An energy-efficient and secure framework for IoMT: An application of smart cities

MANGLA, C.; RANI, S.; HERENCSÁR, N.

Sustainable Energy Technologies and Assessments
Volume 53, Part A, October 2022, 102335, Pages 1-7

ISSN: 2213-1388

DOI: https://doi.org/10.1016/j.seta.2022.102335

Accepted manuscript

An Energy-Efficient and Secure Framework for IoMT: An Application of Smart Cities

Cherry Mangla[a], Shalli Rani[b] and Norbert Herencsar[c]

[a]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura-140401, Punjab., India
[b]Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura-140401, Punjab., India
[c]Department of Telecommunications, Faculty of Electrical Engineering and Communications, Brno University of Technology, Technicka 3082/12, Brno, 616 00, Czechia

ARTICLE INFO

Keywords:
Body-sensor nodes
CH selection
ESRO
IoMT
Remotely operated

ABSTRACT

The Internet of Medical Things (IoMT) has played an unrivaled role in rendering the ever-growing advancements in remote healthcare and sensor informatics. The body-sensor devices employed in remote healthcare applications are not only resource-constrained but are also vulnerable to various security attacks. Hence, to pact with the energy limitations and security vulnerability of these body-sensor devices, in this paper, we suggest ESRO: An **E**nergy-efficient and **S**ecured Communication framework using recently proposed meta-heuristic approach, i.e., **R**emora **O**ptimization **A**lgorithm (ROA). We employ a distributed cluster-based routing mechanism with the novel secured selection of Cluster Head (CH) using ROA. We ensure secured transmission using risky mode and γ risky mode. Extensive simulation of the ESRO demonstrates the supremacy of the proposed work over the existing techniques when evaluated on a benchmark of different performance metrics. ESRO not only preserves the energy but also ensures secured communication for IoMT.

1. Introduction

Smart healthcare is rapidly evolving as an interdisciplinary technology that combines physical components with computer devices to provide Artificial Intelligence (AI)-based solutions for healthcare applications [1]. Smart healthcare is an application of smart cities' [2]. The future lies in smart cities and smart cities dream healthcare is a priority to keep citizens safe [3]. Furthermore, the development of advanced lightweight communication protocols, smart devices, and smart sensors enabled the interconnection of medical things for examining biomedical signals as well as identifying diseases in the absence of human resources [4, 5, 6, 7, 8]. Such medical things, which assisted in transferring the information over a network without human intervention, are referred to as the Internet of Medical Things (IoMT) [9, 10, 11].

IoMT has increasingly played an important role in Remote Health Management (RHM). IoMT is mostly employed to capture remote data for patients via wearable sensors/devices and preserve it on cloud servers. Such data are made available to healthcare professionals for observation and use in real-time. The IoMT is divided into the following stages: fog layer, device layer (WBAN), and cloud service. The device layer dealing with sensing aims to develop reliable and precise sensing methods to collect multiple types of health-related data. RFID (NFC), Bluetooth, ZIGBEE, IrDA, WI-FI, and UWB are examples of communication technologies used for IoMT devices. The information is analyzed and stored in the fog layer. Furthermore, the cloud obtains patient data for analysis, processing, and storage. As a result, healthcare officials acquire access to data [12].

Since body sensor IoT-enabled devices are resource-constrained (i.e., embedded with limited batteries), hence, need to be processed through an energy-efficient communication mechanism for IoMT [13, 14]. It is evident from the retrospective survey of the existing literature [14, 15, 16], the distributed routing mechanism such as the cluster-based technique plays a pivotal role for applications of IoMT. Furthermore, the selection of Cluster Head (CH) has been predominantly targeted over the years [17]. The researchers have focused predominantly on the energy index and distance parameter for the eligible node for its selection on the role of CH. However, it is learned that CH selection is an NP-hard problem. Therefore, it is required to optimize the CH selection through the befitting meta-heuristic approach [18].

The authors explored the concepts of CH selection through optimization methods, for example, Genetic Algorithm, Tunicate Swarm Algorithm, Particle Swarm Optimization, and many more.

Therefore, choosing a particular optimization method for CH selection becomes critically significant. The authors in [19] proposed the Remora Optimization Algorithm (ROA) that is claimed to possess high convergence and better exploration capabilities as compared to the other existing optimization methods when tested on the benchmark of different functions. Therefore, getting motivated by this, we use ROA for CH selection.

Another crucial concern after the aforementioned prospects of IoMT communication is privacy preservation [20]. The phrase "privacy" is a subjective notion with a variety of meanings [21].

cherrymangla@gmail.com (Cherry Mangla); shalli.rani@chitkara.edu.in, shallir79@gmail.com. (Shalli Rani); herencsn@ieee.org (Norbert Herencsar)
ORCID(s): 0000-0002-2476-9063 (Cherry Mangla); 0000-0002-8474-9435 (Shalli Rani); 0000-0002-9504-2275 (Norbert Herencsar)

In this study, we look at an IoMT situation in which body sensor nodes continually capture and transfer information. Such devices can be used in a variety of critical applications, such as monitoring, medical, and transportation. These devices must be protected against a variety of security and privacy issues. It is critical to protect the security of these devices because if it is breached, an attacker can utilize and control them for nefarious reasons. Monitoring, healthcare, and transportation are examples of IoMT activities that create sensitive data that must be submitted regularly for a prompt response. Hence, to address the aforementioned concerns, we devise three objectives; the optimized CH selection by using novel parameters for preserving the energy of the body sensor nodes in IoMT; second, to use appropriate optimization method (i.e., ROA) for the selection of CH, lastly ensuring the security of the data transmission among these nodes.

The major contributions are listed as follows:

1. We suggest ESRO: An **E**nergy-efficient and **S**ecured Communication framework using recently proposed meta-heuristic approach i.e., **R**emora **O**ptimization Algorithm (ROA). In this work, we primarily focus on the novel energy-efficient and secured selection of CH through the ROA. It is, to the best of the authors' knowledge, the first work in the open literature that exploits ROA for the selection of CH.
2. We select CH using the essential novel parameters that are integrated to devise a fitness function. Furthermore, the CH selection is secured using the risky and γ risky mode.
3. The CHs gather data from the other body sensor nodes and, hence, forward the gathered data after aggregating to the data relaying node as shown in Figure 1.
4. The simulation of ESRO is performed and validated against the recently proposed routing techniques. The metrics used for evaluation are network reliability, network survival period, end-to-end delay, the status of alive and exhausted nodes of all rounds are covered.

The remainder of the paper is presented in the following structure. The proposed work presented in Section 2 explains the fitness function optimized by ROA. Security aspect in ESRO is investigated in Section 3. The simulations and outcomes are discussed in Section 4. Finally, we present the conclusion of the proposed work in Section 5.

2. Operational Structure of ESRO

Here, we discuss the functionalities of ESRO; particularly, we formulate the fitness function for the ROA technique that we have incorporated for our proposed work. While performing the implementation of the proposed work, some network assumptions, which we are supposed to follow. These assumptions are incommensurate with the real-time scenarios so that the proposed work can be mapped to various scenarios as far as network dimensions and sensor node parameters are concerned.

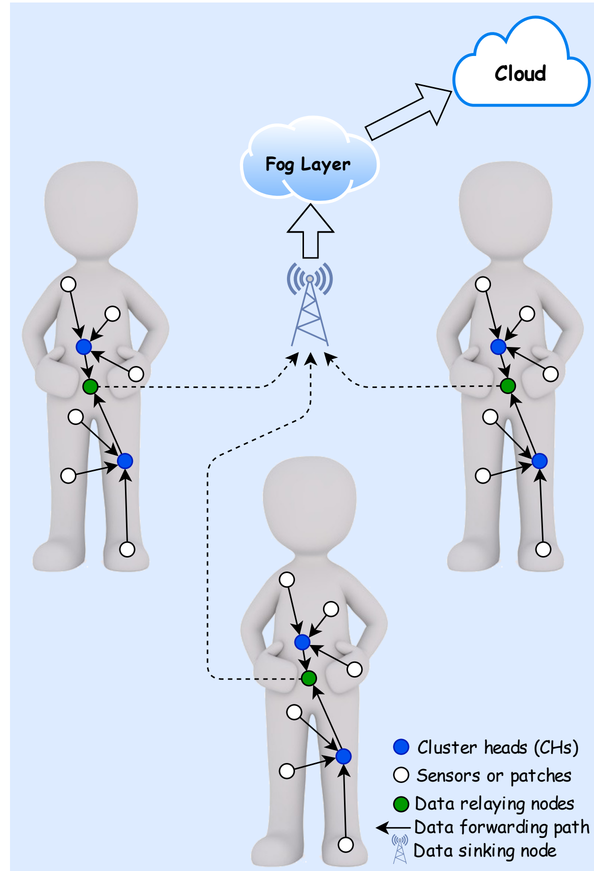

Figure 1: The figure is depicting the proposed scenario of the ESRO.

2.1. Network Assumptions

When MATLAB software is employed, there is command-type programming, which we employ for our proposed work. To perform an empirical investigation in the context of simulation parameters, we state the assumptions as follows:

1. The sensor nodes on the patient are fixed and remain fixed for the entire operation. Similar is the case with the sink, which has to collect data eventually.
2. The network is stationery in a way that the whole network, including the sink and also the sensor nodes, remains static for the entire operational period of the proposed work.
3. The nodes are homogeneous; i.e., the nodes have the same hardware characteristics in terms of energy, sensing coverage, computational energy consumption, etc.
4. The sink has no constraints of energy.

2.2. Selection of CH through the ROA

It is crucial to highlight the primary goal of our ROA-based CH selection is to minimize the energy expenditure incurred due to communication among the sensor nodes and the sink. Conventional methods are given in (1) and (2) as

Table 1
Symbol Definition

Symbols	Description
$E_{st}(b)$	Energy stock of b^{th} node
$E_{in}(p)$	Initial stock of energy a node
$D_S(b)$	Distance within b^{th} node and sink node
Ds_{avg}	Average value of distance of whole nodes from the sink
E_{agg}	Energy expenditure for aggregating data
E_{txn}	Energy expenditure for transmitting data
E_{rxn}	Energy expenditure for ratio of current stock of data
$\lambda, \rho, \gamma, \sigma$ and β	Equal values of weight factors for variables
D_{nodes}	Quantity of dead nodes
A_{nodes}	Quantity of alive nodes
$R_{Current}$	Current round value
D_{k-j}	Euclidean distance within the k^{th} and j^{th} nodes
Nr_S	Nearest sink
tx	Data transmission
S_{NK}	Data gathering sink
CH_{SL}	Selected node as CH

follows:

$$P_n = \frac{\Gamma}{1+\theta} \quad (1)$$

$$P_a = \frac{\Gamma}{(1+\theta\times\beta)(1+\theta)} \quad (2)$$

It is noted that the most significant node in the cluster is the CH. The reason behind this is the essential responsibilities that the CH has to handle. Hence, the selection of the CH node is done through various decisive fitness parameters. These parameters act as gradients to the formulation of the fitness function. To give clarity about the design of the fitness function, we individually define the fitness parameters. For the convenience of the readers, we have used symbols and definitions to understand equations. We have referred to Table 1. The fitness attributes/parameters used in the design of the fitness function for the ROA algorithm are given as follows:

1. ***Fitness evaluating parameters:*** The explanation for each fitness evaluating parameter is given as follows.
   1) Energy ratio of remaining and initial energy of nodes: When it comes to CH, the energy usage is higher in comparison to non-CH nodes that are involved in the data transmission phase to the CH. Hence, it becomes crucial to opt for that node as a CH, which is equipped with a large stock of energy. Furthermore, the initial stock of energy is also considered for a node. Hence, the ratio of parameters mentioned above helps in selecting that particular node as CH, which has the maximum value of this ratio. While doing so, the network is made to operate for a longer possible duration. The (3) demonstrates the significance of energy by representing the ratio of current stock to that of the initial stock of energy of a node.

$$F_1 = \sum_{p=1}^{T_N} \frac{E_{rsd}(p)}{E_{in}(p)} \quad (3)$$

$$E_{rsd}(p) = E_{in}(p) - E_{txn} - E_{rxn} - E_{agg} \quad (4)$$

   Moreover, in (4), we represent how we compute the remaining stock of energy of the particular node. It is learned more the value of this fitness evaluating factor, the more will be the chances of energy preservation by the selected node, which is to act as a CH.
   2) Separation among the sensor nodes and the sink: While data communication is in the wireless medium, it is believed that farther the nodes are located to the sink node, more energy will be devoured of sensor nodes. Therefore, it is indispensable to include this parameter for optimum selection of a node as a CH. It is important to note that the ratio of the distance factors is considered here, which includes the farthest separation of a node from the sink and node, which is closely located. Further to this ratio, the average value of the distance of all participating nodes is considered, which is added to the distance ratio computed above. Normally, the separation between the nodes and the sink varies from 1 to 70 meters. The higher value of this parameter favors the selection of that node as CH, which will be preserving the energy at the maximum level as shown in (5).

$$F_2 = \sum_{p=1}^{T_N} \frac{D_{clos}}{D_{farth}} + \frac{1}{D_{avgsin}(p)} \quad (5)$$

$$D_{avgsin}(p) = \frac{1}{T_N}\sum_{p=1}^{T_N} D_{NoSi}(p) \quad (6)$$

$$D_{NoSi} = \sqrt{(N_{x2}-N_{x1})^2 + (N_{y2}-N_{y1})^2} \quad (7)$$

   Moreover, in (6), we determine the average separation of all participating nodes from the sink, and in (7), the calculation of Euclidean distance is done between two participating nodes.

3) Network's residual energy: This element is taken into account while managing the network's left-over energy. The amount of dead nodes grows as a result of the nodes' consumption of energy during the operation of the network. As a result, the amount of CHs should be determined by this variable. As a result, we classify this component as CH when choosing a node. As shown in (8), the third fitness factor relates to the network's remaining energy.

$$F_3 = \frac{1}{T_N} \times \sum_{p=1}^{T_N} E_{rsd(p)} \tag{8}$$

4) Physical medium consideration: Various physical factors obstruct communication among the sensor nodes. It becomes imperative to understand the fact that a node with the least path loss contribution for the signal will be highly favored for CH selection. To address this concern, we consider the path loss factor calculation for a particular node, which is calculated by (9).

$$P_{TH}L(D_T) = P_L(T_{DST}) + 10 \times T_N \times \log\left(\frac{D_T}{T_{DST}}\right) \tag{9}$$

Further, in (10), the computation of $P_L(T_{DST})$ is done.

$$P_L(T_{DST}) = 10 \times log \times (Tim_{delay} \times 4\pi Fqq) \times c_L \tag{10}$$

We give the (11) to compute the fourth fitness evaluating parameter.

$$F_4 = \frac{1}{P_{TH}L(D_T)} \tag{11}$$

The sole aim to acquire the energy efficiency whilst performing the selection for CH, F_{4th} must be made the highest possible, as also stated by (11).

5) Energy of the whole Cluster: Once the data transmission in the network is initiated, the cluster nodes start consuming energy and once it happens, henceforth the cluster's energy diminishes gradually. Consequently, the urgency of stabilizing the load in the network is created. Due to this, selecting the node as a CH becomes predominantly affected by the status of energy of the whole cluster. During the network initialization, the value for this factor is assigned to be 1, however from the next round onward, there is an important role that cluster energy plays. Therefore, we determine the F_{5th} by using (12), which again must be made higher to acquire the optimal selection as a CH for a participating node.

$$F_5 = \sum_{p=1}^{N_{cls}} E_{rsd(p)} \tag{12}$$

2. ***Compilation of fitness function:*** In proposed work, we deal with the linear integration of multitudinous factors for selecting the CH. As shown in (13), the computation of the fitness function is given below.

$$F = \lambda 1 \times F_1 + \sigma 1 \times F_2 + \gamma 1 \times F_3 + \beta 1 \times F_4 + \rho 1 \times F_5 \tag{13}$$

$$\lambda + \delta + \gamma + \sigma + \beta = 1 \tag{14}$$

The (14) calculates the weighted sum of various factors, which are given weightage differently. The maximum value of fitness for a particular node decides for its selection as CH.

2.3. Data transmission to CH

Upon selecting the CHs, the formation of the various cluster takes place. The remaining nodes join the selected CH node to form a cluster, which ultimately helps in decreasing the energy consumption. TDMA and CDMA are processed for giving slots for data transmission from a cluster member to CH and then from CH to the sink, respectively.

3. Security Aspect in ESRO

The three modes; security, risky, and gamma risky are all considered important features of IoMT routing security [22, 23].

Security mode: In this mode, the CH that best meets the security standards are selected. The security rank and security demands connected with the CHs are denoted by SC_r known as security rank and SC_d known as security demand. The node is regarded to be the better CH if $SC_r <= SC_d$.

Risky mode: By selecting an existing CH, this option assumes all of the risks associated with enabling the best CH. As a result, during CH interpretation, the risky mode is regarded a persistent mode.

γ Risky mode: The sensor node, which is to be selected as CH is investigated for the fact, whether, it can uphold the γ-risk in assortment procedure, which in turn depends on γ-risky mode. Hence, γ is said to be the probability measure having values,$\gamma = 0$ and $\gamma = 1$ (i.e., 100%) that is comparable to the risky and secure modes.

Based on the risk mode, the CH that can hold the highest risk is favored in the selection process. As a result, analogous to the risky and security modes pertain to the probability measure having values $\gamma = 0$ and $\gamma = 1$ (i.e., 100 %).

The secure option is thought to be the most difficult and cost-effective of the three types. The γ-risky mode, on the other hand, is one of the most often used. The qualitative fuzzy measure has five levels of security [22, 23]:

Table 2
Simulation parameters for experiment

Parameters	Values
Industrial network area	100×100 meter^2
Sink location	$(50, 50)$
Total nodes	100
Initial stock of energy for a node	0.25 Joule

1. Extremely low (given as 1).
2. Weak (allotted as 2).
3. Moderate (allotted as 3).
4. Good (allotted as 4).
5. Strong (allotted as 5).

It is claimed to be a secure method if the right CH is elected whilst the selection phase. Equation specifies the probability of the security constraint model (15):

$$W_i^{SQ} = \begin{cases} 0 & \text{if } SC_d - SC_r \leq 0 \\ 1 - e^{\dfrac{(SC_d - SC_r)}{2}} & \text{if } 0 < o_d - o_r \leq 1 \\ 1 - e^{\dfrac{3(SC_d - SC_r)}{2}} & \text{if } 1 < SC_d - SC_r \leq 2 \\ 1 & \text{if } 2 < SC_d - SC_r \leq 5 \end{cases} \tag{15}$$

As given in (15), if selected CH acquires the condition $SC_r < SC_d$, the risks are found to be lesser than 50%. Further, if the state is $(0 < (SC_d - SC_r) <= 1)$, the selection procedure is commenced. If the condition $(1 < SC_d - SC_r) <= 2$, the CH selection is delayed. Even if the selection of CH is not taken place, the state of security is continued till $(2 < SC_d - SC_r) <= 5$.

Lemma 1 (:) The proposed work ESRO accounts to fixed iterations until $round_{max} = O(1)$ and bears computation complexity of $O(r_{max}) \times N)$.

The operational duration of the WSN, which is subjected to the real-life application, is decided by the extent of energy consumption by the sensor nodes whilst they are performing communication among the nodes or with the data collecting sink. It is noted that as the nodes considered for network performance evaluation are fixed in number, hence the network runs for fixed iterations. The energy consumption for every node is due to the wireless data transmission by the sensor nodes to the sink. Hence, it can be stated that the proposed work ESRO accounts for fixed iterations.

Determining the computation complexity helps in the real-time realization of the proposed work. From the Algorithm 1, it is quite evident that the computation complexity of ESRO is $O(r_{max}) \times N)$.

Algorithm 1 ESRO Algorithm

Input: Parameters for network initialization
Output: $Z = CH_{SL}$,

$CH_{SL} = 0$;
for $Round_{value} = 1$ to $Round_{max}$ **do**
    $A_n = N$
    $D_n = 0$
    for p= 1 to T_N **do**
        if $E_{rsd}(p) == 0$ **then**
            $D_{nodes} = D_{nodes} + 1$
            if $D_{nodes} == n$ **then**
                $A\_dead = R_{Curr}$
            end if
            $A_{nodes} = A_{nodes} - D_{nodes}$
        end if
    end for
    for i= 1 to T_N **do**
        if $E_{rsd}(p) > 0$ **then**
            Compute fitness function using ROA
            if F(p) is highest **then**
                Select p^{th} node as CH
                $CH_{SL} = CH_{SL} + 1$
                $CH_{SL} \leftarrow$ CDMA slot
                $CH\_S \longleftarrow p^{th}$ (data tx)
                $S_{NK} \longleftarrow CH_{SL}$ (data tx)
            else
                p^{th} node is non-CH node
                p^{th} node $\leftarrow$ TDMA slot
            end if
            Update $E_{rsd}(i)$ using [24]
        else
            break
        end if
    end for
    if $D_n == T_N$ **then**
        break
    end if
end for
return Z

4. Simulation Results and Discussions for ESRO

The simulation of ESRO is performed in MATLAB to acquire its empirical analysis based on various metrics for evaluating its performance metrics. We consider simulating the proposed work with respect to Table 2. To evaluate its performance in comparison to other protocols, ESRO, is compared with routing protocols; namely, Gu-WOA [25] MS-GAOC [17], ICITS [26] OE2-LB [27], and I-RAW [28].

4.1. Performance evaluating metrics

The performance evaluating metrics for checking the performance of ESRO is given below.

1. **Reliability Duration (RD):** It is a metric to examine the constancy of a given network. The elapsing of the

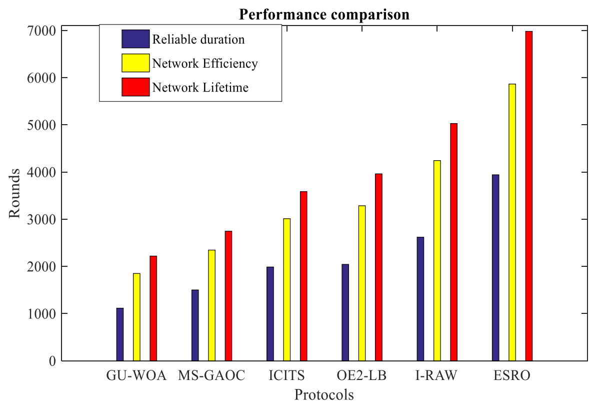

Figure 2: Evaluating the performance of ESRO

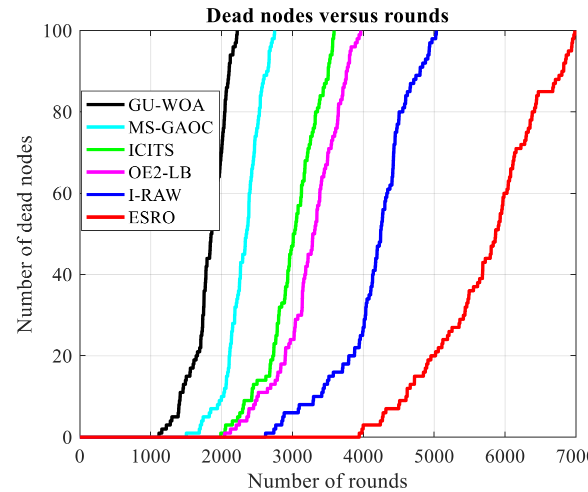

Figure 4: Evaluating the dead nodes status of all the considered algorithms and proposed work ESRO

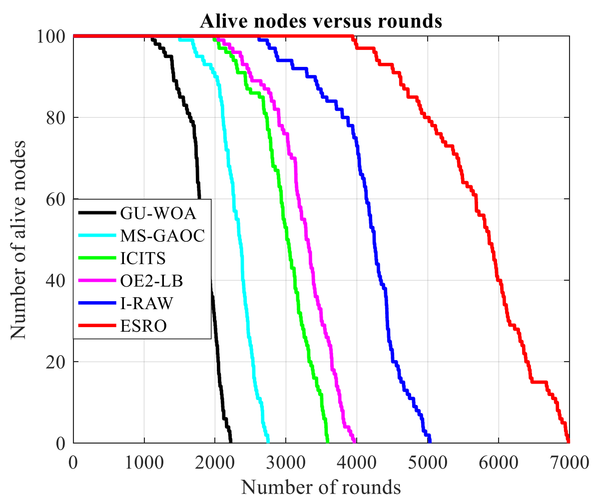

Figure 3: Evaluating the status of alive nodes of all the considered algorithms and proposed work ESRO

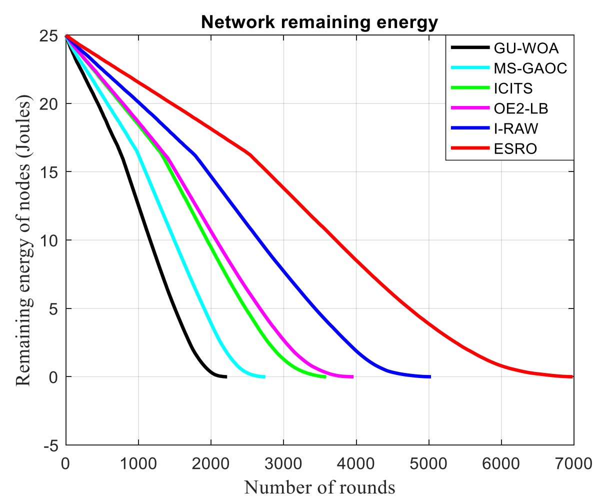

Figure 5: Network's remaining energy of all the considered algorithms and proposed work ESRO

amount of time until the first node is dead. In our work, this node can be of any type among the heterogeneous nodes. The proposed ESRO attains the RD of 3942 rounds; however, the other protocols, namely, acquire the lesser value of rounds. Figure 2 demonstrates the RD for ESRO. The paramount reason behind the improvement in RD is the hybrid approach of the optimization method, i.e., ROA, which supports the optimal selection of CH. The involvement of fitness parameters helps in selecting the node among the other nodes to make the energy preservation to the maximum possible level.

2. **Network Lifetime (NL):** It is the number of rounds that are acquired until every deployment is drained of its energy. This metric is of great significance when the application requires continuous monitoring of a particular area. Figure 3 and Figure 4 demonstrate the improvement acquired by ESRO in comparison to other nodes in terms of alive and dead nodes. The protocol ESRO acquires NL of 6982 rounds wheres I-RAW, OE2-LB, ICITS, MS-GAOC, and GU-WAO acquire 5029, 3962, 3586, 2747, and 2220 rounds, respectively. The consideration of the physical medium helps in preserving the sensor node's energy gigantically. Hence, the overall network lifetime increases to a great amount for the proposed work.

3. **Network's Energy Stock (NES):** NES or network's remaining energy is one essential metric to examine the proposed ESRO for its overall network progress in the context of energy consumption. Figure 5 shows the performance of ESRO, which has a similar stock of energy at the start, which is 25 Joules. However, as the network progress, the energy consumption of the protocols varies according to their adopted methodology. It is observed that the protocol ESRO performs exclusively well in comparison to other protocols. The cause behind such comprehensive improvement is the optimized CH selection.

Table 3
Performance examination for ESRO against other protocols

Performance examining metrics	Name of protocols					
	GU-WAO	MS-GAOC	ICITS	OE2-LB	I-RAW	ESRO
Reliability duration (rounds)	1116	1502	1988	2044	2620	3942
Network efficiency (HND) (rounds)	1851	2347	3012	3286	4244	5865
Network lifetime (rounds)	2220	2747	3586	3962	5029	6982
Number of packets sent	443842	567684	486712	506203	792941	1500809

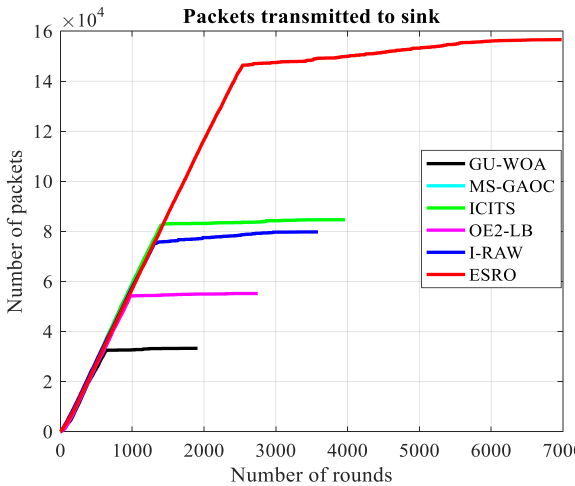

Figure 6: Evaluating the throughput of all the considered algorithms and proposed work ESRO

4. **Throughput Status:** The delivery of data packets is one of the essential elements in data collection from remote areas. Hence, this metric holds great significance as it gives information about the number of data packets that are attained at the sink or any data collection entity. Figure 6 shows the throughput of ESRO against I-RAW, OE2-LB, ICITS, MS-GAOC, and GU-WOA. The primary cause behind improving the throughput is the energy preservation of nodes that eventually makes all nodes transmit data for more longer duration.
5. **Secured CHs:** Figure 7 shows that the proposed protocol ESRO gives a more number of secured CHs as compared to I-RAW, OE2-LB, ICITS, MS-GAOC, and GU-WOA.
6. **Security status:** Figure 8 gives more security levels with respect to the rounds as compared to Gu-WOA. It is due to the secured CH selection, which authentically ensures data transmission using risky mode and γ risky mode.

The overall analysis for the proposed work is given in Table 3 and Table 4, wherein the former gives the information in rounds. In contrast, the latter renders the information about percentage improvement reported by the proposed protocol.

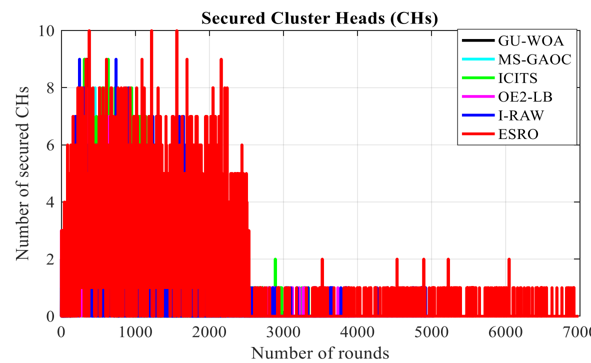

Figure 7: Number of secured CHs for all the considered algorithms and proposed work ESRO

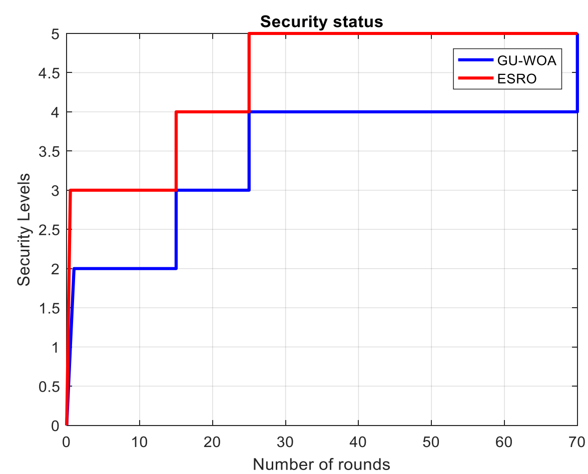

Figure 8: Evaluating the security of ESRO against GU-WAO for different rounds

5. Conclusion and Future Work

In this paper, we address the remote healthcare application by presenting an energy-efficient and secured communication framework that uses the ROA optimization method and is abbreviated as ESRO. The security of communicating sensor devices is ensured by using risky mode and γ risky mode, which helps in selecting the secured CH. The simulation proves the supreme performance of ESRO over the existing protocols.

Table 4
Performance examination for ESRO against other protocols (in %)

Performance examining metrics	Name of protocols				
	GU-WAO	MS-GAOC	ICITS	OE2-LB	I-RAW
Reliability duration (%)	253.2	162.4	98.2	92.8	50.4
Network efficiency (HND) (%)	216.8	149.8	94.7	78.48	38.1
Network lifetime (%)	214.5	154.1	94.7	76.2	38.8

Although the proposed work renders energy-saving communication, it still encompasses some shortcomings. Firstly, the ESRO scenario is dynamic, so we will employ sink mobility to ensure data reliability in the future.

References

[1] A. Gatouillat, Y. Badr, B. Massot, E. Sejdic, Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine, IEEE Internet of Things Journal 5 (2018) 3810–3822. doi: 10.1109/JIOT.2018.2849014.

[2] S. H. Ahmed, S. Rani, A hybrid approach, Smart Street use case and future aspects for Internet of Things in smart cities, Future Generation Computer Systems 79 (2018) 941–951. doi: 10.1016/j.future.2017.08.054.

[3] S. Rani, S. H. Chauhdary, A novel framework and enhanced QoS big data protocol for smart city applications, Sensors 18 (2018) 3980. doi: 10.3390/s18113980.

[4] Y. Qian, J. Shen, P. Vijayakumar, P. K. Sharma, Profile matching for IoMT: A verifiable private set intersection scheme, IEEE journal of biomedical and health informatics 25 (2021) 3794–3803. doi: 10.1109/JBHI.2021.3088289.

[5] A. Sekhar, S. Biswas, R. Hazra, A. K. Sunaniya, A. Mukherjee, L. Yang, Brain Tumor Classification Using Fine-Tuned GoogLeNet Features and Machine Learning Algorithms: IoMT Enabled CAD System, IEEE Journal of Biomedical and Health Informatics 26 (2022) 983–991. doi: 10.1109/JBHI.2021.3100758.

[6] Y. Gao, H. Lin, Y. Chen, Y. Liu, Blockchain and SGX-enabled edge-computing-empowered secure IoMT data analysis, IEEE Internet of Things Journal 8 (2021) 15785–15795. doi: 10.3390/s20102798.

[7] Z. Askari, J. Abouei, M. Jaseemuddin, A. Anpalagan, Energy-Efficient and Real-Time NOMA Scheduling in IoMT-Based Three-Tier WBANs, IEEE Internet of Things Journal 8 (2021) 13975–13990. doi: 10.1109/JIOT.2021.3069659.

[8] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, G. Srivastava, Security aspects of Internet of Things aided smart grids: A bibliometric survey, Internet of Things 14 (2021) 100111. doi: 10.1016/j.iot.2019.100111.

[9] M. A. Rahman, M. S. Hossain, An Internet-of-Medical-Things-Enabled Edge Computing Framework for Tackling COVID-19, IEEE Internet of Things Journal 8 (2021) 15847–15854. doi: 10.1109/JIOT.2021.3051080.

[10] M. Rajasekaran, A. Yassine, M. S. Hossain, M. F. Alhamid, M. Guizani, Autonomous monitoring in healthcare environment: Reward-based energy charging mechanism for IoMT wireless sensing nodes, Future Generation Computer Systems 98 (2019) 565–576. doi: 10.1016/j.future.2019.01.021.

[11] Y. Zhang, Z. Dong, L. Wu, S. Wang, A hybrid method for MRI brain image classification, Expert Systems with Applications 38 (2011) 10049–10053. doi: 10.1016/j.eswa.2011.02.012.

[12] S.-H. Wang, Y.-D. Zhang, Densenet-201-based deep neural network with composite learning factor and precomputation for multiple sclerosis classification, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 16 (2020) 1–19. doi: 10.1145/3341095.

[13] G. Manogaran, M. Alazab, H. Song, N. Kumar, CDP-UA: cognitive data processing method wearable sensor data uncertainty analysis in the internet of things assisted smart medical healthcare systems, IEEE Journal of Biomedical and Health Informatics 25 (2021) 3691–3699. doi: 10.1109/JBHI.2021.3051288.

[14] T. Han, L. Zhang, S. Pirbhulal, W. Wu, V. H. C. de Albuquerque, A novel cluster head selection technique for edge-computing based IoMT systems, Computer Networks 158 (2019) 114–122. doi: 10.1016/j.comnet.2019.04.021.

[15] S. Verma, N. Sood, A. K. Sharma, A novelistic approach for energy efficient routing using single and multiple data sinks in heterogeneous wireless sensor network, Peer-to-Peer Networking and Applications 12 (2019) 1110–1136. doi: 10.1007/s12083-019-00777-5.

[16] D. K. Anguraj, K. Thirugnanasambandam, R. RS, S. SV, Enriched cluster head selection using augmented bifold cuckoo search algorithm for edge-based internet of medical things, International Journal of Communication Systems 34 (2021) e4817. doi: 10.1002/dac.4817.

[17] S. Verma, N. Sood, A. K. Sharma, Genetic Algorithm-based Optimized Cluster Head selection for single and multiple data sinks in Heterogeneous Wireless Sensor Network, Applied Soft Computing 85 (2019) 105788. doi: 10.1016/j.asoc.2019.105788.

[18] Y.-D. Zhang, S. C. Satapathy, D. S. Guttery, J. M. Górriz, S.-H. Wang, Improved breast cancer classification through combining graph convolutional network and convolutional neural network, Information Processing & Management 58 (2021) 102439. doi: doi.org/10.1016/j.ipm.2020.102439.

[19] H. Jia, X. Peng, C. Lang, Remora optimization algorithm, Expert Systems with Applications 185 (2021) 115665. doi: 10.1016/j.eswa.2021.115665.

[20] W. Gan, J. Chun-Wei, H.-C. Chao, S.-L. Wang, P. S. Yu, Privacy Preserving Utility Mining: A Survey, in: Proc. of the 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 2617–2626. doi: 10.1109/BigData.2018.8622405.

[21] Y.-D. Zhang, Z. Dong, S.-H. Wang, X. Yu, X. Yao, Q. Zhou, H. Hu, M. Li, C. Jiménez-Mesa, J. Ramirez, et al., Advances in multimodal data fusion in neuroimaging: overview, challenges, and novel orientation, Information Fusion 64 (2020) 149–187. doi: 10.1016/j.inffus.2020.07.006.

[22] S. Song, K. Hwang, Y.-K. Kwok, Risk-resilient heuristics and genetic algorithms for security-assured grid job scheduling, IEEE Transactions on Computers 55 (2006) 703–719. doi: 10.1109/TC.2006.89.

[23] S. Song, Y.-K. Kwok, K. Hwang, Security-driven heuristics and a fast genetic algorithm for trusted grid job scheduling, in: 19th IEEE International Parallel and Distributed Processing Symposium, IEEE, 2005, pp. 1–10. doi: 10.1109/IPDPS.2005.397.

[24] T. S. Rappaport, Wireless communications: Principles and practice, volume 2, prentice hall PTR New Jersey, 1996.

[25] D. L. Reddy, C. G. Puttamadappa, H. N. G. Suresh, Hybrid optimization algorithm for security aware cluster head selection process to aid hierarchical routing in wireless sensor network, IET Communications 15 (2021) 1561–1575. doi: 10.1049/cmu2.12169.

[26] S. Verma, S. Zeadally, S. Kaur, A. K. Sharma, Intelligent and Secure Clustering in Wireless Sensor Network (WSN)-Based Intelligent Transportation Systems, IEEE Transactions on Intelligent Transportation Systems (2021) 1–9. doi: 10.1109/TITS.2021.3124730.

[27] A. S. Raj, M. Chinnadurai, Energy efficient routing algorithm in wireless body area networks for smart wearable patches, Computer Communications 153 (2020) 85–94. doi: 10.1016/j.comcom.2020.01.069.

[28] S. Sharma, V. Mishra, M. Tripathi, Intelligent-Routing Algorithm for wireless body area networks (I-RAW), International Journal of Communication Systems 34 (2021) e4984. doi: 10.1002/dac.4984.