency and packet delivery ratio.

The Huffman compression algorithm is employed for the reduction of data packets in the network. To mitigate security attacks, RSA cryptographic algorithm is used for reliable and secure transmission of data packets in WBAN.

The rest of the paper is arranged as: Section 2 reviews the existing research work. The basic models used in proposed work are presented in Section 3. The details of the proposed protocol are reported in Section 4. Section 5 deals with the analysis and discussion of the simulation results. Section 6 finally concludes the paper.

II. RELATED WORK

The summarized overview of WBAN literature over the past 20 years is presented below:

A. WBAN TECHNOLOGY: A LEAP INTO FUTURE HEALTHCARE

In [31], the authors presented a review on WBANs with regards of its architecture, routing protocols, channel modelling, address allocation, layers, sensors, radio technologies and its applications. Khan *et al.* [32] introduced a unique and comprehensive cloud-based framework for mobile healthcare system owing to their secure nature. This system emphasized on secure intra WBAN communication and security of patient data. The framework consisted of i) biosensors embedded in or wearable by patient, ii) a client interface iii) personal server iv) a hospital community cloud and v) Remote Base Station (RBS). The results revealed that this cloud-based framework is a practical and provably secure solution for mobile healthcare systems. In [33], the authors presented the IoT (Internet of Things) platform for healthcare which is more accessible, provides timely services, having eminent popularity in marketplace and is expected to attain $1 trillion by 2025. Various domains associated with IoT, its technology stack, open research issues and challenges are also discussed. In [34], the authors considered IoT as an operative scenario on WBAN and reviewed state-of-the-art network topology and various applications of the WBAN based IoT. IoT healthcare faces several challenges viz. security and privacy, QoSs and resource management due to its unstructured architecture. Research gaps are reviewed and future aspects have been discussed. In [35], the authors proposed the WBAN big data processing framework. Google MapReduce model has used for processing of data and Hadoop and HBase for storing and analysing the WBAN big data. The infancy state of research in this area is still to address problems like interference and storage.

B. SECURITY AWARE ROUTING PROTOCOLS

The medical information of the patients is strictly private and confidential. So, the communication of medical information of the patient's needs to be secure. Lack of security may lead to dangerous consequences. Therefore, security and privacy protection methods must form an important part of WBAN. Singelée *et al.* [36] reported secure cross-layer Cascading Information retrieval by Controlling Access with Distributed slot Assignment (CICADA-S) protocol that is an expansion of CICADA. This paper concluded that privacy protection and security mechanisms have low impact on the throughput and energy consumption of WBAN. Raza *et al.* [37] presented a lightweight AES-128 cipher based on chaos scrambling for saves computation time more than 99% than ordinary AES-128 cryptographic algorithm. Raja and Kiruthika [27] proposed a Reliable AODV

(RelAODV) for secure and reliable transmission of patient data in an energy efficient way. The sensors are classified into direct and relay modes to achieve energy efficiency. RSA cryptographic algorithm is considered to provide security, privacy and authenticity to the patient data. RelAODV shown a low packet drop ratio and high-energy efficiency along with the incorporation of security mechanisms. To provide security to ECG signals, Lin *et al.* [38] proposed a chaotic map and a Multilayer Machine Learning Network (MMLN) that updates the network weights using back-propagation algorithm in Multilayer Perceptron Neural Network (MPNN). The authors identified that symmetric cryptographic protocols are prone to active and passive hacker attacks. To overcome passive attacks, chaotic map-based systems are preferred due to generation of random and non-periodic shared secret key [39]–[43]. This proposed solution turned out to be feasible as the mean CPU execution time for cryptographic process was very low and uses less computational resources than Chaotic Synchronization Cryptographic System (CSCS). Li *et al.* [44] reviewed 1-round WBAN authentication protocol reported by Liu *et al.* [45] and found several security flaws such as Key-Compromise Impersonation attack (KCI), DoS attack and guessing session key attacks. To fix the loopholes, Li *et al.* [44] has introduced an enhanced 1-round lightweight authentication protocol for WBAN with wearable devices and provably secure using formal and informal security analysis. The results have proven that this enhanced protocol attained additional security features with the same cost as Liu *et al.* [45] protocol. Sammoud *et al.* [46] proposed a new biometrics-based key establishment protocol for WBAN with minimal energy consumption and optimizes its performance. This protocol allows creating and sharing of a symmetric key based on ECG signal between two WBAN nodes. To remove dissimilarity between two recorded ECG signals, Bose-Chaudhuri-Hocquenghem (BCH) error correcting code is used to obtain identical sequences. Through informal security analysis, the authors proved that this protocol resists various security attacks viz. replay attack, masquerade parent node attack, key guessing attack, eavesdropping, impersonation attack, MITM attack and forward/backward security.

C. RELABILITY AWARE ROUTING PROTOCOLS

Javaid *et al.* [47] introduced the improved routing protocol named as Stable Increased-Throughput Multi-Hop Link Efficient (iM-SIMPLE) that extends SIMPLE routing protocol [48] by considering mathematical models and mobility for increasing the reliability and energy efficient routing for WBANs. Additionally, a cost function is introduced with parameters namely residual energy and distance for the selection of next hop node for minimizing the energy consumption in the network. iM-SIMPLE has improved the throughput and network stability period of WBAN. Kaur and Singh [49] has given two protocols namely Optimized Cost Effective and Energy Efficient Routing protocol (OCER) and Extended-OCER (E-OCER) to increase throughput along with the reliability of WBAN. These protocols has chosen the next hop node with least value of a cost-based function optimized using Genetic Algorithm (GA) having parameters viz. residual energy, link reliability. Manfredi *et al.* reported a Cooperative AODV protocol (C-AODV) [30] that has assured a better balance between reliability and energy efficiency of WBAN. It has distributed the traffic through load balancing mechanism amongst the sensor nodes and demonstrated the efficiency by considering reliability, scalability, energy, packet-dropping rate and latency of WBAN. Khan *et al.* [26] presented the Energy aware Peering Routing protocol (EPR) by considering the Body Area Network (BAN) architecture within the hospital. This protocol has lowered the network traffic, minimized the energy utilization and improved the reliability in the network. EPR consisted of three components (a) new Hello protocol, (b) construction of neighbour table and (c) construction of routing table. The test of EPR protocol has been performed on both scenarios of static and mobile patient. EPR has demonstrated the lesser energy consumption, reduced traffic load and better packet reception rate in the network simultaneously.

D. COMPRESSION BASED SECURITY AWARE ROUTING PROTOCOLS

Compressed and Secure Energy Efficient Routing Protocol (CSEER) [28] is a cost based routing protocol that has selected an effective route of data packets based on cost function. CSSER used the RSA algorithm for secure data packet transmission and Arithmetic data compression model to reduce network traffic. CSSER has shown the high energy efficiency and throughput. The authors of [50] proposed Compressed Sensing (CS) encoder device to measure physiological signals of WBAN to reduce the energy consumption of the sensor nodes. Two models are proposed: (i) virtual prototype with SystemC-AMS (ii) SPICE model and hardware prototype of CS encoder and saves 82.9% and 75% of the energy consumption of sensors. In [51], the authors proposed Discrete Wavelet Transform (DWT) based data compression technique at the BC, called as B-DWT. The optimal payload size is used for network longevity. The results reveal that B-DWT having high execution speed and low memory consumption at BC.

III. METHODS

The proposed WBAN optimization framework based on [27] and various models viz. the network model, compression model, security model and the energy model. Packets are transmitted to next hop node on the basis of proposed optimized cost function using PSO. The proposed protocol accesses the patient's medical information with high security, proposes an effective solution for the problem and evaluates the network parameters for proposed scenarios.

A. RELABILITY AWARE ROUTING PROTOCOLS

A hierarchical wireless dynamic WBAN model has been demonstrated in Figure 1. It is consisted of three communication tiers. In Tier 1, which is known as "Intra-WBAN

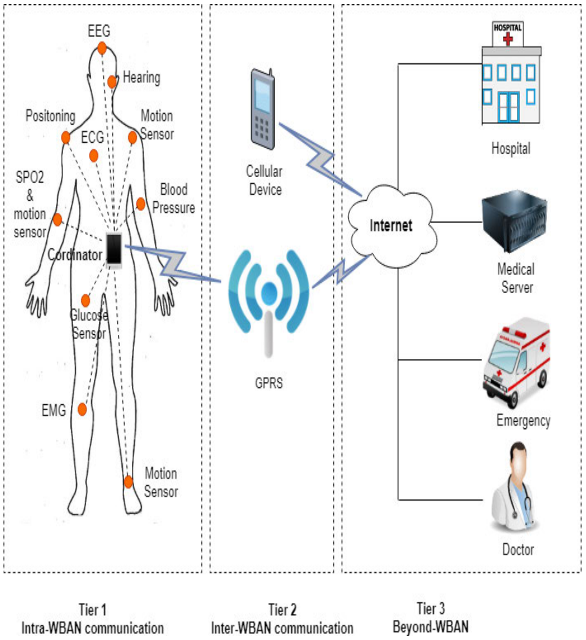

FIGURE 1. WBAN architecture [26].

communication'', sensor nodes are located on a human body for communicating with each other having transmission range approximately 2 meters and transmit the sensed data to the Body Coordinator (BC) [52]. BC is located either on garments of human or near to the human body. Tier 2 ''Inter-WBAN'' interconnects various WBANs with different networks such as Internet and cellular networks. Further, the collected data is processed and combined by the BC and transmitted to the access points (APs). The design of Tier-3 ''Beyond-WBAN'' is an application-specific.

The access points transfer the data of tier 2 to the physician/doctor. Zigbee network has been used for inter-WBAN and intra-WBAN communication. Internet or cellular networks are used for beyond-WBAN communication [49]. All WBAN sensor nodes have equal energy and communication capabilities and has the same transmission range. In the proposed work, a hierarchical WBAN scenario has been considered consisting of thirty sensor nodes. The position of sensor nodes keeps changing due to postural movements of body. Let $SN = SN_1, SN_2, SN_3, \ldots, SN_n$ denote the set of sensor nodes. The notations utilized in the proposed work has been listed in Table 1. All sensor nodes can establish wireless link only if nodes are in radio range.

B. ENERGY MODEL

The BC consumes more energy in comparison to conventional sensor nodes because of its additional aggregation activities and data processing. The communication in sensor nodes is at the cost of huge extent of energy. The consumption of energy per bit for operating the transmitter circuit has been denoted by $E_{Tx-elec}$. The dissipation of energy per bit for running the receiver circuit has been signified by $E_{Rx-elec}$. The energy required for amplification of radio signals has been represented by E_{amp} and the energy costs for data reception, transmission, amplification and aggregation of data packet of length k has been represented in equation 1 and 2. E_{amp} has been considered due to the attenuation to radio signal in communication medium.

TABLE 1. Notations.

Notations	Meaning
n	Total sensor devices in the network
ID_{dn}	ID of destination node *dn*
ID_i	ID of neighboring node *i*
Lo_i	Location of neighboring node *i*
CE_i	Total consumed energy by node *i*
Lo_{dn}	Location of destination node
$Dist_{sn,dn}$	Distance from source node *sn* to destination node *dn*
$Dist_{sn,i}$	Distance from *sn* to neighbor node *i*
$Dist_{i,dn}$	Distance from *i* to node *dn*
$Dist_{i,j}$	Distance between node *i* to node *j*
$Cost_i$	Cost of transmitting packets from *sn* and node *i*
L_{PDi}	Length of Patient Data at node *i*
L_{CDi}	Length of Compressed Data at node *i*
E_0	Initial energy of sensor nodes
RE_i	Residual energy of sensor node *i*
HP	Hello Packet
NT	Neighbor Table
NH	Next Hop
Pu_{sn}	Public Key of *sn*
Pu_{dn}	Public Key of *dn*
Pr_{sn}	Private Key of *sn*
Pr_{dn}	Private Key of *dn*
X_i, Y_i	X and Y coordinates of node *i*
ED	Encrypted Data
PD	Patient Data

$$E_{Tx}\left(k, Dist_{i,j}, PL\right) = kE_{Tx-elec} + \left(kE_{amp}Dist_{i,j}^{PL}\right) \quad (1)$$

$$E_{Rx(k)} = kE_{Rx-elec} \quad (2)$$

The proposed protocol has used the first order radio model [47] for calculation of total energy that is consumed in the network. Table 2 presents the considered energy parameters of Nordic nRF 2401A transceiver.

C. COMPRESSION MODEL

The energy consumption for data transmission in WBAN is much greater than both encryption computations and encryption transmissions [31]. Limited battery capacity of wireless sensors has been studied as an extremely challenging problem in WBAN for decades. In WBAN, energy savings

TABLE 2. Radio parameters of Nordic nRF 2401A transceiver [18].

Parameters	Description	Value	Units
$E_{Tx-elec}$	Energy dissipation for transmission	16.7	nJ/bit
$E_{Rx-elec}$	Energy dissipation for reception	36.1	nJ/bit
E_{amp}	Energy for amplification of signals	1.97	nJ/bit/mn
V_{sup}	Supply voltage	1.9	V
k	Packet length	4000	bits
PL	Path loss coefficient for human body	3.38	dB

is not only important from battery life perspective, but also from the network perspective. Sensor nodes are constantly fed with sensed physiological parameters of the body that are further forwarded to the BC. This increases the network traffic. Moreover, the limited storage capacity of sensor nodes is another issue. Data compression acts as a solution for the above-mentioned problems [53].

Huffman data compression is a lossless and non-uniform data compression algorithm. It compresses as well as encrypts the data that enhances the security of a network. It uses lesser number of bits for transmission of data than Run Length Encoding (RLE) algorithm. Lesser the number of bits, lesser will be the consumption of energy for transmission of data and lesser amount of storage space is required in sensor nodes [54]. This will increase the speed of data packet transfer, eliminates the redundancy of sensed data, provides space and time efficiency, decrease costs for storage hardware and increases network bandwidth [55]–[57]. Several criteria have been used for the performance evaluation of Huffman data compression algorithm that is described in Equation 3 to Equation 11.

$$\text{Compression Ratio} = \frac{L_{CD}}{L_{PD}} \tag{3}$$

Compression factor can be obtained as the inverse of the compression ratio as represented in Equation 4.

$$\text{Compression factor} = \frac{L_{PD}}{L_{CD}} \tag{4}$$

The saving percentage calculates the reduction in original data and is given in equation 5.

$$\text{Saving percentage} = \frac{L_{PD} - L_{CD}}{L_{CD}}\% \tag{5}$$

Code efficiency percentage is represented in equation 6.

$$\eta = \frac{H(z)}{L(z)} * 100 \tag{6}$$

$$0 \le \eta \le 100 \tag{7}$$

where $H(z)$ is the entropy (Equation 8), $L(z)$ is the average length of codewords for Huffman encoding (Equation 9) and η is code efficiency.

Suppose there are an alphanumeric of n symbols $\{a_i | i = 1, 2, 3 \ldots\ldots\ldots, n\}$ having probabilities of occurrences $P(a_1), P(a_2), P(a_3), \ldots\ldots\ldots\ldots, P(a_n)$. The entropy (S) and is calculated as represented in Equation 8.

$$H(z) = -\sum\nolimits_{i=1}^{n} P(a_i)\, logP(a_i) \tag{8}$$

If $L(a_i)$ is the codeword length of symbol a_i, then the codeword length is represented in equation 9.

$$L(z) = \sum\nolimits_{i=1}^{n} P(a_i)\, L(a_i) \tag{9}$$

Compression speed is the ratio of the number of bits that needs compression to the speed of algorithm for compression is described in equation 10.

$$\text{Compression speed} = \frac{\textit{Uncompressed bits}}{\text{seconds to compress}} \tag{10}$$

Decompression speed is the ratio of number of bits that needs compression to the speed of algorithm for decompression as shown in equation 11.

$$\text{Decompression speed} = \frac{\textit{Uncompressed bits}}{\text{seconds to decompress}} \tag{11}$$

D. SECURITY MODEL

Sensor nodes collect sensitive (life-critical) information that is vulnerable to security attacks. The physiological information of the patients is strictly private and confidential. The tampering of medical information by any intruder may harm the patient and lead him into serious consequences. In addition, it should reach the medical personnel securely on time. Therefore, communication of physiological information among sensors over the Internet to servers needs to be secure. The malicious intruder can use the acquired information for illegitimate purposes. Therefore, along with security mechanisms, privacy protection also becomes a crucial research problem of WBAN in past years. Thus, scalable, lightweight and strict security and privacy protection mechanisms are required for WBAN to resist vulnerabilities and security attacks.

RSA is a popular asymmetric key cryptographic technique that is used for security and privacy protection mechanisms. Each sensor node of WBAN as well as BC have both private and public keys to encrypt and decrypt in order to implement high level security. The encryption and decryption process of RSA is represented in Equation 12 and Equation 13 respectively. The decryption of message is done by using private key whereas encryption is provided by the public key.

$$ED = PD^{e} mod\ x \tag{12}$$

$$PD = ED^{d} mod\ x \tag{13}$$

where ED is encrypted data used for transmission, PD is patient data, the pair of numbers (x, e) forms the RSA public key (Pu), d is private key (Pr). The relationship between public and private key is written mathematically as follows:

$$ed = 1\ mod(p-1)(q-1) \tag{14}$$

where p and q are two large prime numbers and $x = p * q$.

As the public keys of sensor nodes are comprised of two large prime numbers. Therefore, it will be tough for an intruder to decrypt the data without having the prior information of used prime numbers [58]. Thus, RSA algorithm enhances the security of WBAN.

E. OPTIMAL ROUTE SELECTION

As size of the human body is limited, the nodes lie within limited range. To provide better QoS and to improve the stability of WBAN, a cost based function has been proposed that transmits the data packets from source to destination nodes reliably. The proposed cost function is represented in Equation 15. The proposed work attempts to choose the optimum channel for transmission of data packets with minimum energy consumption and high throughput.

Minimize

$$Cost_i = w_1 * \left|\frac{Dist_{sn,i}}{Dist_{sn,dn}}\right| + w_2 * \left|\frac{L_{PDi} - L_{CDi}}{L_{PDi}}\right| + w_3 * \left|\frac{E_0 - RE_i}{E_0}\right| \tag{15}$$

Subject to:

$$w_1 + w_2 + w_3 = 1 \tag{16}$$

where

$$0.7 < w_3 < 1 \tag{17}$$

$$0 < w_1 < 1 - w_3 \tag{18}$$

$$w_2 = 1 - w_1 - w_3 \tag{19}$$

w_1, w_2, w_3 Oare three weights optimized using PSO. The weights provide the relative significance to three parameters namely distance, data length and energy within the proposed cost function.

Distance from the source node (sn) to destination node (dn) has been determined by equation 20.

$$Dist_{(sn,dn)} = \sqrt{(x_{dn} - x_{sn})^2 - (y_{dn} - y_{sn})^2} \tag{20}$$

Residual energy (RE_i) of node i is calculated as:

$$RE_i = E_0 - CE_i \tag{21}$$

where CE_i is calculated using summation of Equation 1 and 2.

The parameters employed in PSO algorithm are summarized in Table 3.

PSO find optimal solution of a problem by updating position and velocities of particles. The particles of PSO have two best values i.e. personal best and global best. Each particle is figured out using an objective (fitness) function i.e. cost based function represented in Equation 15. The particle updates its velocity and position using equation 22 and 23 respectively after finding the best values.

$$v_{i,j}[t+1] = w_0 * v_{i,j}[t] + c_1 * rand() * (pbest_{i,j} - p_{i,j}[t]) + c_2 * rand() * (gbest_{i,j} - p_{i,j}[t]) \tag{22}$$

$$p_{i,j}[t+1] = p_{i,j}[t] + v_{i,j}[t] \tag{23}$$

TABLE 3. Parameter setting of PSO.

PSO Parameter	Value	Description
N	100	Population size
maxite	10	Maximum iterations
Maxrun	5	Maximum runs need to be
wmax	0.4	Minimum inertia weight
wmin	0.9	Minimum inertia weight
c_1	2	Acceleration factor
c_2	2	Acceleration factor
LB	0.1	Lower bounds of variables
UB	1	Upper bounds of variables
Penalty	1	Penalty on each constraint violation

where $v_{i,j}[t+1]$ is the new velocity for the i^{th} particle, c_1 and c_2 are the weighting coefficients for the personal best and global best respectively, $p_{i,j}[t]$ is the location of particle at time t, $pbest_{i,j}$ is the personal best j^{th} component of i^{th} particle and $gbest_{i,j}$ is the globally best j^{th} component of the particle, $p_{i,j}[t+1]$ is the updated position of particle at time $[t+1]$. The $rand()$ function produces a uniform random variable $\in [0, 1]$. w_0 is inertial weight and calculated as represented in Equation 24.

$$w_0 = \frac{wmax - (wmax - wmin) * ite}{maxite} \tag{24}$$

where ite is current iteration.

Penalty is added on each constraint violation of above stated weights represented from Equation 16 to Equation 19:

$$Newcost = Previous\ cost + Penalty \tag{25}$$

F. CLASSIFICATION OF NODES

To achieve energy efficiency, the nodes are classified into two Direct Mode (DM) and Relay Mode (RM). Initially all sensor nodes are in DM. The transmission power will be maximum in DM. In DM, direct communication is used between source nodes and destination node (BC) to transmit data packets. The transmission power will be lowest in relay mode. The relay node can communicate to only nearby nodes i.e. Multi-hop technique is used for the transmission of message to BC. The nodes change their mode by calculating their residual battery power. The illustration of nodes having different modes is represented in Figure 2. The residual battery power is mathematically estimated as shown in Equation 21.

Let E_{th} be the pre-defined threshold value of the threshold battery energy. Algorithm 1 presents the procedure for nodes change their mode.

G. CLASSIFICATION OF MESSAGES

The physiological parameters are sensed by sensors after regular intervals of time and transmitted to medical authorities

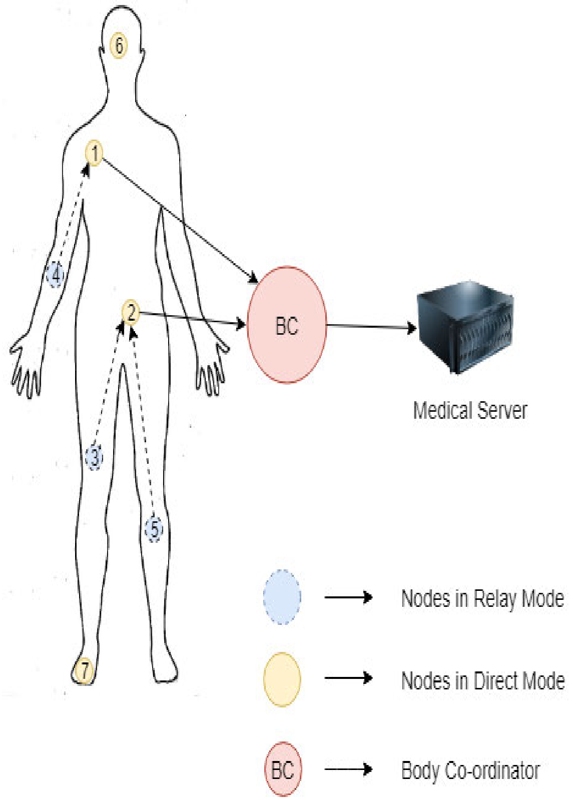

FIGURE 2. Nodes in relay modes and direct modes.

Algorithm 1 Mode switching procedure for nodes

```
Input: $E_{th}$, $RE_i$ of node i
    if ($RE_i > E_{th}$)
    then
        the node activates DM
    else
        the node activates RM
    end if
```

for analysis. These messages can be regular messages or messages arising out of any abnormality. Therefore, the messages can be characterized as non-critical messages and critical messages. Non-critical messages have regularly monitored parameters such as glucose metabolism, body temperature, ECG, pulse rate etc. Critical messages are those, which have sudden change in physiological parameters such as sudden fall or rise in temperature, in blood pressure or in heart rate.

IV. PROPOSED OPTIMIZED ENERGY EFFICIENT SECURE ROUTING PROTOCOL (OEESR)

The current work proposes an Optimized Energy Efficient Secure Routing (OEESR) protocol that aims to attain high energy efficiency, throughput, and security of the network. The proposed work extends the work of Rel-AODV protocol [27] by considering Huffman Data Compression Technique and optimized cost function. The proposed OEESR protocol is implemented based on the similar scenarios as that of Rel-AODV [27]. The Optimized Energy-Efficient and Secure Routing Protocol is described below:

A. INTIALIZATION PHASE

BC has more energy than ordinary nodes and broadcast Hello packets at regular intervals. Ordinary BAN nodes broadcast Hello packets after receiving it from other nodes. Suppose that node, neighbor node of sending source node *sn*, lies between node *sn* and destination node *dn*. The design of Hello Packets is shown in Figure 3a. After receiving hello packets from node *i*, *sn* has recorded the information in the neighbor table and added its own information in the received Hello Packets for broadcasting. Hello packets contain information for building and keeping the neighbor table. The design of neighbor table is shown in Figure 3b. The method to form and alter the neighbor table for every sending node *sn* is represented in Figure 3c.

B. ROUTING ALGORITHM

The proposed routing algorithm has selected the route having minimal communication cost for the same destination. The fields of routing table of any sensor node *sn* are shown in Figure 3d. If the distance between the destination node *dn* and node *sn* is one hop, then the destination ID (ID_{dn}) will be taken as the next hop. Otherwise the neighbor node *i* with minimal communication cost ($Cost_i$) will be chosen as the next hop as shown in Figure 3e.

C. MESSAGE TRANSMISSION AT SOURCE

The sensor node collects physiological information of the patients and store in its memory. Each node compresses the collected physiological information using Huffman Data Compression Technique. Huffman coding compresses as well as encrypts data that enhances the security of the network. Furthermore, RSA asymmetric key cryptographic algorithm encrypts the compressed patient data.

RSA helps to achieve both authentication and data confidentiality between sender *i* and receiver *j* using Equation 26 and 27.

$$ED_i = encrypt(encrypt(Pr_i, PD_i), Pu_j) \tag{26}$$

$$PD_i = decrypt(decrypt(Pr_j, ED_i), Pu_i) \tag{27}$$

The data packet design at source node is shown in Figure 3f. If the transmitted message is critical then critical flag is set (=1) otherwise 0. When a critical message occurs at a particular node then it temporarily activates to DM. The node adds its id and signature at the reserved place in the packet and chooses next hop node using Figure 3e. Adding signature in packet header helps to prevent backward routing of packets. This saves battery power, reduces network traffic and improves the QoS of network.

D. MESSAGE INTERPRETATION AT THE DESTINATION

On receiving data packets, the node checks its destination field. If the ID of destination node matches, the data packet is decrypted using private key as represented in Equation 13. Further decoding of data is performed using Huffman

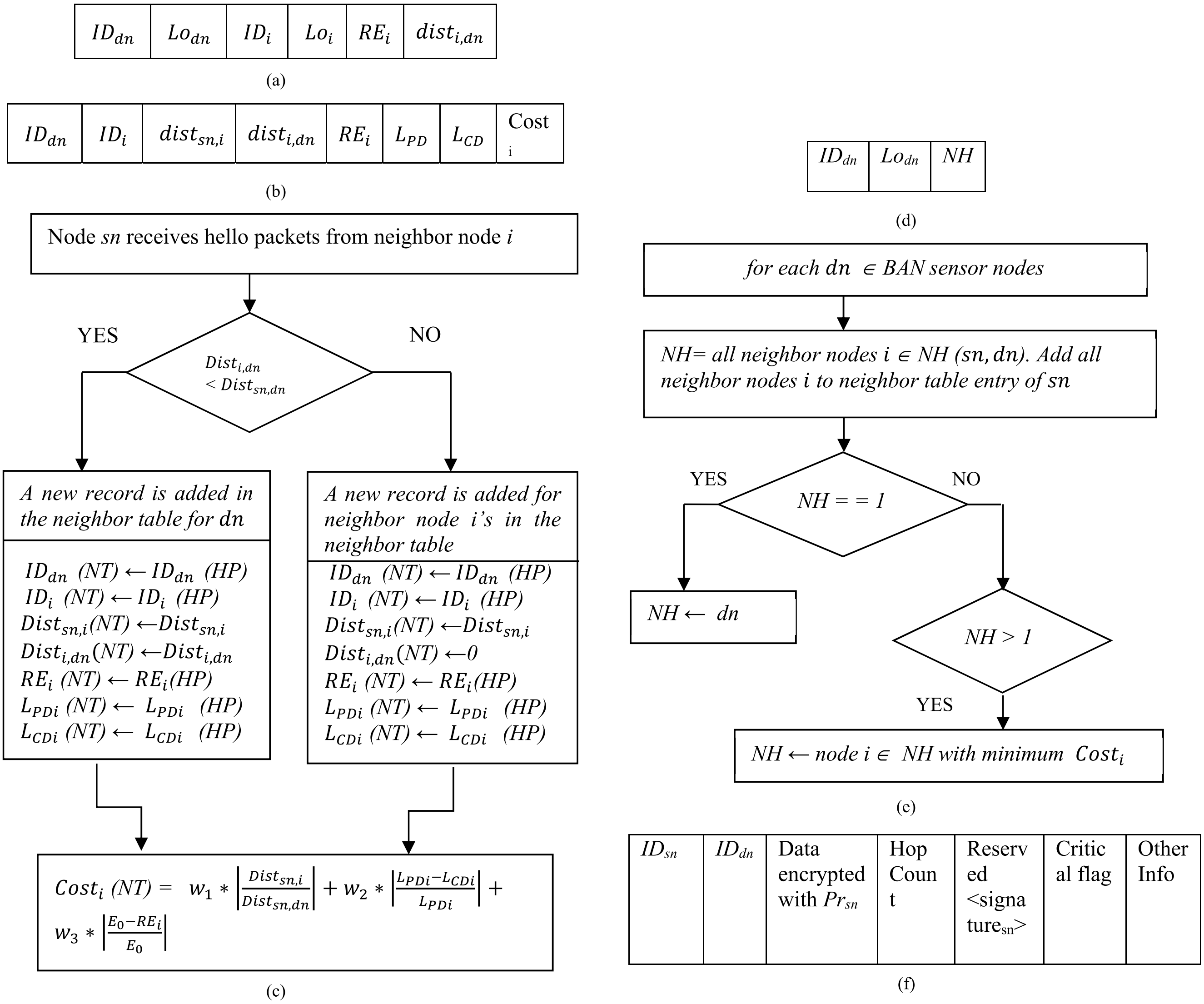
ID_{dn} | Lo_{dn} | ID_i | Lo_i | RE_i | $dist_{i,dn}$
(a)
ID_{dn} | ID_i | $dist_{sn,i}$ | $dist_{i,dn}$ | RE_i | L_{PD} | L_{CD} | $Cost_i$
(b)
Node *sn* receives hello packets from neighbor node *i*
YES
NO
$Dist_{i,dn} < Dist_{sn,dn}$
A new record is added in the neighbor table for dn
ID_{dn} (NT) ← ID_{dn} (HP)
ID_i (NT) ← ID_i (HP)
$Dist_{sn,i}$(NT) ←$Dist_{sn,i}$
$Dist_{i,dn}$(NT) ←$Dist_{i,dn}$
RE_i (NT) ← RE_i(HP)
L_{PDi} (NT) ← L_{PDi} (HP)
L_{CDi} (NT) ← L_{CDi} (HP)
A new record is added for neighbor node i's in the neighbor table
ID_{dn} (NT) ← ID_{dn} (HP)
ID_i (NT) ← ID_i (HP)
$Dist_{sn,i}$(NT) ←$Dist_{sn,i}$
$Dist_{i,dn}$(NT) ←0
RE_i (NT) ← RE_i(HP)
L_{PDi} (NT) ← L_{PDi} (HP)
L_{CDi} (NT) ← L_{CDi} (HP)
$Cost_i\ (NT) = w_1 * \left|\frac{Dist_{sn,i}}{Dist_{sn,dn}}\right| + w_2 * \left|\frac{L_{PDi}-L_{CDi}}{L_{PDi}}\right| + w_3 * \left|\frac{E_0-RE_i}{E_0}\right|$
(c)
ID_{dn} | Lo_{dn} | NH
(d)
for each dn ∊ BAN sensor nodes
NH= all neighbor nodes i ∊ NH (sn, dn). Add all neighbor nodes i to neighbor table entry of sn
YES
NO
NH = = 1
NH ← dn
NH > 1
YES
NH ← node i ∊ NH with minimum $Cost_i$
(e)
ID_{sn} | ID_{dn} | Data encrypted with Pr_{sn} | Hop Count | Reserved <signature$_{sn}$> | Critical flag | Other Info
(f)

FIGURE 3. **(a) Fields of hello packet of node *i*. (b) Fields of neighbor table of node *sn*. (c) Neighbor table construction procedure at each node *sn*. (d) Fields of routing table of any sensor node *sn*. (e)Routing table construction procedure. (f) Packet at the sender.**

decoding algorithm. Further BC sends patient data to the required destination or doctor.

E. OVERALL ALGORITHM

V. RESULTS AND ANALYSIS

A. COMPARATIVE ANALYSIS OF OEESR WITH EXISTING PROTOCOLS

1) PACKET DROPPING RATE VS. NUMBER OF NODES

The rate of packet-dropping has been plotted against by considering varying number of nodes as illustrated in Figure 4. The packet dropping rate has been remained constant with the rise in number of nodes in the network for proposed protocol whereas packet dropping rate show an increasing trend in other protocols. Results show that OEESR has 10% least packet dropping rate as compared to 17% of CSEER, 22.9% of Rel-AODV, 25% of EPR and 57% of conventional methods. This is owing to the use of compression technique for data transmission.

The compression technique minimizes the number of bits to be transmitted that will result in lower number of packets dropped, as there will be no congestion in the network. Also, in OEESR protocol, proposed optimized cost function with distance, data length and energy as its parameters play an important role for selecting the next optimal hop node for transmitting packets. The optimized cost function has allowed the uniform energy dissipation in the network as well as chooses next hop node with minimal distance to prevent packet loss. This results in low packet dropping rate which indicates high reliability and better QoS provided by the network. The graph also depicts the scalability of OEESR protocol as addition of more number of nodes will not add to the packet-dropping rate of OEESR.

2) TRANSMISSION POWER VS. PACKET DROPPING RATE

The packet-dropping rate has been plotted against variations in transmission power as illustrated in Figure 5. As expected,

Algorithm 2 At the Sensor on Sensing an Event

Input: physiological parameters sensed by sensor node (PD)

```
 1. $CD = compressPD$
 2. $ED = encrypt(CD, Pu_{BC})$
 3. if event == Critical()
 4. Set critical flag $= 1$
 5. Set mode $= DM$
 6. Search for next hop in routing table using Figure 3e
      a. If next hop == destination
           i. Add signature
          ii. Send packet to destination
         iii. Exit
      b. Else
           i. Add signature
          ii. Send packet to next hop
 7. else
 8. Set mode $= RM$
 9. Set critical flag $= 0$
10. Search for next hop in routing table using Figure 3e
      a. If next hop == destination
           i. Add signature
          ii. Send packet to destination
         iii. Exit
      b. Else
           i. Add signature
          ii. Send packet to next hop
```

Algorithm 3 At Intermediate Relay Nodes

Input: Packet from source sensor nodes

```
1. if critical flag == 1
2. Set mode $= DM$
3. Search for next hop in routing table using Figure 3e
     a. If next hop == destination
          i. Add signature
         ii. Send packet to destination
        iii. Exit
     b. else
          i. Add signature
         ii. Send packet to next hop
4. else
5. Set mode $= RM$
6. Search for next hop in routing table using Figure 3e
     a. If next hop == destination
          i. Add signature
         ii. Send packet to destination
        iii. Exit
     b. else
          i. Add signature
         ii. Send packet to next hop
```

Algorithm 4 At the Destination Node

Input: Packet from sensor nodes

```
  i. $CD = decrypt(ED, Pr_{BC})$
 ii. $PD =$ decompress CD
iii. Send PD to higher authorities
```

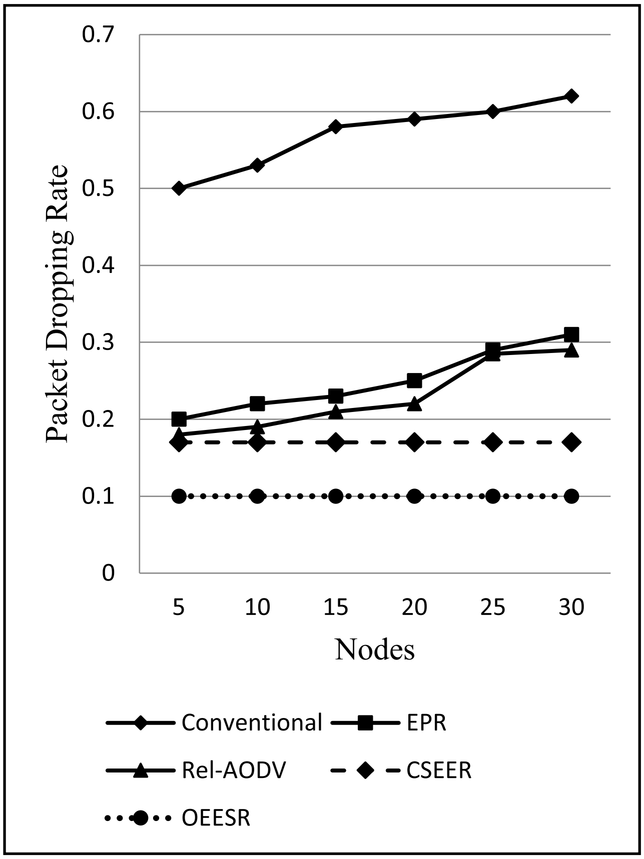

FIGURE 4. Number of nodes vs. packet dropping rate.

fewer packets are dropped when transmission power is high. This is because the nodes will come in the range of the next hop node with increase in transmission power and therefore, there are lesser chances of packets being dropped.

In OEESR scheme, the proposed optimized cost function based on distance, energy and data length choose the best next hop node in the network. This balances the energy consumption in the network resulting in increased network lifetime, and hence lesser packets are dropped. Moreover, utilization of data compression technique lessen the number of packets to be transmitted in the network, hence lesser number of packets will be dropped. It is seen from the Figure 5 that OEESR has 12.64% least packet dropping rate as compared to 25.33% of CSEER, 33% of Rel-AODV, 41.1% of EPR and 46% of conventional methods with increase in transmission power.

3) NUMBER OF NODES VS. PACKET DELIVERY RATIO

The variation in ratio of packet delivery with the increase in number of nodes in the network has been illustrated in Figure 6. With the increase in number of nodes in the network, there is a decrease in packet delivery ratio. Buffer overflow of sensor nodes as well as collision among transmitted data occurs with more number of nodes in the network,

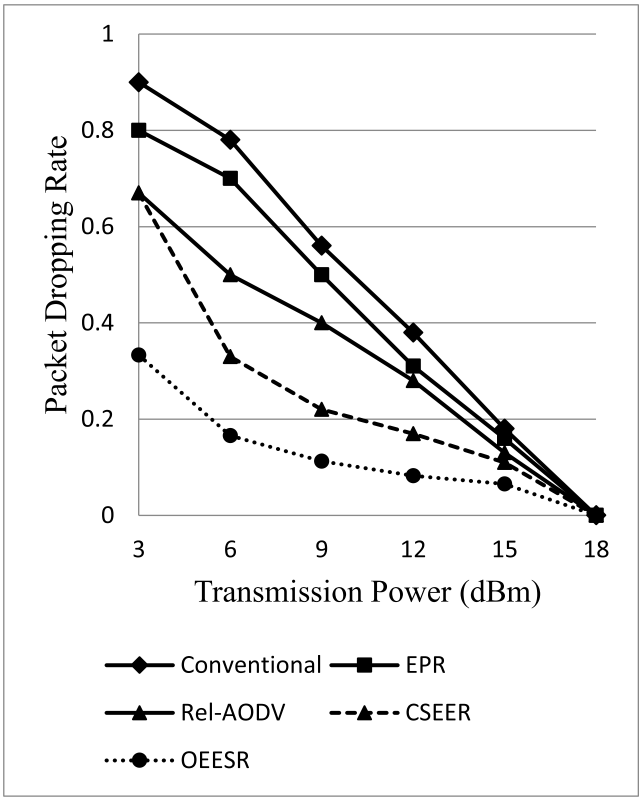

FIGURE 5. Packet dropping rate vs. transmission power.

causing reduction in packet delivery ratio. For C-AODV, CSEER and RelAODV, lesser number of nodes gives better efficacious transmission rate of packets, but as the number of nodes increases, transmission rate decreases. In the proposed approach, with the implementation of data compression technique as well as optimized cost function, the data in compressed form is transmitted which results in reduction of data. Therefore, no buffer overflow or collisions have taken place. Hence, more number of packets have been successfully transmitted.

4) THROUGHPUT

Throughput can be defined as the amount of packets successfully obtained at the destination node per unit time. For WBAN nodes, it is vital to give high throughput as the data of patient is crucial and its loss in any form is intolerable. Figure 7 highlights the proposed protocol that has provided a throughput of 90%, which is much greater than CSEER (83%), Rel-AODV (80%), EPR (60%) and conventional protocols (49.2%). This is owing to the use of compression technique and optimized cost function while data transmission. The compression minimizes the number of bits to be transmitted that will result in increase in throughput, as there will be no congestion in the network. Therefore, more packets are delivered without any loss. Moreover, the proposed optimized cost function chooses the next hop node based on its residual energy. More residual energy of nodes, more will be the network lifetime and results in more packet delivery to the destination.

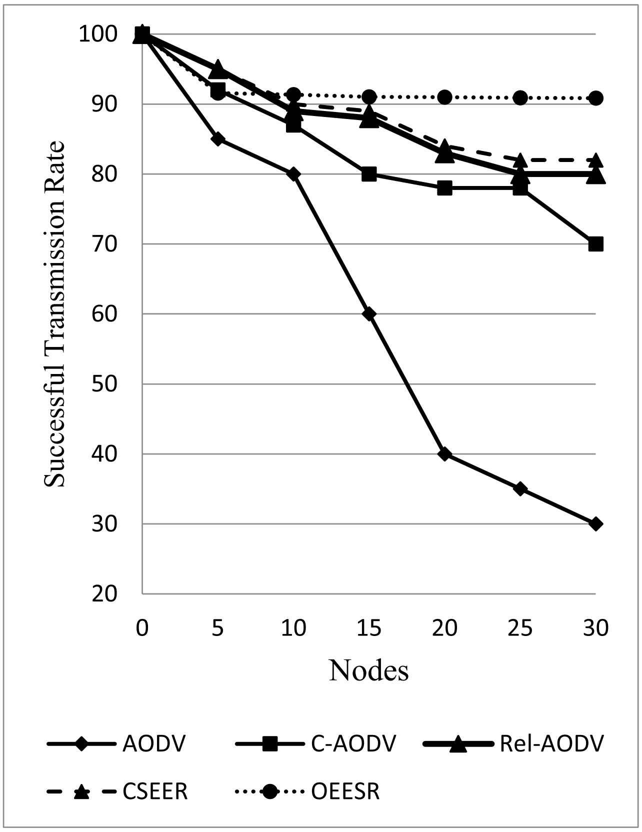

FIGURE 6. Number of nodes vs. packet delivery ratio.

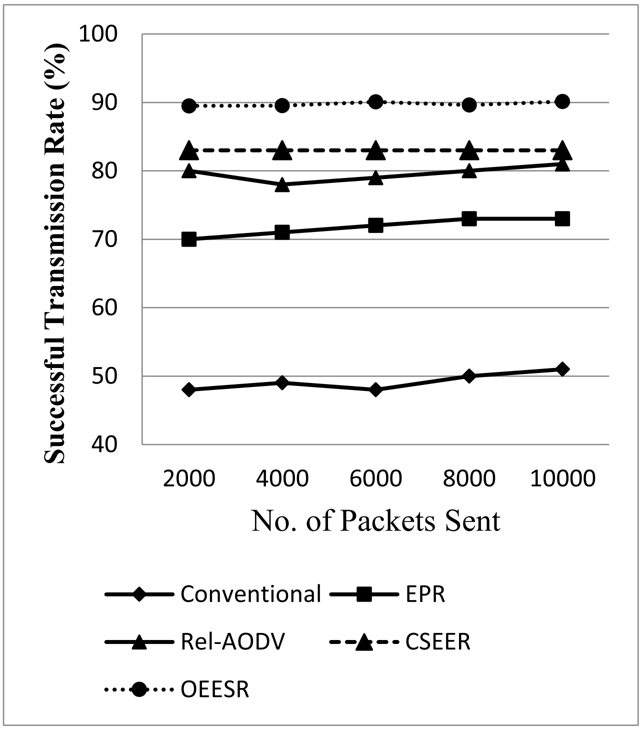

FIGURE 7. Throughput of network.

5) ENERGY CONSUMPTION

The weight optimized cost function has been presented for choosing the next optimal hop node where maximum weight is assigned to the energy parameter that has illustrated its

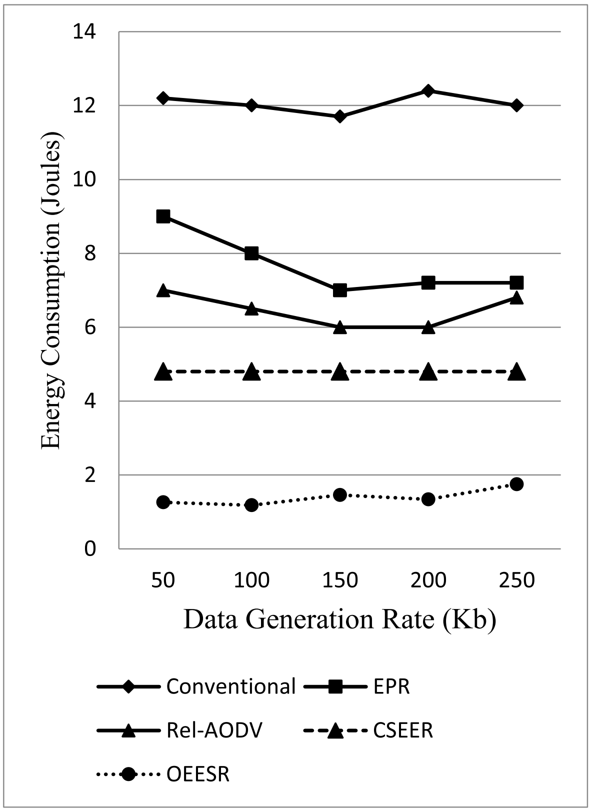

FIGURE 8. Energy consumption.

significance in the proposed work. Further, PSO technique has been employed to optimize the weights, which caused lesser consumption of energy in the network.

Moreover, the packets are transmitted in compressed form, which further leads to energy saving during transmission. The overall energy consumption of OEESR is 8.8%, which is remarkably lower than 30% of CSEER, 40.3% of Rel-AODV, 48% of EPR and 77% of conventional protocols as shown in Figure 8. Nevertheless, the consumption of energy increased with the rise in data generation rate. This is because with the increase in data generation rate, more energy is consumed for encoding and decoding of Huffman data compression technique as well as cryptographic RSA algorithm.

B. OEESR EVALUATION AND DISCUSSION BY CONSIDERING DIFFERENT SCENARIOS

Scenario 1: Variable amount of packets are transmitted at different transmit powers and mobility of all nodes is taken into consideration except BC.

1) PACKETS ACCELERATED BY INTERMEDIARY NODES

Figure 9 displays the amount of packets delivered through intermediary nodes are plotted against different transmit powers. The amount of packets delivered through intermediate nodes in OEESR for all three-transmission powers of −10 dBm, −15 dBm and −25 dBm are 1072, 1356 and 453 respectively. As transmission power raises from −25 dBm to −15 dBm, the numbers of packets forwarded through intermediate nodes also increases. This is due to the multihop communication in OEESR as well as low congestion in the network. When transmission power is increased from −15 dBm to −10 dBm, the numbers of packets redirected through intermediary nodes decreases. Because at high transmit power, the destination node comes in the range of sending nodes which results in lesser packet forwarding through intermediate nodes in the network.

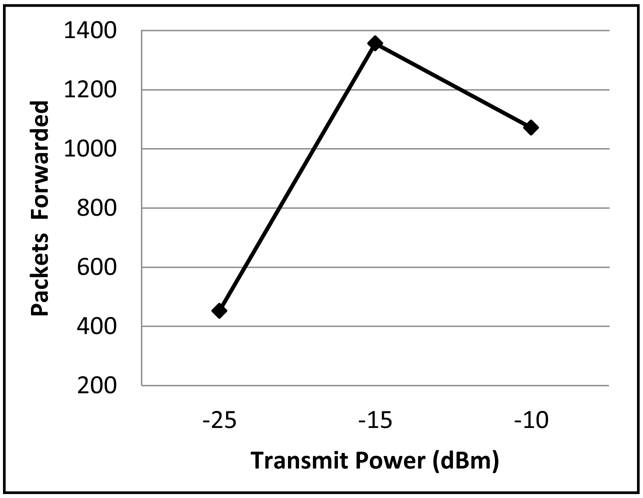

FIGURE 9. Packets forwarded by intermediate nodes.

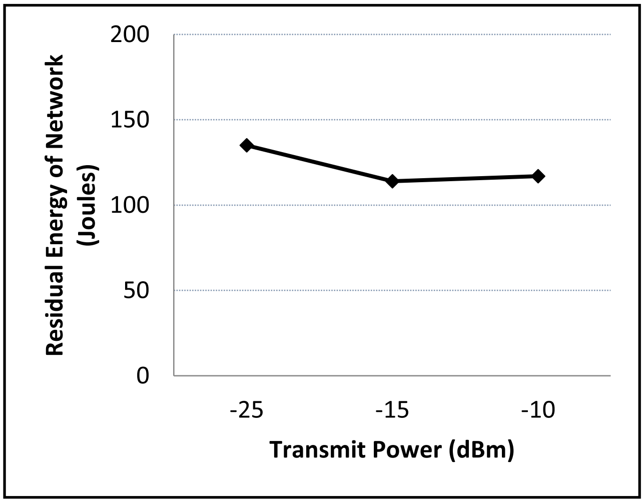

FIGURE 10. Residual energy of network.

2) RESIDUAL ENERGY OF NETWORK

The residual energy of network for different values of transmission powers has been depicted in Figure 10. The residual energy values are 117, 114 and 135 Joules in OEESR for all three-transmit powers of −10 dBm −15 dBm and −25 dBm respectively. At low transmission power of −25 dBm, residual energy of the network is high due to multihop communication and low congestion. However, as transmission power increases from −25 dBm to −10 dBm, the residual energy of the network decreases. This is owing to the direct communication of nodes due to high transmit powers.

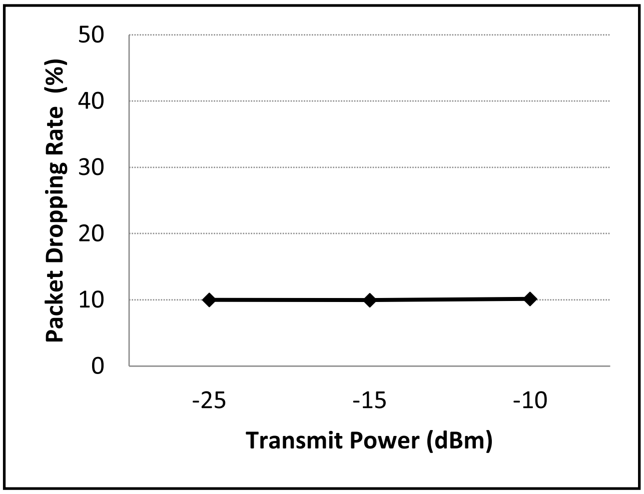

FIGURE 11. Packets dropped at different transmit powers.

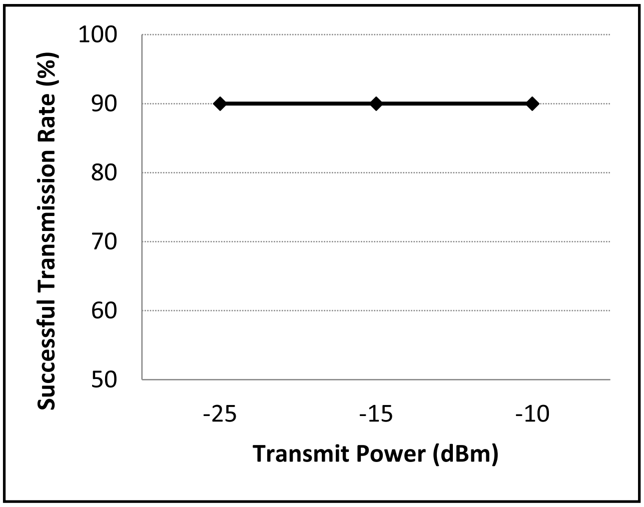

FIGURE 12. Successful transmission rate (%).

3) PACKET DROPPING RATE

Figure 11 shows the values of packets dropping rate in network at different transmit powers. From simulations, it is observed that 1693, 1702 and 1588 packets are dropped out of total of 16896, 17063 and 15644 packets in OEESR for all transmission powers of −25 dBm, −15 dBm and −10 dBm respectively. It has been observed that for all transmit powers, OEESR has constant 10% packet dropping rate. Packet dropping rate remains constant because of optimal route selection for transmitting data packets by considering proposed cost function, which increased the reliability of the links.

4) SUCCESSFUL TRANSMISSION Rate(%)

Figure 12 shows successful transmission rate (%) in network at different transmit powers. From simulations, it is observed that 15203, 15361 and 14056 packets are received out of 16896, 17063 and 15644 total packets in OEESR for the transmission powers of −25 dBm, −15 dBm and −10 dBm respectively.

It has been observed that for all transmission powers, OEESR has constant 90% successful transmission rate.

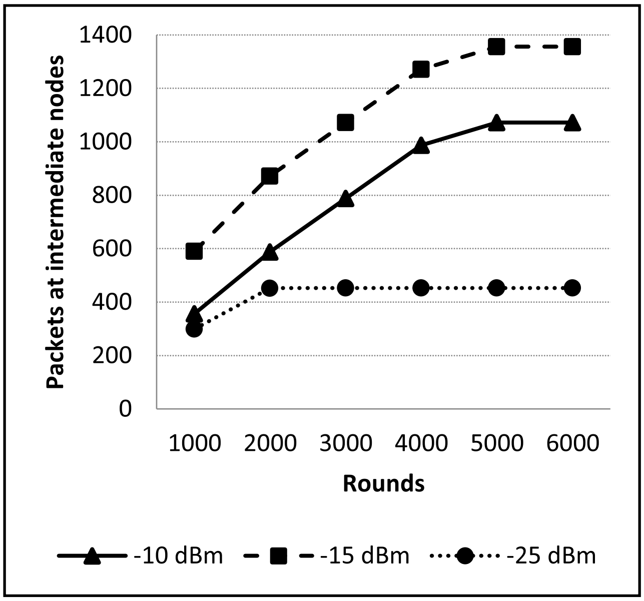

FIGURE 13. Packets forwarded by intermediate nodes.

Successful transmission rate remains constant in OEESR for all transmit powers because of optimal route selection for transmitting data packets by considering proposed cost function, which increases reliability of the links.

Scenario 2: Varying number of packets are forwarded at different transmit powers for different rounds and mobility of all nodes is taken into consideration except BC.

5) PACKETS TRANSMITTED BY INTERMEDIARY NODES

Figure 13 shows the amount of packets delivered through intermediate nodes are plotted against different number of rounds. It is found that as the number of rounds has been increased, the packets accelerated by intermediary nodes have also been increased. After 2000 rounds packets delivered through intermediate nodes remains constant for low transmission power of −25 dBm because of less number of nodes in range. But at high transmission power of both −15 dBm and −10 dBm, an increasing trend is observed. High transmit power leads to more number of nodes in range. The multihop communication in OEESR accounts for more packets delivered through intermediate nodes for all three transmit powers.

6) NUMBER OF DEAD NODES

Figure 14 illustrates the number of dead nodes plotted against different number of rounds. It has been observed that as the number of rounds has increased, dead nodes in OEESR are also got increased. After 2000 rounds, −10 dBm has less number of dead nodes as compared to both −25 dBm and −15 dBm transmit powers. At high transmit power, destination node comes in the range of sending nodes lowers the multihop communication in the network resulted in less number of dead nodes. As number of rounds have been increased, network load of network has also been increased that has reduced

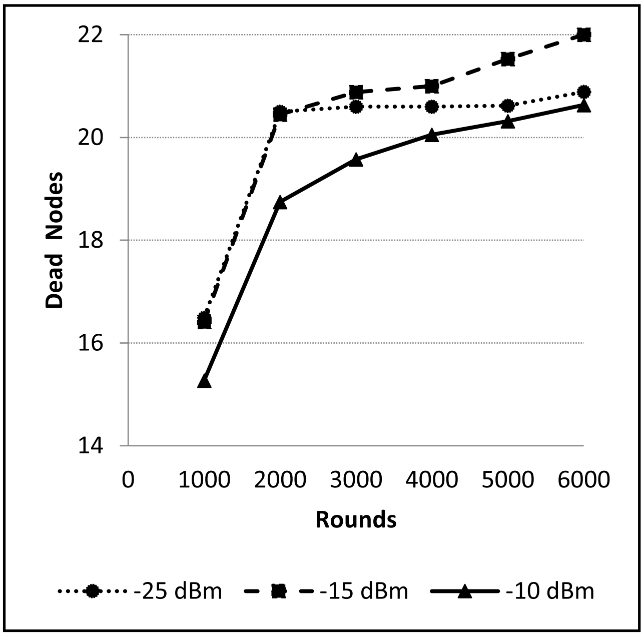

FIGURE 14. Dead nodes.

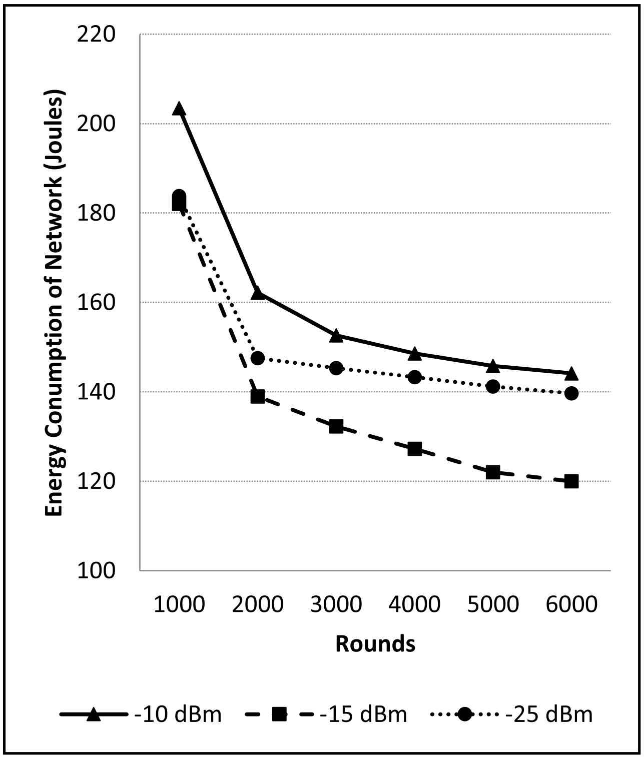

FIGURE 15. Residual energy at different rounds.

the energy of sensor nodes. Therefore, network lifetime is decreased with the increase in rounds for all transmit powers.

7) RESIDUAL ENERGY OF NETWORK

The residual energy of the network for all three transmission powers is plotted against varying number of rounds. From 1000 to 2000 rounds, the graph shows a huge decreasing trend for all transmit powers. This is owing to the initialization of network at an expense of huge part of energy. It is observed that when rounds are increasing, -10 dBm transmit power has high residual energy as compared to transmit power of -15 dBm due to the direct communication of nodes.

VI. CONCLUSION RESULTS AND ANALYSIS

The proposed OEESR protocol is an energy-efficient routing protocol for highly secure transmission of data in WBAN. The proposed protocol utilizes three techniques. Firstly, Huffman Data Compression technique is used for compression of patient data as well as to add a layer of encryption. Secondly, RSA cryptographic algorithm is used to provide more secure encryption to the private patient data. Thirdly, the proposed cost based function is optimized using PSO to determine the optimal next hop node. The performance of OEESR has been evaluated for different transmit powers as well as compared with CSEER, EPR, Rel-AODV and conventional protocols in terms of energy efficiency, packet dropping rate and throughput.

The integration of big data, blockchain technology, machine learning and deep learning technologies with the acquired patient's data generated from WBANs will have great impact on analyzing and improving the general healthcare monitoring and assisting as a second opinion in decision-making. Moreover, cognitive networks will also show a futuristic trend in captivating WBAN's to its next level.

REFERENCES

[1] *World Health Statistics*. Accessed: Mar. 20, 2021. [Online]. Available: https://www.who.int/data/gho/whs-2020-visual-summary

[2] M. J. Deen, "Information and communications technologies for elderly ubiquitous healthcare in a smart home," *Pers. Ubiquitous Comput.*, vol. 19, nos. 3–4, pp. 573–599, 2015.

[3] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, Standard 802.15.6-2012, 2012.

[4] R. Punj and R. Kumar, "Technological aspects of WBANs for health monitoring: A comprehensive review," *Wireless Netw.*, vol. 25, no. 3, pp. 1125–1157, Apr. 2019.

[5] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, Aug. 2010.

[6] G. Biagetti, P. Crippa, L. Falaschetti, S. Orcioni, C. Turchetti, "Human activity recognition using accelerometer and photoplethysmographic signals," in *Proc. Int. Conf. Intell. Decision Technol.* Cham, Switzerland: Springer, Jun. 2017, pp. 53–62.

[7] P. Crippa, A. Curzi, L. Falaschetti, and C. Turchetti, "Multi-class ECG beat classification based on a Gaussian mixture model of Karhunen-Loève transform," *Int. J. Simul. Syst. Sci. Technol*, vol. 16, no. 1, pp. 1–2, 2015.

[8] S. C. Mukhopadhyay, "Wearable sensors for human activity monitoring: A review," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1321–1330, Mar. 2015.

[9] D. Brunelli, A. M. Tadesse, B. Vodermayer, M. Nowak, and C. Castellini, "Low-cost wearable multichannel surface EMG acquisition for prosthetic hand control," in *Proc. Int. Workshop Adv. Sensors Interfaces (IWASI)*, Jun. 2015, pp. 94–99.

[10] A. Baca, G. Biagetti, M. Camilletti, P. Crippa, L. Falaschetti, S. Orcioni, L. Rossini, D. Tonelli, and C. Turchetti, "CARMA: A robust motion artifact reduction algorithm for heart rate monitoring from PPG signals," in *Proc. 23rd Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2015, pp. 2646–2650.

[11] G. Biagetti, P. Crippa, A. Curzi, S. Orcioni, and C. Turchetti, "Analysis of the EMG signal during cyclic movements using multicomponent AM–FM decomposition," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 5, pp. 1672–1681, Sep. 2015.

[12] A. Kurian and R. Divya, "A survey on energy efficient routing protocols in wireless body area networks (WBAN)," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2017, pp. 1–6.

[13] S. Singh and D. Prasad, "Wireless body area network (WBAN): A review of schemes and protocols," *Mater. Today, Proc.*, Jun. 2021.

[14] J. H. Majeed and Q. Aish, "A remote patient monitoring based on WBAN implementation with Internet of Thing and cloud server," *Bull. Electr. Eng. Informat.*, vol. 10, no. 3, pp. 1640–1647, Jun. 2021.

[15] A. K. Sagar, S. Singh, and A. Kumar, "Energy-aware WBAN for health monitoring using critical data routing (CDR)," *Wireless Pers. Commun.*, vol. 4, pp. 1–30, Jan. 2020.

[16] N. Yessad, M. Omar, A. Tari, and A. Bouabdallah, "QoS-based routing in wireless body area networks: A survey and taxonomy," *Computing*, vol. 100, no. 3, pp. 245–275, Mar. 2018.

[17] K. N. Qureshi, M. Q. Tayyab, S. U. Rehman, and G. Jeon, "An interference aware energy efficient data transmission approach for smart cities healthcare systems," *Sustain. Cities Soc.*, vol. 62, Nov. 2020, Art. no. 102392.

[18] T. Kaur, N. Kaur, and G. Sidhu, "Optimized energy efficient and QoS aware routing protocol for WBAN," *Recent Patents Eng.*, vol. 14, no. 3, pp. 286–293, Jan. 2021.

[19] V. Nivedhitha, A. G. Saminathan, and P. Thirumurugan, "DMEERP: A dynamic multi-hop energy efficient routing protocol for WSN," *Microprocessors Microsyst.*, vol. 79, Nov. 2020, Art. no. 103291.

[20] P. K. D. Pramanik, A. Nayyar, and G. Pareek, "WBAN: Driving e-healthcare beyond telemedicine to remote health monitoring: Architecture and protocols," in *Telemedicine Technologies*. New York, NY, USA: Academic, 2019, pp. 89–119.

[21] Y. Qu, G. Zheng, H. Ma, X. Wang, B. Ji, and H. Wu, "A survey of routing protocols in WBAN for healthcare applications," *Sensors*, vol. 19, no. 7, p. 1638, 2019.

[22] A. Khanna, V. Chaudhary, and S. H. Gupta, "Design and analysis of energy efficient wireless body area network (WBAN) for health monitoring," in *Transactions on Computational Science* Berlin, Germany: Springer, 2018, pp. 25–39.

[23] A. S. Alzahrani and K. Almotairi, "Performance comparison of WBAN routing protocols," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–5.

[24] J. Anand and D. Sethi, "Comparative analysis of energy efficient routing in WBAN," in *Proc. 3rd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Feb. 2017, pp. 1–6.

[25] M. A. Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, pp. 93–101, Feb. 2012.

[26] Z. A. Khan, S. Sivakumar, W. Phillips, and N. Aslam, "A new patient monitoring framework and energy-aware peering routing protocol (EPR) for body area network communication," *J. Ambient Intell. Hum. Comput.*, vol. 5, no. 3, pp. 409–423, 2014.

[27] K. S. Raja and U. Kiruthika, "An energy efficient method for secure and reliable data transmission in wireless body area networks using RelAODV," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2975–2997, Aug. 2015.

[28] R. Singla and N. Kaur, "Compressed and secure energy efficient routing protocol for WBAN," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 7, pp. 252–258, Jul. 2018.

[29] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc on Demand Distance Vector (AODV) Routing*, document RFC 3561, IETF, 2003.

[30] S. Manfredi, "Reliable and energy-efficient cooperative routing algorithm for wireless monitoring systems," *IET Wireless Sensor Syst.*, vol. 2, no. 2, pp. 128–135, Jun. 2012.

[31] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, 3rd Quart., 2014.

[32] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks," *Procedia Comput. Sci.*, vol. 34, pp. 511–517, Oct. 2014.

[33] T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, "IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Cham, Switzerland: Springer, 2020, pp. 127–151.

[34] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

[35] Y. Du, F. Hu, L. Wang, and F. Wang, "Framework and challenges for wireless body area networks based on big data," in *Proc. IEEE Int. Conf. Digit. Signal Process. (DSP)*, Jul. 2015, pp. 497–501.

[36] D. Singelée, B. Latré, B. Braem, M. Peeters, M. De Soete, P. De Cleyn, B. Preneel, I. Moerman, and C. Blondia, "A secure cross-layer protocol for multi-hop wireless body area networks," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*. Berlin, Germany: Springer, 2008, pp. 94–107.

[37] S. F. Raza, C. Naveen, V. R. Satpute, and A. G. Keskar, "A proficient chaos based security algorithm for emergency response in WBAN system," in *Proc. IEEE Students' Technol. Symp. (TechSym)*, Sep. 2016, pp. 18–23.

[38] C.-H. Lin, J.-X. Wu, P.-Y. Chen, C.-M. Li, N.-S. Pai, and C.-L. Kuo, "Symmetric cryptography with a chaotic map and a multilayer machine learning network for physiological signal infosecurity: Case study in electrocardiogram," *IEEE Access*, vol. 9, pp. 26451–26467, 2021.

[39] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion–substitution based gray image encryption scheme," *Digit. Signal Process.*, vol. 23, no. 3, pp. 894–901, May 2013.

[40] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," *Multimedia Syst.*, vol. 20, no. 1, pp. 45–64, 2014.

[41] S. Anwar and S. Meghana, "A pixel permutation based image encryption technique using chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27569–27590, Oct. 2019.

[42] W. San-Um and N. Chuayphan, "A lossless physical-layer encryption scheme in medical picture archiving and communication systems using highly-robust chaotic signals," in *Proc. 7th Biomed. Eng. Int. Conf.*, Nov. 2014, pp. 1–5.

[43] A. N. Kengnou Telem, C. Meli Segning, G. Kenne, and H. B. Fotsin, "A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network," *Adv. Multimedia*, vol. 2014, pp. 1–13, Oct. 2014.

[44] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K.-K. R. Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Comput. Electr. Eng.*, vol. 61, pp. 238–249, Jul. 2017.

[45] J. Liu, L. Zhang, and R. Sun, "1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, p. 728, May 2016.

[46] A. Sammoud, M. A. Chalouf, O. Hamdi, N. Montavont, and A. Bouallegue, "A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101838.

[47] N. Javaid, A. Ahmad, Q. Nadeem, M. Imran, and N. Haider, "IM-SIMPLE: Improved stable increased-throughput multi-hop link efficient routing protocol for wireless body area networks," *Comput. Hum. Behav.*, vol. 51, pp. 1003–1011, Oct. 2015.

[48] Q. Nadeem, N. Javaid, S. N. Mohammad, M. Y. Khan, S. Sarfraz, and M. Gull, "SIMPLE: Stable increased-throughput multi-hop protocol for link efficiency in wireless body area networks," in *Proc. 8th Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Oct. 2013, pp. 221–226.

[49] N. Kaur and S. Singh, "Optimized cost effective and energy efficient routing protocol for wireless body area networks," *Ad Hoc Netw.*, vol. 61, pp. 65–84, Jun. 2017.

[50] A. Ravelomanantsoa, H. Rabah, and A. Rouane, "Simple and efficient compressed sensing encoder for wireless body area network," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 12, pp. 2973–2982, Dec. 2014.

[51] T. Manna and S. Misra, "Implementation of energy efficient WBAN using IEEE 802.15. 6 scheduled access MAC with fast DWT based backhaul data compression for E-healthcare," in *Proc. Int. Conf. Commun. Syst. Netw.* Cham, Switzerland: Springer, 2018, pp. 26–51.

[52] Y. Liao, M. S. Leeson, Q. Cai, Q. Ai, and Q. Liu, "Mutual-information-based incremental relaying communications for wireless biomedical implant systems," *Sensors*, vol. 18, no. 2, p. 515, 2018.

[53] B. R. Stojkoska and Z. Nikolovski, "Data compression for energy efficient IoT solutions," in *Proc. 25th Telecommun. Forum (TELFOR)*, Nov. 2017, pp. 1–4.

[54] S. Chen and J. G. Wang, "VLSI implementation of low-power cost-efficient lossless ECG encoder design for wireless healthcare monitoring application," *Electron. Lett.*, vol. 49, no. 2, pp. 91–93, Jan. 2013.

[55] S. L. Chen, G. A. Luo, and T. L. Lin, "Efficient fuzzy-controlled and hybrid entropy coding strategy lossless ECG encoder VLSI design for wireless body sensor networks," *Electron. Lett.*, vol. 49, no. 17, pp. 1058–1060, Aug. 2013.

[56] S.-L. Chen, T.-L. Lin, M.-C. Tuan, and T.-K. Chi, "VLSI architecture of lossless ECG compression design based on fuzzy decision and optimisation method for wearable devices," *Electron. Lett.*, vol. 51, no. 18, pp. 1409–1411, Mar. 2015.

[57] A. Negi and A. Goyal, "Optimizing fully homomorphic encryption algorithm using RSA and Diffie- Hellman approach in cloud computing," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 5, pp. 215–220, May 2018.

RIPTY SINGLA received the B.Tech. and M.Tech. degrees in computer engineering from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, in 2016 and 2018, respectively. She is currently an Assistant Professor with the Department of Computer Science and Engineering, Chandigarh University, India. Her current research interests include wireless sensor networks and wireless body area networks.

NAVNEET KAUR (Member, IEEE) received the B.Tech. degree in computer science and engineering from Panjab Technical University, Jalandhar, India, in 2000, and the M.E. degree (Hons.) in computer science and engineering from Panjab University, Chandigarh, India, in 2007. Her Ph.D. thesis is focused on healthcare domain. She is currently associated with Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India. She is having 21 years of teaching and research experience at various reputed universities of india. She has published more than 20 research articles in reputed SCI and scopus indexed journals, conferences, and one book. Her research interests include wireless sensor networks, wireless body area networks, and cloud computing. She is the Awardee of the Best Engineering College Teacher Award for Punjab State for at the 49th ISTE National Annual Convention at Siksha 'O' Anusandhan, Bhubaneshwar, India, in 2019, in recognition of her outstanding contribution to the academic community and the students. She also received the Certificate for Appreciation for High Impact Factor Publication from UIET Panjab University, in 2017.

DEEPIKA KOUNDAL received the B.Tech. degree in computer science and engineering from Kurukshetra University, Kurukshetra, Haryana, India, and the M.E. and Ph.D. degrees in computer science and engineering from UIET, Panjab University, Chandigarh, India. She is currently associated with the University of Petroleum and Energy Studies, Dehradun. She is having 12 years of teaching and research experience at various reputed universities of india. She was previously associated with NIT Hamirpur as an Assistant Professor. Prior to that, she worked at UIET, Panjab University, Chandigarh. Her Ph.D. thesis is focused on healthcare domain. She has published more than 30 research articles in reputed SCI and scopus indexed journals, conferences, and two books. Her research interests include wireless sensor networks, wireless body area networks, image processing in healthcare, and agriculture domain. She is the Awardee of the Research Excellence Award given by Chitkara University, in 2019. She also received the Recognition and Honorary Membership from Neutrosophic Science Association from the University of Mexico. She is a Guest Editor in journal titled *Computer and Electrical Engineering*.

SAIMA ANWAR LASHARI received the bachelor's degree (Hons.) in computer science from the University of Engineering and Technology (UET), Lahore, Pakistan, in 2004, and the M.Sc. and Ph.D. degrees in information technology from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia, in 2012 and 2016, respectively. Her research interests include image and signal processing, soft computing, and machine learning.

SURBHI BHATIA received the bachelor's degree in information technology, in 2010, the master's degree in technology from Amity University, in 2012, and the Ph.D. degree in computer science and engineering from Banasthali Vidypaith, India. She is currently an Assistant Professor with the Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia. She has rich eight years of teaching and academic experience. She has published many research papers in reputed journals and conferences in high indexing databases and have patents, granted from USA, Australia, and India. She has authored two books and edited seven books from Springer, Wiley, and Elsevier. She has completed two funded research projects from the Deanship of Scientific Research, King Faisal University, and the Ministry of Education, Saudi Arabia. She has delivered talks as a keynote speaker in IEEE conferences and in faculty development programs. Her research interests include machine learning, sentiment analysis, and information retrieval. She has earned professional management professional certification from PMI, USA. She is an Editorial Board Member with Inderscience Publishers in the *International Journal of Hybrid Intelligence*, *SN Applied Sciences* (Springer). She is currently serving as a guest editor of special issues in reputed journals.

MOHAMMAD KHALID IMAM RAHMANI (Senior Member, IEEE) was born in Patherghatti, Kishanganj, Bihar, India, in 1975. He received the B.Sc. degree in computer engineering from Aligarh Muslim University, India, in 1998, the M.Tech. degree in computer engineering from Maharshi Dayanand University, Rohtak, in 2010, and the Ph.D. degree in computer science engineering from Mewar University, India, in 2015. From 1999 to 2006, he was a Lecturer with Maulana Azad College of Engineering and Technology, Patna. From 2006 to 2008, he was a Lecturer and a Senior Lecturer with Galgotias College of Engineering and Technology, Greater Noida. From 2010 to 2011 he was an Assistant Professor with GSMVNIET, Palwal. Since 2017, he has been an Assistant Professor with the Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia. He has published more than 30 research papers in journals and conferences of international repute and holds one patent of innovation. He also reviewed articles of differents journal, including *Sādhanā* (Springer) and *International Journal of Advanced Computer Science and Applications*. His research interests include algorithms, the IoT, cryptography, image retrieval, machine learning, and deep learning.