

Advanced Authentication and Energy-Efficient Routing Protocol for Wireless Body Area Networks*

Padma Vijetha Dev Bakkiahgari ^{*,†,‡} and K. Venkata Prasad ^{*,§}

**Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Guntur (Dist), Vaddeswaram 522502, India*

*†Department of Computer Science and Engineering,
Gokaraju Rangaraju Institute of Engineering and Technology,
Kukatpally, Hyderabad, India
‡padmavijetha@gmail.com
§prasad_kz@yahoo.co.in*

Received 25 February 2023

Revised 5 September 2023

Accepted 4 December 2023

Published 25 March 2024

Recently, wireless body area network (WBAN) becomes a hot research topic in the advanced healthcare system. The WBAN plays a vital role in monitoring the physiological parameters of the human body with sensors. The sensors are small in size, and it has a small-sized battery with limited life. Hence, the energy is limited in the multi-hop routing process. The patient data is collected by the sensor, and the data are transmitted with high energy consumption. It causes failure in the data transmission path. To avoid this, the data transmission process should be optimized. This paper presents an advanced authentication and energy-efficient routing protocol (AAERP) for optimal routing paths in WBAN. Patients' data are aggregated from the WBAN through the IoMT devices in the initial stage. To secure the patient's private data, a hybrid mechanism of the elliptic curve cryptosystem (ECC) and Paillier cryptosystem is proposed for the data encryption process. Data security is improved by authenticating the data before transmission using an encryption algorithm. Before the routing process, the data encryption approach converts the original plain text data into ciphertext data. This encryption approach assists in avoiding intrusions in the network system. The encrypted data are optimally routed with the help of the teamwork optimization algorithm (TOA) approach. The optimal path selection using this optimization technique improves the effectiveness and robustness of the system. The experimental setup is performed by using Python software. The efficacy of the proposed model is evaluated by solving parameters like network lifetime, network throughput, residual energy, success rate, number of packets received, number of packets sent, and number of packets dropped. The performance of the proposed model is measured by comparing the obtained results with several existing models.

Keywords: Wireless body area network; data security; energy efficiency; optimal path selection; network lifetime.

*This paper was recommended by Regional Editor Giuseppe Ferri.

†Corresponding author.

1. Introduction

Health monitoring on the Internet of Medical Things (IoMT) is widely used in wireless communication systems due to the authorized user's easy access to patients' health data. These kinds of monitoring systems improve the health conditioning of humans. The IoMT-based healthcare systems may attempt to monitor several healthcare things like body temperature, Electrocardiogram (ECG), Electroencephalogram (EEG) and Electromyography (EMG), blood pressure, hemoglobin level, abnormal muscle movement, etc.¹ through the wireless body area network (WBAN). This BAN can be placed inside or on the surface of the body.² This depends on the type of monitoring systems or type of monitoring required by the patients. Generally, the concept of medical monitoring requires several sensors to be fixed to the patient's body. The mentioned sensor nodes are termed body sensor units (BCUs). In these BSUs, the data are collected and forwarded to the body control unit (BCU). In BCU, the data are forwarded to the destination through the base station. The incessant monitoring of corresponding parameters executes efficient early warning and prevention methods.

The WBAN technologies are mainly utilized in several applications in the medical field. Also, it faces many challenges. The medical applications are feasibly related to WBAN and can be classified into professional and consumer. The sensor collects the physical information, processes that data, and then sends it to the local processing unit³ for the authenticated data transfer. The authenticated data transfer is through internet technology like Wi-Fi, GSM, Bluetooth, and WiMAX.⁴ Due to the use of these public resource-sharing systems, the data transmitted is not secure. The loop powered ultrasonic (LPU) processes the sensor data and finds the abnormality in data acquired from the patients' bodies. This is subjected to open resources with a high risk of involvement for the intruders. This raises the problem of whether the data gathered from the patient's body through BSN is real or not (true or not). Many kinds of attacks may happen on the wireless communication medium, such as encryption attacks, cyber-attacks, physical attacks, software attacks,⁵⁻⁷ etc. These attacks made the researchers look for efficient security and privacy-preserving schemes.

The energy-aware routing based on blockchain technology provides a lightweight and secure communication strategy⁸ but suffers from overhead on the network. The critical data routing is done by considering the on-body medical supersensor node.⁹ The model saves energy usage, but there is a problem of computation complexity. Authentication can be done by both cryptography-based and non-cryptography based. Cryptography involves key-based authentication (symmetric, asymmetric and hash function), whereas non-cryptography involves biometric, proximity and channel-based authentication. The Bilinear ElGamal cryptosystem¹⁰ is used for the health monitoring of remote systems. The authentication by multi-modal biometrics¹¹ could be applied for the WBAN, but the complexity analysis of the model is not performed. The secure crypto-based authentication is provided in Ref. 12 with a low execution time. The authentication scheme is provided by accelerating the data

in the WBAN between the legal and the node¹³ under transmission. If the nodes are attacked, there will be a false delivery of the information. The delay-aware healthcare monitoring system is proposed in Ref. 14 using an enhanced message authentication code (MAC)-based health monitoring system.

To improve the development of WBAN technology, various challenges are exhibited, like the requirement of quality of service (QoS), restricted node energy, heterogeneous data generation rate, dynamic network topology and reduced transmit power.¹⁵ Energy management is essential to improve the network's lifetime as energy resources in WBAN are restricted. A direct interaction between source and sink nodes absorbs extra energy because of the minimum range of communication and enhanced path loss in WBANs. The data in multi-hop communication are routed with the help of intermediate nodes, but it provides various constraints on the energy dissipation of the transmitted nodes. The secure three-party authentication protocol¹⁶ is used in WBAN. As a certificate with fewer authentication protocols, the cloud-aided lightweight is used¹⁷ to preserve anonymity and reduce storage load. But the system is not tolerable to the attack is a power-consuming protocol. Hence, these issues focus on the authentication, security and energy-efficient protocol for the WBAN-based IoMT. The main contribution of the proposed model is given as follows:

- Advanced authentication and energy-efficient routing protocol (AAERP) is designed for WBAN by enhancing security through encryption of sensed patient data.
- Developing an energy-efficient routing protocol using the teamwork optimization algorithm (TOA) to make optimal routing decisions between the IoMT and the medical centers.
- A reliable authentication system based on asymmetric cryptography is proposed to secure healthcare information from intruders in the network with high integrity to avoid harming the patients.
- The evaluations of the proposed model are extended with the existing security schemes in terms of different metrics.

This paper is summarized as follows. Section 2 describes the literature survey related to this work. Section 3 discussed the proposed methodology and system architecture. Section 4 explains the simulation results and discussion, and Sec. 6 concludes.

2. Related Work

Several techniques are proposed in the literature to deal with the aggregation, authentication and routing problems in WBAN. For the data authenticated scheme related to IoMT, Mahendran *et al.*¹⁸ proposed the fuzzy extractor with a fuzzy vault approach for security. The fuzzy extracted features, such as QRS, QT and PR interval, are used to process the private key biometric authentication process.

These functions generated the private key that allowed the user to access the medical data. The IP address of the end local processing unit was used to determine the bit rate of the data retriever, which will be used in the decoding section as a public key. Here, the independent hash variables were used to enhance the security of the data transmission network. Azeem *et al.*¹⁹ proposed an efficient and secured data transmission and aggregation (ESDTA) scheme based on FoG. The proposed efficient and secure data transmission and aggregation scheme utilized a secure message aggregation and decryption algorithm between the mobile node and the fog node. The fragmentation principle shared the session key between the user and the authentication device. The data is collected and processed after encryption at the sensor node instead of the fog node. The redundant data was removed at the fog node itself.

Cano and Sanchez proposed a dual signature-based data privacy scheme.²⁰ To frame that, the elliptical curve digital signature algorithm (ECDSA). The solution improved security and privacy between the IoMT and cloud devices through the edge device. The invariable hash functions were used between the cloud and IoMT for the dual signature between the encryption and decryption. The complexity and computational cost for the proposed algorithm with dual signature were lesser than the other methods. Using the blockchain, Arul *et al.*²¹ proposed the multi-modal secure data dissemination framework (MMSDDF) through IoMT devices. The proposed multi-modal scheme provides controlled access to the patients' data concerning blockchain technology. The IoMT devices will store the data on the off-chain database and blockchain using the timestamp and transaction hash. The method was evaluated with a lesser delay of 0.48 s, having a response time of 1.5% reduced from the other models.

The routing protocols designed for traditional sensor networks cannot be directly implemented in the WBAN due to the changes in the network's topology. To maintain the functionalities of the WBAN applications, Ullah *et al.*²² developed a clustering mechanism-based routing protocol following two major phases. The two-phased techniques were named energy-efficient harvested-aware clustering and cooperative routing protocol (E-HARP) for WBAN. It involved a dynamic cluster head (CH) selection and cooperative routing phases. A multi-attribute-based technique was designed to select optimal CHs for data transmissions by reducing cost. Finally, routing was carried out to reduce energy consumption in the sensor nodes with the prohibition of redundant data packets. The model experimented with the NS-2 simulation tool, and the performance metrics such as throughput, packet delivery ratio, network stability, end-to-end delay and network lifetime were considered for evaluation.

Since several nodes are present in a WBAN for effective monitoring of patient's health information, reliability and power consumption have become crucial issues to be addressed to gain better performance. With this in mind, Geetha and Ganesan²³ introduced a new protocol, cooperative energy efficient and priority-based reliable routing protocol with network (CEPRAN) coding, that enhanced

the energy-efficiency reliability of WBAN. The model was built with two major phases: the first phase worked on data forwarding, and the second phase worked on improving the packet transfer rate. The authors introduced an enhanced cuckoo search optimization algorithm to identify the relay node from the nodes in the network for data forwarding. Then, a cooperative random linear network coding approach was fused into the obtained relay node to improve the transmission rate. CEPRAN was implemented in the NS-3 simulator, and the results suggested that the protocol outperformed the existing protocols.

Due to the resource-constrained nature of the WBAN nodes, efficient and reliable data transmissions are highly important to achieve better performance. Thus, Ullah *et al.*²⁴ formulated a solution called the energy efficient and reliable routing scheme (ERRS) to improve the reliability and stability period of the resource-constrained WBAN. The approach involved four phases: node deployment and initialization, forwarder node selection, data transmission, and load balancing. The first three phases performed the initial operations, such as data gathering for the WBAN application. In contrast, the final phase was reached after numerous rounds of data collection reached the predefined threshold. In this approach, a forwarding rotation technique was used to ensure equal load balancing between nodes and to allow all sensor nodes in the network to become forwarding nodes. The experimentations of the approach were conducted in Matlab, and the metrics such as stability, throughput and delay were considered for evaluation.

To solve the energy consumption problem, Qu *et al.*²⁵ proposed an energy-efficient routing protocol in WBAN. Several parameters are taken, such as bandwidth, energy efficiency, residual energy and amount of hops. Priority-based energy efficient approach (PERA) and modified new-attempt (NEW-ATTEMPT) routing protocol are used for comparison analysis. In this, several challenges have occurred. Ahmad *et al.*²⁶ develop a reliability enhanced-adaptive threshold-based thermal unaware energy-efficient multi-hop protocol (RE-ATTEMPT) model for WBAN with improved energy efficiency. This model utilizes several sensor nodes, which are placed based on the energy level. The developed model chooses a route with a reduced hop count to transmit data. The delay factor is decreased in this model.

The authentication of healthcare data is poor due to the data transmission through the open source. The major focus is improving the authentication of the data transmitted over a network. The existing protocols for authenticated routing focused more on optimal routing than authentication, a critical issue requiring major attention. Some newer techniques reduce the computing power and runtime of the protocols. This is also an important issue that needs to be addressed, but these protocols are not effective enough to maintain trust from both parties. Additionally, the percentage of successful key recovery for these systems is less than 100%. A recent survey on secured routing protocols in WBANs found that network optimization should focus on improving performance. Moreover, advanced and low-overhead security protocols are needed to meet all the security constraints. For resource-constrained networks, the symmetric encryption schemes are advantageous

in handling the data in WBAN. However, these schemes use only one key, and it isn't easy to maintain integrity and security in this scenario. The authentication is improved by implementing an advanced security protocol combining asymmetric with the partially homomorphic encryption scheme to overcome these issues.

3. Proposed Methodology

This paper proposes AAERP to enable optimal routing between IoMT and medical centers with high security for patient data. Initially, the data are aggregated from the WBAN through the IoMT devices from the hospitals. The transmission path between the IoMT and the medical centers is prone to intrusions. Thus, the proposed work combines the elliptic curve cryptosystem (ECC) and Paillier cryptosystem for the data encryption process. The data before transmission is authenticated using a hybrid data encryption algorithm for security. This system converts the original data into cipher-text before routing. This data encryption process helps to prevent the tracing of sensitive information. A TOA is introduced to route the data optimally to the servers.

The routing process is performed to forward the cipher text. Each route is evaluated iteratively to improve the effectiveness and robustness of the system. This optimization provides a low cost with higher energy efficiency to enhance the lifetime of the network. Figure 1 shows the schematic diagram of the proposed model. The complexity associated with the proposed data aggregation procedure is NP-hard, and the complexity associated with the ECC encryption procedure is $O \log 2$. The complexity of the Paillier cryptosystem is $O(\log(N)3)$. The computational burden is lower than other traditional approaches to data encryption. Therefore, the communication costs are not increased by the data aggregation and the proposed hybrid encryption method.

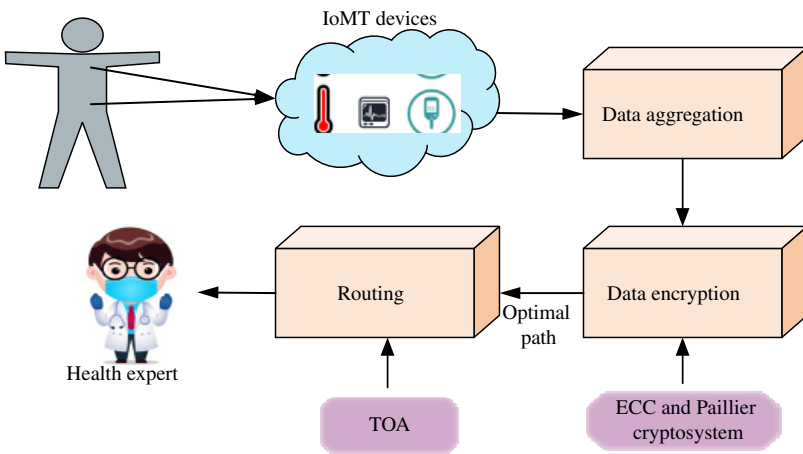


Fig. 1. Schematic diagram of proposed model.

3.1. System architecture

The WBAN architecture has several sensors placed on the human body to notify the changes in parameters. The sensor nodes capture the parameters and transmit the information to a sink node. A sink node is also positioned on the human body or else located outside of the body. A sink node interacts with this information to intermediate devices. The intermediate devices could be devices or personal digital assistants (PDAs). It receives the information from the sink node and interacts with that as per their need or as per the guidance forwarded to needed organizations such as ambulance services, databases for maintaining records and medical centers. The benefits of reduced-size, wearable sensors in WBASN are carried around with the body without difficulty. A Holter monitor only senses up to reduced hours, and electrodes are attached to a device that must be carried endlessly. The monitoring time is unrestricted in WBAN, and the time is maximized compared to other tools. Sensor nodes are processed with physiological parameters in which the information is processed to interact with other services. The sensors are generally operated by using a battery. Small-size batteries are used due to the size of the sensors are small. The batteries have a limited capacity for energy sources. The sensors are placed on different parts of the human body to observe the parameters. The proposed work utilized heart rate, systolic blood pressure, diastolic blood pressure, pulse rate, respiratory rate, and oxygen saturation for measuring human health were sensed by utilizing the sensors as observed. The system architecture of WBAN is shown in Fig. 2.

3.2. Data aggregation

Data aggregation is collecting a high volume of data from a provided database and arranging it into a more usable and extensive medium. Data aggregation is

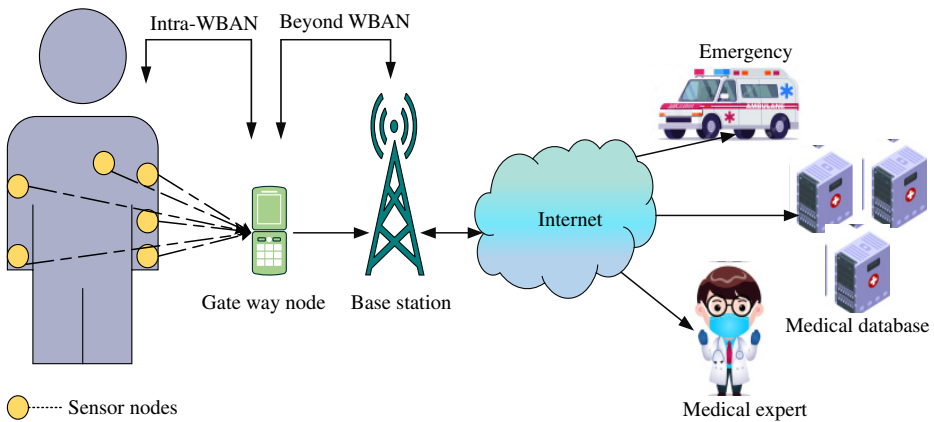


Fig. 2. System architecture of WBAN.

supported to assemble the data from multiple, disparate and numerous sources. It improves the information value and reduces the performance problem. The major intention of data aggregation is to collect and aggregate the data in an energy-effective way; thus, the network's lifetime gets improved. The proposed work collects heart rate, systolic blood pressure, diastolic blood pressure, pulse rate, respiratory rate and oxygen saturation data from the human body through the IoMT devices. The health data collected from the patients face several security issues, and it is important to ensure security before transmission. The proposed methodology improves the security of the health data by encrypting the data before finding the optimal path for transmission. For this purpose, the data are initially aggregated from the patients. Several IoMT devices are located in or out of the patient's body to collect the patient's health information. All patient information is collected via the sensors and stored on the cloud servers for further processing.

3.3. Data encryption

The sensitive private information transmitted over communication channels is not very secure because of the increasing number of attackers who trace private information. Cryptography is introduced to protect the individual's private data. Data privacy controls access to information, which can be enabled through an encryption procedure. With the encryption procedure, the data is accessed by the user with the encryption key. The encryption process is significant for transmitting the data over the internet. Encrypted data can only be accessed with a decryption procedure. The data are initially converted into cipher text in the encryption process of the cryptography system. After that, the cipher text is converted into plain text in the decryption process. The proposed model combines the ECC approach with the Paillier cryptosystem to improve the security of patients' private data. By using the ECC approach, the private and public keys are generated. The encryption and decryption processes are then carried out using the Paillier cryptosystem. In addition, the encryption process ensures reliability and authentication.

3.3.1. ECC approach

An ECC approach is a secure platform to protect the patient's private data. The public key encryption model generates a smaller, faster, more effective cryptography key. The proposed ECC approach generates the key for further encryption and decryption process. This approach offers a minimized key size, reduced storage space, and increased security. Like RSA, an ECC can attain the same level of security in the problems of discrete logarithms with minimized computation. Based on the elliptic curve, the ECC approach is employed. The coefficients and variables of elliptic curves are all limited to elements of a restricted field, proving extra efficiency in the ECC operation. An example of an elliptic curve is illustrated in Fig. 3.

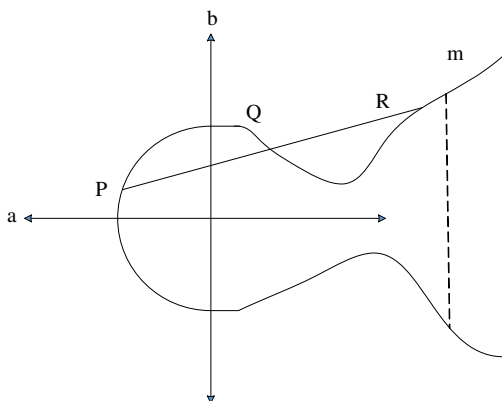


Fig. 3. Given the example of the elliptic curve.

Let us consider an elliptic curve

$$b^2 = a^3 + pa + q, \tag{1}$$

where p and q are the coefficients of the elliptic curve.

Consider $E_n(p, q)$ as an elliptic curve, and the following equation is

$$Q = kP, \tag{2}$$

where P and Q are considered by the two points in $P \in E_n(p, q)$ curve and k is less than m . In Eq. (2), it is not very difficult to determine Q were k and P are given, but trouble will occur in the evaluation of k . This is due to the trapdoor function, or a single-way function termed a discrete logarithm.

Key exchange based on ECC

$E_n(p, q)$: The parameters of the elliptic curve p, q and n

: n is an integer or prime in the 2^x form.

X : Point on the elliptic curve, and the order is a higher value m .

Key generation using ECC

Two keys are generated in the key generation process, such as private and public keys. The private key is used to receive the information of the patient, and the public key is used to encrypt the patient's information. Consider two patients, Alice and Bob, whose private key is exchanged over an insecure network, like the following concepts:

The private key of Alice is

$$K_P = R_P. \tag{3}$$

The public key of Bob is

$$K_Q = R_Q. \tag{4}$$

From Fig. 3, R_P and R_Q should be lower than m . The evaluation of public key of Alice is

$$Z_P = R_P * X. \quad (5)$$

The evaluation of the public key of Bob is given as

$$Z_Q = R_Q * X. \quad (6)$$

From this, the evaluation of the private key can be performed. The private key calculation of Alice is given as

$$Y_P = R_P * Z_Q. \quad (7)$$

The private key formulation of Bob is defined as

$$Y_Q = R_P * Z_P. \quad (8)$$

Thus, the keys are generated based on the ECC approach, and by using these keys, the encryption and decryption process is performed by the Paillier cryptosystem.

3.3.2. Encryption using Paillier cryptosystem

Paillier cryptosystem is one of the homomorphic encryption approaches that helps to encrypt the data by avoiding online attackers. The proposed work utilizes a Paillier cryptosystem for the encryption and decryption process. In the encryption process, the public key has to encrypt each patient's data, which can be considered a message bit and the cipher text is evaluated.

Based on the Paillier cryptosystem, the encryption process is done by evaluating the cipher texts as

$$C = v^x l^y \text{ mod } y^2. \quad (9)$$

In this encryption process, the patient's private data are encrypted by converting the plain text into cipher text with the help of a hybrid mechanism. After completing the encryption approach, the encrypted data are optimally routed.

3.4. Routing

Routing is the next important phase in determining the optimal transmission path. After the encryption of medical information, the path to transmit the data to the medical centers in an energy-efficient way must be identified. All the nodes in the network hold the same amount of energy at the time of deployment. This energy slowly fades during the time of broadcasting, transmitting and receiving data. The energy consumption on these operations varies for the number of hops required between the source and destination nodes. Thus, the optimal path between the source and destination is determined by minimizing the number of hops and their distance. The proposed approach introduces a novel optimization algorithm called

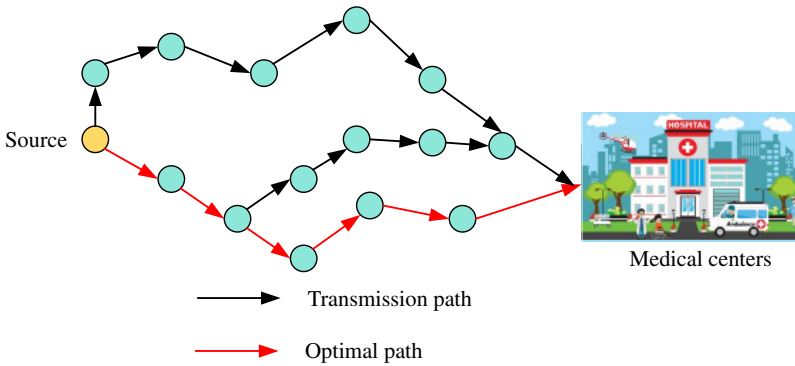


Fig. 4. Routing process for optimal path selection in WBAN.

the TOA to determine the optimal route between the nodes. TOA is the latest optimization algorithm that is inspired by the teamwork behavior of the members of a team in performing a task. This algorithm minimizes the objectives to identify the optimal path from the network for data transmission. After this step, decryption is performed at the medical centers to retrieve the original health information of the patients. The process of routing in optimal path selection is shown in Fig. 4.

3.4.1. Proposed TOA for the routing process

The TOA is one of the population-based optimizations constructed according to the simulation of behaviors and relationships of team members in processing their work demands and attaining the desired aim of the team. Hence, in the TOA approach, the search agents are considered the team members. The relation between each team member helps to forward the information, and the team's objective is the solution to the problem of optimization. The team that performs teamwork to obtain a similar goal, the behavior and relationship of team members can be represented as supervisor, team members, the influence of best members on worst team members, and activities of individual members. The following three stages of the TOA algorithm are supervisor guidance, information sharing and individual activity.

When considering multi-objective optimization, the fitness value is estimated with more than two objectives. The distance, throughput and residual energy are considered in the objective function for finding the optimal path. Multi-objective is a vector optimization that tradeoff between two or more conflicting objectives. In real-time applications, the optimization problem should consider more objectives. Instead of a single solution, a set of non-dominated solutions are obtained. It is based on the representative set of detecting optimal solutions. The fitness value is evaluated by considering the entire objective for performance enhancement. Finally, the optimal solution is selected with the best fitness value.

3.4.1.1. Fitness function

To identify the optimal path using the TOA approach, each path's fitness value is required. This fitness value will be utilized to choose the optimal solution for TOA. The proposed work performs the multi-objective function for finding the optimal routing path. The path with reduced distance between the nodes will be considered as the better optimal solution. The fitness function is considered the objective function for the presented algorithm. The node distance is evaluated as

$$D_{ij} = \sqrt{(m_i - m_j)(n_i - n_j)}, \quad (10)$$

where (m_i, n_i) and (m_j, n_j) mention the coordinates of nodes i and j correspondingly, D_{ij} represents the distance between the nodes. Throughput is the second objective function used to evaluate the proposed model. The maximization of throughput is considered an objective function of the presented framework. The computation of throughput is represented as

$$\eta = \frac{T + D_r}{d}, \quad (11)$$

where η denotes the throughput function, and it is considered the deciding factor of the fitness function to identify an optimal routing path for transmitting the patient's private data. T signifies the throughput, D_r represents the data rate and d is denoted by delay in the network. The third objective function of the proposed framework is residual energy. The minimization of residual energy is assumed as the objective function of the proposed work. The evaluation of residual energy is given as

$$RE_i = I_0 - TE_i, \quad (12)$$

where RE_i mentions the residual energy of i th node, I_0 is denoted by the initial energy of each node, TE_i represents the total energy consumed by i th node. Thus, the fitness function is given as

$$\text{Fitness function} = \eta + 1/D_{ij} + 1/RE_i. \quad (13)$$

In the proposed TOA approach, each population individual mentions the solution to the optimization problem. Based on the TOA approach, the initialization of the search agent is represented as

$$P = \begin{bmatrix} P_1 & p_{1,1} & \cdots & p_{1,h} & \cdots & p_{1,l} \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ P_i & p_{i,1} & \cdots & p_{i,h} & \cdots & p_{i,l} \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ P_N & p_{N,1} & \cdots & p_{N,h} & \cdots & p_{N,l} \end{bmatrix}_{N \times l}, \quad (14)$$

where P is considered by the matrix of search agent of the TOA approach, N denotes the number of search agents, h is the problem variable recommended by

the search agent i and l is the number of problem variables. As described above, each search agent of the algorithm population provides values for the problem variables. By locating these values in the variables of the objective function, a target value function is achieved. Hence, depending on the search agent of the population, the value is calculated for the goal function. The vectors of the values of the objective function are formulated as

$$V = \begin{bmatrix} V_1 & V(P_1) \\ \vdots & \vdots \\ V_i & V(P_i) \\ \vdots & \vdots \\ V_N & V(X_N) \end{bmatrix}_{N \times 1}, \quad (15)$$

where V is represented by the vector of the objective function and the value of the objective function of the search agent i . The path that the search agent chooses in each iteration is updated and compared to the fitness function. The attained value with the best performance by satisfying the fitness function is selected as the supervisor in the search agent. The selection of supervisor in the TOA approach is given as

$$S = P_r, \quad (16)$$

where r is denoted by the row number of the search agent with a reduction of vectors V , S represents the supervisor in the search agent team. In the TOA approach, the population of search agents is updated in three stages.

First stage: Supervisor guidance

In the initial stage, the search agents are updated depending upon the supervisor's guidance. Also, the search agent team supervisor shares the information, forwards it to another agent, and instructs toward attaining the intention. The stage is updated as

$$P_i^{S_1} : p_{i,h}^{S_1} = p_{i,h} + a \times (S_h - U_I \times p_{i,h}), \quad (17)$$

$$P_i = \begin{cases} P_i^{S_1}, & V_i^{S_1} < V_i, \\ P_i, & \text{else,} \end{cases} \quad (18)$$

$$U_I = \text{round}(1 + a), \quad (19)$$

where $P_i^{S_1}$ represents the new status of the search agent i according to the guidance of a supervisor. The value of an objective function is denoted as $V_i^{S_1}$, the new value for the problem variable h recommended by the search agent i updated depending on the instructions of the supervisor is denoted as $p_{i,h}^{S_1}$, the update index is mentioned as U_I and a random number ranging from 0 to 1 is denoted as a .

Second stage: Information sharing

In this stage, each search agent attempts to utilize the information of other search agents who have processed better performance than others. This stage is updated by the following equations:

$$P^{L,i} : p_h^{L,i} = \frac{\sum_{j=1}^{N_i} p_{j,h}^{c,i}}{N_i}, \quad (20)$$

$$P_i^{S_2} : p_{i,h}^{S_2} = p_{i,h} + a \times (p_h^{L,i} - U_I \times p_{i,h}) \times \text{sign}(V_i - V^{L,i}), \quad (21)$$

$$P_i = \begin{cases} P_i^{S_2}, & V_i^{S_2} < V_i \\ P_i, & \text{else} \end{cases}, \quad (22)$$

where $P^{L,i}$ represents the average of the search agent, which is excellent than the search agent i , the value of the objective function is denoted as $V^{L,i}$, the number of search agents with improved performance than the search agent i is represented as V_i , the value of the h variable recommended by the excellent search agent j for the i th search agent is given as $p_{j,h}^{c,i}$, the new status for the i th search agent depends on the second stage is denoted as $P_i^{S_2}$ and the value of the objective function is mentioned as $V_i^{S_2}$.

Third stage: Individual activity

In the third stage, each search agent attempts to enhance their performance depending on the current situation. This stage is updated by

$$P_i^{S_3} : p_{i,h}^{S_3} = p_{i,d} + (-0.01 + a \times 0.02) \times p_{i,d}, \quad (23)$$

$$P_i = \begin{cases} P_i^{S_3}, & V_i^{S_3} < V_i \\ P_i, & \text{else,} \end{cases} \quad (24)$$

where $P_i^{S_3}$ is considered as the new status for the search agent i depends on the third stage and the value of an objective function is denoted as $V_i^{S_3}$. In every iteration, the search agents of the population are in three stages based on the above equations. The process of updation is continued until the TOA algorithm meets the stopping condition. After the overall implementation of the proposed algorithm, the TOA provides the optimal solution to an optimization problem. The algorithm of the TOA approach is illustrated in Table 1.

3.4.1.2. Decryption

The information is transmitted to the medical centers after identifying the optimal path with the TOA approach's aid. The medical centers decrypt this information by using a private key. The information is decoded from the ciphertexts and other hidden parameters in the decryption stage. The ciphertext C to be encrypted and

Table 1. Pseudocode of proposed TOA algorithm for optimal routing path.

```

begin TOA
Input: The problem information including Variables, constraints and objective function
Assign the number of iterations ( $t$ ) and team members ( $N$ )
Initialize random matrix for team members
Compute the objective function
  For  $n = 1 : t$ 
    Update supervisor using equation (16)
    For  $i = 1 : N$ 
      First stage: Supervisor guidance
      Update  $P_i$  according to first stage using equations (17) and (19)
      Second stage: Information sharing
      Find best search agents and  $N_i$  for search agent  $i$ .
      Evaluate according to equation (20)
      Update  $P_i$  according to the second stage using equations (21)
      and (22)
      Third stage: Individual activity
      Update  $P_i$  according to the third stage using equations (23)
      and (24).
    End for  $i = 1 : N$ 
    Save the optimal routing path attained with the TOA approach so far
  End for  $n = 1 : t$ 
Output better optimal routing path attained with the TOA
End TOA

```

the plain text to be evaluated as

$$P = \frac{H(C^\lambda \bmod y^2)}{H(v^\lambda \bmod y^2)} \bmod y. \quad (25)$$

After routing the data to the medical centers with optimal path, the information is decrypted by using Eq. (25). The proposed framework effectively transmits the data from IoMT devices to the medical centers.

4. Results and Discussion

The proposed framework is simulated in Python software version 3.9. The hardware configuration and specific framework of the proposed approach are listed in Table 2.

The dataset information is collected by placing six sensor nodes in the human body. The sink node is located outside the body for collecting the data. It collects information on the human body in terms of heart rate, systolic blood pressure, diastolic blood pressure, pulse rate, respiratory rate and oxygen saturation. The performance of the proposed model is evaluated by comparing the present work with various existing approaches like Priority based Energy-efficient Routing Algorithm (PERA), newATTEMPT, Energy Efficient Routing Protocol (EERP), Adaptive Threshold-based Thermal-aware Energy-efficient Multi-hop Protocol (ATTEMPT), and Reliability Enhanced (RE)-ATTEMPT. For performance evaluation, parameters like network lifetime, throughput, residual energy, success rate, total packet drop, total packet received and total packet sent are computed.

Table 2. Hardware and software configuration.

Hardware requirement		
Sl. No.	Hardware type	Specification
1	Processor	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00 GHz 2.99 GHz processor
2	Storage	195 GB
3	RAM	8.00 GB
4	Display	SVGA monitor resolution \times 768
Software requirement		
Sl. No.	Software type	Specification
1	Operating System	Windows 10 Pro

Table 3. Simulation parameters.

Number of sensor nodes	6
Number of sink	1
Initial energy	0.5 J
Packet size	128 bits
$E_{TX-elec}$	15 J/bits
$E_{RX-elec}$	35 J/bits
E_{amp}	2 Nj/bit/mn

The attained results are compared with the previous methods to measure the efficacy of the proposed techniques. The simulation parameters of the proposed framework are illustrated in Table 3.

4.1. Network lifetime

The lifetime of the network is described as the amount of time taken in rounds from the initial network process to the death of the last node. The period from the beginning of the network up to the initial node processed without battery is the stability duration of the network. Figure 6 illustrates a network lifetime comparison of the proposed work with existing techniques like PERA, NEW ATTEMPT, and EERP. This clearly shows that the proposed framework is more excellent than the other techniques in terms of network lifetime by verifying the experimental results. The previous PERA model chooses the node with reduced hops to sink as the better next hop. This PERA protocol minimizes the transmission delay but generates extra energy losses because of the highest distance of transmission. According to this, the PERA protocol is not a better choice in WBAN. A cost function is utilized in the NEW-ATTEMPT protocol to choose the optimal next hop node. However, the only drawback is that the cost function cannot consider the overall reliability transmission between the nodes. Thus, it leads to failure of data transmission and higher retransmission. Also, it maximizes energy consumption and influences the lifetime of the network. The EERP framework has several weight values, which

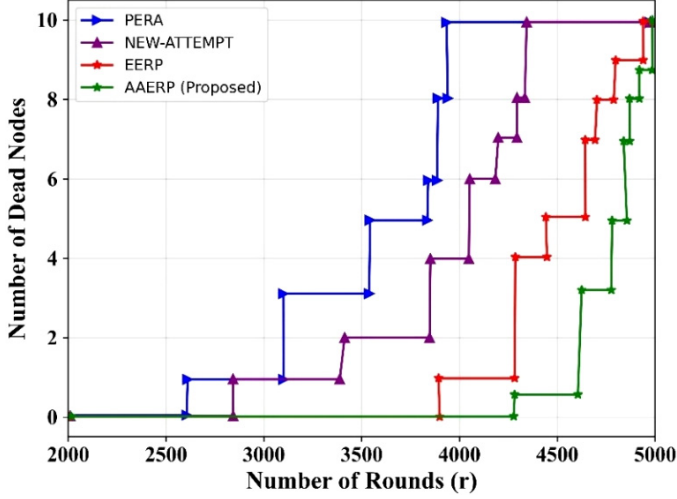


Fig. 5. Network lifetime analysis by varying the number of nodes.

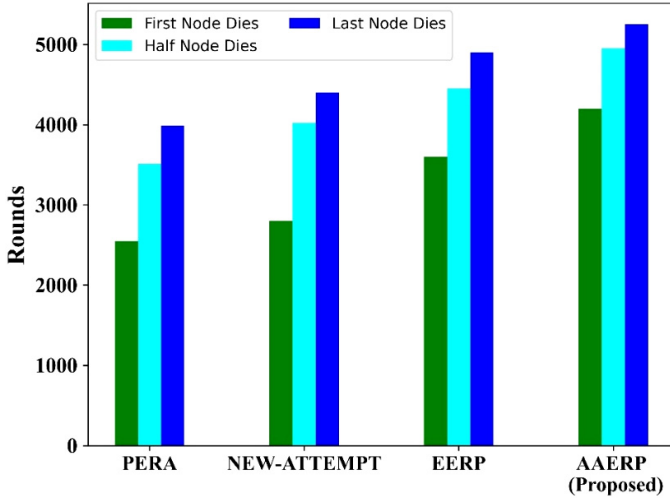


Fig. 6. Network lifetime analysis of the proposed model with the existing frameworks.

are not very reasonable. Thus, the requirement of QoS is not satisfied; hence, it becomes a drawback of the EERP model. In the proposed AAERP model, energy usage efficiency is improved, and the network lifetime is extended. Figure 5 compares the proposed model’s network life with existing techniques.

Figure 5 proves that the proposed model attains an improved network lifetime than the previous works. The throughput of the network is evaluated by varying the number of nodes and number of dead nodes in the network.

Table 4 reveals that the previous methods attain a reduced network lifetime than the proposed AAERP framework. In Fig. 6, the first dead node appeared after

Table 4. Analysis of the network lifetime of the proposed model with existing protocols.

	PERA	NEW-ATTEMPT	EERP	AAERP (proposed)
First node dies	2604	2852	3548	4200
Half node dies	3510	4020	4450	4950
Last node dies	3990	4400	4900	5250

4,000 rounds, but in the previous models PERA, NEW-ATTEMP, and EERP, the initial dead node is 2,604 rounds, 2,852 rounds and 3,548 rounds, respectively. The half-dead node that appeared for the proposed model is 4,950 rounds, PERA is 3,510 rounds, NEW-ATTEMPT is 4,020 rounds, and EERP is 4,450 rounds. The last dead node of the proposed framework is 5,250 rounds, PERA is 3,990 rounds, NEW-ATTEMPT is 4,400 rounds, and EERP is 4,900 rounds. This reveals that the proposed framework enhances energy efficiency and improves the lifetime of the network.

4.2. Network throughput

The throughput of the network is defined as the total amount of successful data forwarded to the destination node. The throughput of the proposed model is compared with the existing frameworks like PERA, EERP, and NEW-ATTEMPT. The previous methods attained minimized network throughput because the reliable interaction between nodes is not considered. Therefore, it also affects the throughput of the network, while the stability and lifetime of the network were reduced in the previous techniques. Hence, the throughput is minimized. In the proposed model, the transmission efficiency is improved and thereby, reliable interaction between nodes is performed. Hence, the successful data transmission is enhanced, leading to improved throughput of the network. The performance comparison of proposed and existing models in terms of throughput is shown in Fig. 7.

Table 5 illustrates that the proposed AEERP model achieves improved throughput of a network than the existing works. The attained throughput of the proposed AAERP model at round is 53.81, at round 1,000, the throughput is 2206.08. At round 2,000, the throughput of the network is 2984.51, at round 3,000, the obtained throughput is 3412.83. At round 4,000 the attained throughput is 3733.32. At round 5,000, the network throughput is 3824.94. This results analysis reveals that the proposed model attains improved through of network than others.

4.3. Residual energy

The energy efficiency of the proposed model is analyzed by determining the utilization of energy in each of the rounds. The evaluation results prove that the proposed model attains improved energy efficiency than the previous frameworks like PERA, NEW-ATTEMPT, and EERP. The PERA model rejects the curve quickly due to

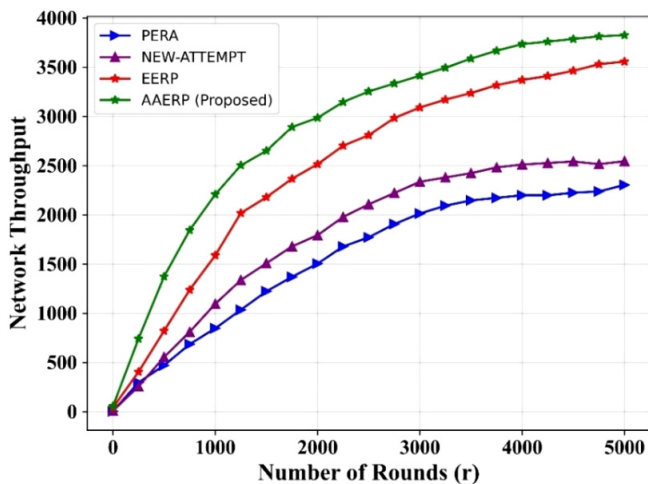


Fig. 7. Network throughput analysis of the proposed model with existing works.

Table 5. Network throughput comparison of proposed and existing protocols.

Rounds	0	1000	2000	3000	4000	5000
PERA	2.87	845.75	1503.03	2012.14	2197.94	2303.09
NEW-ATTEMPT	8.27	1094	1792.18	2334.93	2510.34	2544.1
EERP	40.34	1586.52	2513.15	3089.55	3369.72	3555.57
AAERP (proposed)	53.81	2206.08	2984.51	3412.83	3733.32	3824.94

the simple routing technique. Because of the enlarged communication distance, the routing model with a reduced hop count will make a minimum feasibility of successful data transmission. Hence, more energy from the PERA model is utilized for data retransmission, and the utilization of energy efficiency is minimized. Also, the NEW-ATTEMPT and EERP protocols cannot consider reliable parameters in constructing cost function, which improves the transmission failure rate. Thus, the previous protocols attain seduced energy efficiency than the proposed AAERP model. Figure 8 compares the attained residual energy of proposed and existing models.

Figure 8 proves that the proposed model attains improved residual energy than the previous protocols. The residual energy is computed by varying the number of rounds. The obtained residual energy proposed from the rounds 0 to 5,000 is 4.01 J, 3.71 J, 3.37 J, 2.9 J, 2.53 J, 2.21 J, 1.94 J, 1.65 J, 1.31 J, 1.01 J, 0.73 J, 0.49 J, 0.31 J, and 0.12 J. These results show that the proposed AAERP model has improved residual energy. It attains better performance than the existing protocols.

4.4. Success rate

The success rate is defined as the protocol that allows reliable transmission of improved priority data, and it is essential to detect and record the priority data.

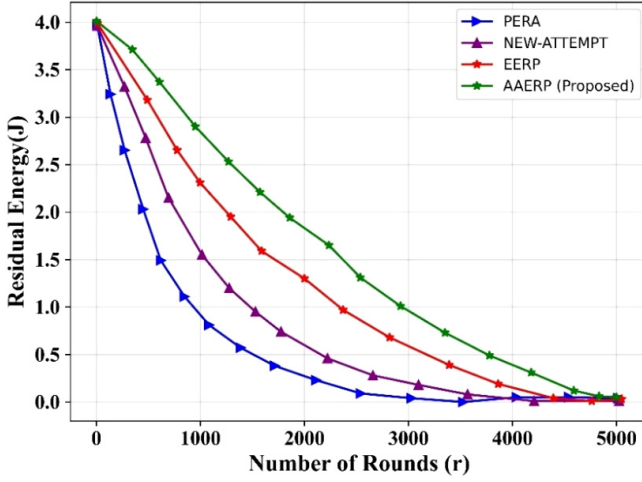


Fig. 8. Residual energy of proposed framework and existing protocols.

The route with reduced hops is not guaranteed reliable data transmission in the PERA protocol. Also, the NEW-ATTEMPT model cannot consider the data priority; hence, it has diminished the reliable data transmission, and the EERP model cannot achieve an enhanced success rate. The proposed AAERP model attains an improved success rate of the network by enhancing reliable data transmission. The obtained success rate of the proposed model is shown in Fig. 9.

In this figure, the success rate of the proposed model is evaluated by varying the time and the efficacy of the proposed model is measured by comparing the success rate of the proposed protocol with the existing methods.

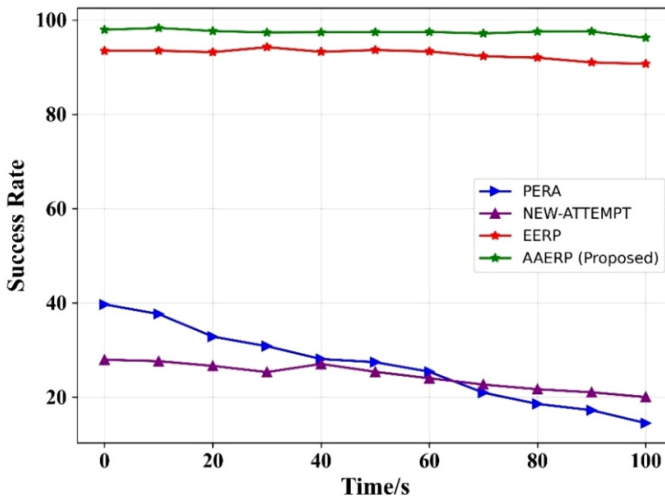


Fig. 9. Success rate comparison of the proposed and existing framework.

Table 6. Success rate comparison of the proposed framework with existing models.

Time/sec	0	20	40	60	80	100
PERA	39.65	32.83	28.07	25.38	18.55	14.48
NEW-ATTEMPT	27.93	26.62	27.04	24	21.66	20
EERP	93.45	93.17	93.24	93.31	92	90.69
AAERP	97.93	97.66	97.38	97.45	97.52	96.21

Table 6 illustrates the success rate of the proposed and previous models. The success rate of the proposed work is compared with the existing techniques like PERA, NEW-ATTEMPT, and EERP. At 0s, the success rate of the proposed model is 97.93%; at 20s, the success rate is 97.66%; at 40 sec, the success rate of the proposed model is 97.38%. In 60s, the success rate is 97.45%, in the 80s, the success rate is 97.52%; and in the 100s, the success rate of the proposed model is 96.21%. This result proves that the proposed model improved success rate than other models.

4.5. Packet sent

A packet in a network is a small number of data transmitted over the protocols. In general, a packet is the unit of data routed from source to destination on the network system. The proposed protocol sent more packets because of reduced multi-hopping and enlarged network lifetime. The amount of packets sent of the proposed and existing model is shown in Fig. 10.

Table 7 resembles the comparison of the number of packets sent of proposed and previous techniques such as ATTEMPT and RE-ATTEMPT. At round 0, the

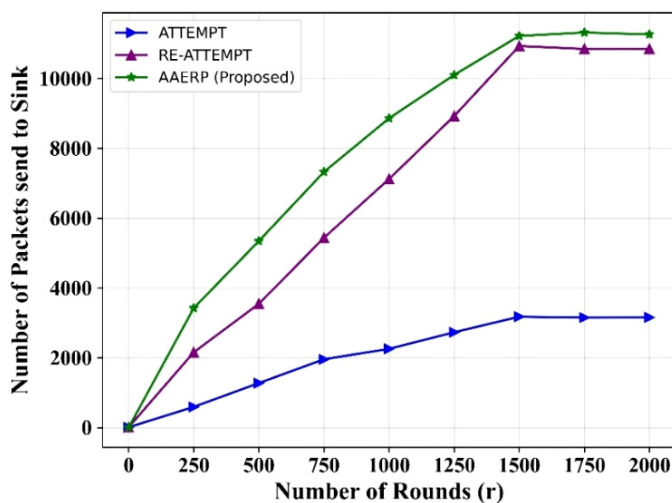


Fig. 10. Number of packets sent of the proposed and existing framework.

Table 7. Amount of packets sent comparison of the proposed and existing model.

Rounds	0	250	500	750	1,000	1,250	1,500	1,750	2,000
ATTEMPT	9	593	1275	1957	2256	2731	3,177	3,152	3,155
RE-ATTEMPT	8	2,157	3,546	5,437	7,121	8,924	10,933	10,849	10,852
AAERP	0.12	3,424	5,345	7,324	8,861	10,103	11,222	11,320	11,264

average amount of packets sent in the proposed model is 0.12. At round 250, the number of packet sent is 3,424; at round 500, the 5,345 packets are sent. At round 750, the number of packets transmitted is 7,324; at round 1,000, the packet transmitted is 8,861; at round 1,250, 10,103 packets are sent. At round 1,750, the number of packets sent is 11,320; at round 2,000, the number of packets sent is 11,264. This result analysis shows that the proposed model has enhanced the number of packets sent to the sink node.

4.6. Packet drop

When accessing the network, the packets are transmitted and received generally. When some packets fail to reach the destination, it is termed packet drop. The minimized packet drop leads to improved performance of the network. The previous models, like RE-ATTEMPT and ATTEMPT, have network congestion and inadequate infrastructure. Thus, it results in enhanced packet drops in the network system. Figure 11 illustrates the packet drop of proposed and existing models.

The above figure shows that the proposed model has reduced packet drop compared to the existing methods like ATTEMPT and RE-ATTEMPT. The packet

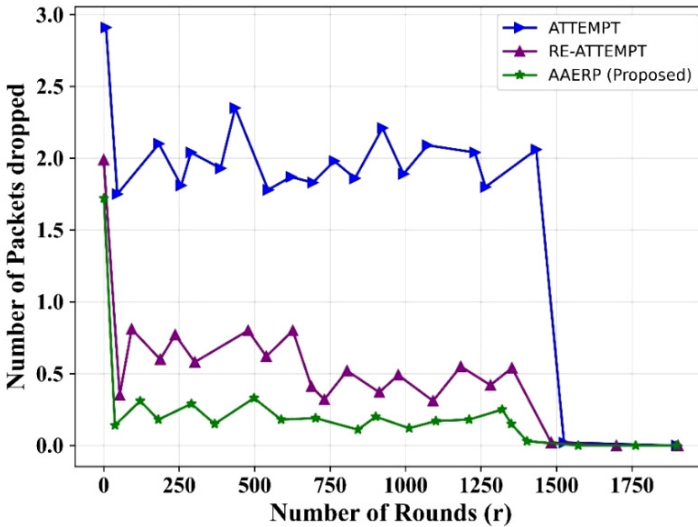


Fig. 11. Number of packets dropped in proposed and existing models.

drop is measured by varying the number of rounds from 0 to 1,750. The proposed model attains a reduced packet drop for each round than others.

5. Packet Received

The number of packets that are successfully received is discussed in this analysis. The proposed AAERP framework is more reliable than the other two existing methods. Due to the improved reliability, the amount of packets received is improved in the proposed model. The performance of a proposed model in terms of the amount of packet received is compared with the previous models like ATTEMPT and RE-ATTEMPT. Figure 12 compares a packet received in the proposed and state-of-the-art models.

Table 8 describes the analysis of the total number of packets received in the proposed and existing models. Compared with the ATTEMPT and RE-ATTEMPT models, the proposed AAERP model received more packets. At round 250, the proposed model received packets of 1,685; at round 500 the received packets are 3,102. At round 750, the number of received packets is 4,499; at round 1,000, the received packets are 5,648; at round 1,250, the number of packets received is 6,528.

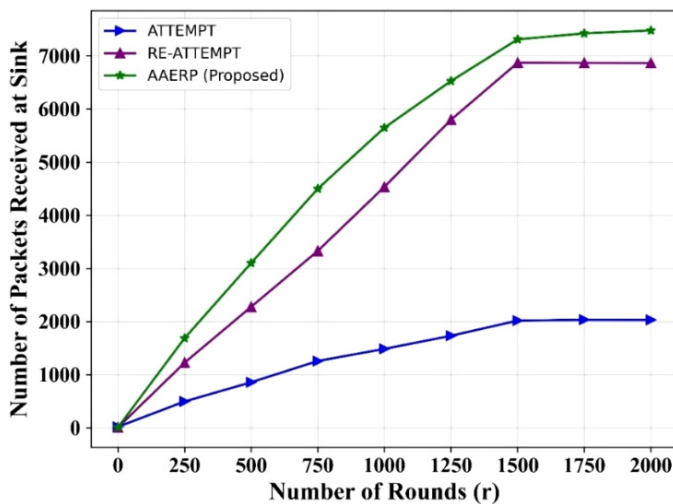


Fig. 12. Amount of packet received of proposed and existing framework.

Table 8. Comparison of total number of packets received.

Rounds	0	250	500	750	1,000	1,250	1,500	1,750	2,000
ATTEMPT	7	495	858	1,258	1,486	1,733	2,018	2,035	2,032
RE-ATTEMPT	5	1,225	2,277	3,330	4,535	5,798	6,870	6,867	6,865
AAERP	0	1,685	3,102	4,499	5,648	6,528	7,311	7,424	7,479


At round 1,500, the received packets are 7,311; at round 2,000, the number of packets received is 7,479.

6. Conclusion

This study introduces AAERP to provide an optimal routing path between IoMT devices and medical centers with improved security. In the beginning, the patient's sensitive data are aggregated from the WBAN with the assistance of IoMT devices from the hospitals. To secure the patient's data from attackers, a data encryption process is performed. The proposed work combines the ECC approach and Paillier cryptosystem for data encryption. These two methods encrypt the data by generating appropriate keys, which helps to enhance the secureness of data. The data encryption process converts the original data into ciphertext before routing. The optimal path for routing helps to improve the network performance. Thus, the proposed work utilizes the TOA approach for optimal path selection. Each route is evaluated iteratively to improve the effectiveness and robustness of the system. This optimization provides a reduced cost, enhanced energy efficiency, and improved network lifetime. The simulation results show that the proposed framework attains enhanced performance over several existing models.

ORCID

Padma Vijetha Dev Bakkaiahgari  <https://orcid.org/0000-0002-6210-4994>

K. Venkata Prasad  <https://orcid.org/0000-0002-5305-4155>

References

1. O. AlShorman, B. AlShorman, M. Alkassaweneh and F. Alkahtani, A review of internet of medical things (IoMT)-based remote health monitoring through wearable sensors: A case study for diabetic patients, *Indonesian J. Electr. Eng. Comput. Sci.* **20** (2020) 414–422.
2. S. Misra, P. K. Bishoyi and S. Sarkar, I-MAC: In-body sensor MAC in wireless body area networks for healthcare IoT, *IEEE Syst. J.* **15** (2020) 4413–4420.
3. M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez and D. Lymberopoulos, A survey on security threats and countermeasures in internet of medical things (IoMT), *Trans. Emerg. Telecommun. Technol.* **33**(6) (2022) e4049.
4. E. A. Adeniyi, R. O. Ogundokun and J. B. Awotunde, IoMT-based wearable body sensors network healthcare monitoring system, *IoT in Healthcare and Ambient Assisted Living* (Springer, Singapore, 2021), pp. 103–121.
5. P. Kumar, G. P. Gupta and R. Tripathi, An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks, *Comput. Commun.* **166** (2021) 110–124.
6. J. Singh and N. A. A. Rahman, IoMT: A review of open APS system security for type 1 diabetes mellitus, *Int. J. Curr. Res. Rev.* **12** (2020) 93–100.
7. S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos and M. A. Jan, SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT), *Comput. Commun.* **160** (2020) 697–705.

8. Z. Shahbazi and Y. C. Byun, Towards a secure thermal-energy aware routing protocol in Wireless Body Area Network based on blockchain technology, *Sensors* **20** (2020) 3604.
9. A. K. Sagar, S. Singh and A. Kumar, Energy-aware WBAN for health monitoring using critical data routing (CDR), *Wireless Personal Commun.* **112** (2020) 1–30.
10. A. Ara, M. Al-Rodhaan, Y. Tian and A. Al-Dhelaan, A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems, *IEEE Access.* **5** (2017) 12601–12617.
11. M. A. M. El-Bendary, H. Kasban, A. Haggag and M. A. R. El-Tokhy, Investigating of nodes and personal authentications utilizing multi-modal biometrics for medical application of WBANs security, *Multimedia Tools Appl.* **79** (2020) 24507–24535.
12. F. H. Khan, R. Shams, H. H. Rizvi and F. Qazi, A secure crypto base authentication and communication suite in wireless body area network (WBAN) for IoT applications, *Wireless Personal Commun.* **103** (2018) 2877–2890.
13. B. Liu, H. Luo and C. W. Chen, A novel authentication scheme based on acceleration data in WBAN, in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies* (IEEE, 2017), pp. 120–126.
14. A. H. Sharmila and N. Jaisankar, E-MHMS: Enhanced MAC-based secure delay-aware healthcare monitoring system in WBAN, *Cluster Comput.* **23** (2020) 1725–1740.
15. N. Kaur and S. Singh, Optimized cost-effective and energy efficient routing protocol for wireless body area networks, *Ad Hoc Networks* **61** (2017) 65–84.
16. R. Vishwakarma and R. K. Mohapatra, A secure three-party authentication protocol for wireless body area networks, in *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)* (IEEE, 2017), pp. 99–103.
17. J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks, *J. Network Comput. Appl.* **106** (2018) 117–123.
18. R. K. Mahendran and P. Velusamy, A secure fuzzy extractor based biometric key authentication scheme for body sensor network in internet of medical things, *Comput. Commun.* **153** (2020) 545–552.
19. M. Azeem, A. Ullah, H. Ashraf, N. Jhanjhi, M. Humayun, S. Aljahdali and T. A. Tabbakh, FoG-oriented secure and lightweight data aggregation in IoMT, *IEEE Access* **9** (2021) 111072–111082.
20. M. D. Cano and A. Cañavate-Sanchez, Preserving data privacy in the internet of medical things using dual signature ECDSA, *Security Commun. Networks.* **2020** (2020) 1–9.
21. R. Arul, Y. D. Al-Otaibi, W. S. Alnumay, U. Tariq, U. Shoaib and M. D. J. Piran, Multi-modal secure healthcare data dissemination framework using blockchain in IoMT, *Personal Ubiquitous Comput.* **28** (2024) 3–15.
22. Z. Ullah, I. Ahmed, F. A. Khan, M. Asif, M. Nawaz, T. Ali, M. Khalid and F. Niaz, Energy-efficient harvested-aware clustering and cooperative routing protocol for WBAN (E-HARP), *IEEE Access.* **7** (2019) 100036–100050.
23. M. Geetha and R. Ganesan, CEPRAN-cooperative energy efficient and priority-based reliable routing protocol with network coding for WBAN, *Wireless Personal Commun.* **117** (2021) 3153–3171.
24. F. Ullah, M. Z. Khan, M. Faisal, H. Ur Rehman, S. Abbas and F. S. Mubarek, An energy efficient and reliable routing scheme to enhance the stability period in wireless body area networks, *Comput. Commun.* **165** (2021) 20–32.

25. Y. Qu, G. Zheng, H. Wu, B. Ji and H. Ma, An energy-efficient routing protocol for reliable data transmission in wireless body area networks, *Sensors* **19** (2019) 4238.
26. A. Ahmad, N. Javaid, U. Qasim, M. Ishfaq, Z. A. Khan and T. A. Alghamdi, RE-ATTEMPT: A new energy-efficient routing protocol for wireless body area sensor networks, *Int. J. Distrib. Sensor Networks*. **10** (2014) 464010.