TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 22, No. 2, April 2024, pp. 340~350
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v22i2.24759

Enhancing the performance of network in wireless body area network based on novel encryption algorithm

Othman Atta Ismael[1], Ahmed Talal Kamil[2], Layth A. Jasim[2], Poh Soon JosephNg[3,4]
[1]Department of Networks Engineering, College of Engineering, AL Iraqia University, Baghdad, Iraq
[2]Department of Computer Engineering, College of Engineering, AL Iraqia University, Baghdad, Iraq
[3]Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia
[4]Department of Communication Technology Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq

Article Info

Article history:

Received Oct 30, 2022
Revised Nov 18, 2023
Accepted Dec 9, 2023

Keywords:

Ant colony optimization
Computer science
Multi-fractional triphase duplex data encryption
Privacy
Wireless body area network

ABSTRACT

The efficiency of tools used to collect private medical data on people has significantly improved over time. These include implanted, surface-mounted, or encircling devices that form a wireless body area network (WBAN). Although the most recent secure authentication techniques in the industry offer privacy and security, these schemes have a higher time cost for authentication and take longer to complete owing to the restricted computational power of WBAN devices. We provide a novel authentication method depending on the lightweight wearable device scheme for the WBAN environment. Wearable devices are used to capture sensor data from the patient's body in the beginning, after which any redundant data is removed by normalization. The method we suggest for encrypting the data is multi-fractional triphase duplex data encryption (MTDDE) with ant colony optimization (ACO). The method considers not only the security of the data but also the many limitations of sensor nodes, such as battery life, throughput, computing power limitations, and dynamic topology. The thorough research demonstrates that our suggested technique saves computing costs while maintaining security and privacy together with anonymous verification. The suggested system's effectiveness in protecting the privacy and confidentiality of patient health data in WBAN is demonstrated by the simulation model.

Corresponding Author:

Layth A. Jasim
Department of Computer Engineering, College of Engineering, AL Iraqia University
Baghdad, Iraq
Email: layth.jasim@aliraqia.edu.iq

1. INTRODUCTION

A wireless body area network (WBAN) is a collective of sensors that can be worn or put into the body and a controller. The sensors are used to keep records of a patient's heart rate, breath rate, electrocardiogram, blood pressure, and other health information, as well as environmental factors like light, humidity, and heat. The nodes transmit the gathered information to the controller, which acts as a gateway and transmits the gathered health data to the caregiver through medical healthcare servers [1]. One of the most exciting topics that wireless sensor networks (WSNs) are used for is WBAN. In WBAN, patients' vital signs like saturation of oxygen (SpO_2), electrocardiogram (ECG), electromyogram (EMG), electroencephalogram (EEG), blood pressure, respiratory rate, body temperature, and pulse rate are controlled using different biosensor nodes located inside and outside the body in a way that doesn't get in the way of their normal activities. Different biosensor nodes with limited resources can be used in healthcare applications. These nodes can be connected to gateways/BS and MS using wireless technologies like 4G, 5G, long term evolution (LTE), universal mobile telecommunication system (UMTS), Wi-Fi, worldwide interoperability for microwave access (WiMax), and satellite communication. Also, after mutual authentication, medical experts can get real-time medical information about a patient from the MS in a safe way, and by using a firewall, we can stop attacks from our enemies and keep an eye on internal and external data traffic in a reliable way [2]. Controlling these physiological values of older people or people with chronic diseases gives patients more freedom and flexibility and makes it possible to act quickly when needed. As a result, both the total cost of health care systems and the number of overworked doctors and nurses are expected to rise by a lot. This makes it more likely that the latest WBAN innovations will be used to improve the lives of patients, enhance monitoring procedures, make decisions about interventions promptly, and lower the overall cost of health systems and the long working hours of medical staff [3]. This information about the human body that is in the wireless communication medium can be changed by the attackers. Small changes in medical data can have a big effect on the health of people. So, security is one of the most important parts of wireless body sensor networks. The devices in WBSN have few restrictions, so they can be attacked. To secure the data, a cryptographic method must be used. Eavesdroppers can change the contents of encrypted messages once the medical data record is in the network. Classical cryptosystems use mathematical functions and various numerical methods to encrypt the information [4]. Doctors need real-time data about their patients, so then they can make quick decisions in different forms of critical situations. For telemedicine, we need an advanced network that lets users communicate with patients in real-time and send high-quality video without slowing down the network. Website and app developers are used to keep an eye on a patient's health in a remote area [5]. The contribution of this technique is to give an immediate response if something goes wrong with a patient. The contribution of our suggested technique is to reduce the computation cost while managing the security and privacy information of patients' health. The further part of the section includes the following, section 2 includes literature survey, section 3 indicates suggested method, section 4 shows a result and discussion, and section 5 indicates the conclusion part.

2. RELATED WORKS

Bharathi and Venkateswari [6] shows how quantum cryptography can be used to create a high-level security system for WBANs. A quick look at how it compares to the improved BB84 quantum key distribution (QKD) method in terms of performance and time complexity. The suggested EB92 method turned out to be 29% efficient and 2 times as complicated as the existing EBB84 method, which was 42% efficient and 2.86 times as complicated. In addition, the security analysis is processed for the time-shift quantum attack. Zhong *et al*. [7] described the most recent WBAN medical applications, as well as their requirements, problems, and solutions. They looked into every aspect of WBANs, from the sensing devices used to collect data to the wireless transmission technology used to send it, like frequency bands, channel models, medium access control (MAC), and networking protocols. Then they discussed its specific energy and safety use problems. In particular, an application-specific integrated circuit (ASIC)-based WBAN scheme is proposed to develop its privacy and safety to get an ultra-low energy consumption.

Research by Rameshkumar and Ganeshkumar [8] addressed a collection of WBAN methods and other things that could be done to learn more in this field. The research study denotes that present network are also upgraded to give WBAN processes more reliable solutions. The basic idea behind WBAN technology is to put them around sensor nodes that are inside or around the patient's body in the medical system. It gives patients more comfort and lets them watch the healthcare staff from a distance. Ojelade *et al*. [9] introduced a new architecture with a sink node made to reduce power consumption and develop the quality of service (QoS) of WBAN. Also, to make the network last longer and improve QoS, we used the MAC protocol to divide the physiological data into normal and critical data. A routing protocol called the efficient energy and QoS (EEQ) algorithm is used to send data along the shortest and best route.

Kamruzzaman and Alruwaili [10] describes an energy efficient sustainable network using network optimization method (EES-NOT) as suggested in this study to make the WBAN as energy-efficient as possible. The adaptive scheduling procedure for energy efficiency (ASPEE) is integrated with EES-NOT to improve the network's reliability and QoS. A secured routing protocol for energy efficiency (SRPEE) also makes networks less crowded and chooses the best route. WBAN technology has to deal with a lot of problems. The sensors' batteries don't charge quickly, the network topology can modify, there are strict QoS requirements, and the rate at which files are created and stored can change. WBANs depends on how much energy they use, which is why they are one of the most common issues in the system. With this capacity, solving these issues is crucial for the WBAN to function effectively.

Research by Hussain *et al*. [11] examined the most recent findings on encryption, as well as the communication architecture, security needs, and key problems with WBANs. The most recent encryption security methods utilized in WBAN contexts are also covered in this survey. The research will assist the academic community in understanding security issues and their causes by locating and contrasting all encryption algorithms that are currently used in the WBANs industry. This survey aims to assess and contrast the current encryption security solutions and examine the WBANs solution.

Research by Shanmugavadivel *et al*. [12] proposes better data security through advanced encryption standard (AES) and more efficient task flow scheduling through genetic algorithm (GA). Tasks are efficiently scheduled by the suggested approach, which significantly lowers interference and boosts system throughput. The suggested model's throughput, execution, response, and encryption times have all been examined. To verify the suggested model's superior performance, findings from standard models like DES and 3DES are compared, and the proposed model outperforms them. Bhardwaj *et al*. [13] examined and looked into the role, need, and use of the cloud in empowering WBAN. Also, they discussed different parts of this integrated ecosystem, such as definitions, technologies, QoS parameters, and existing solutions.

Ali and Liu [14] attains to get around these problems, and the idea of WBANs that use the cloud has been put forward. In these kinds of networks, the cloud server has a lot of computing and storage power to process and store the data. But sending data to a third-party provider raises concerns about data security, data integrity, and fine-grained control over access and searches. To deal with these worries, we came up with a plan called lightweight verifiable data management (LVDM). Saleem *et al*. [15] describes a metaheuristic method for choosing the best clusters in WBANs to make a routing protocol for monitoring livestock health and behavior that uses less energy. The proposed method uses ant lion optimizer (ALO) to choose the best clusters for different pasturage sizes, taking into account the user's preferences about cluster density. Recent methods like ant colony optimization (ACO), grasshopper optimization, and moth flame optimization are compared to the ALO method.

Concerns about security and privacy are the main things holding back the widespread use of WBAN. Sensor nodes transmit very important and sensitive information. Such a console would be a breach of the patient's privacy and might even endanger their lives. For example, if a doctor gets a false reading from an ECG sensor, it could lead to wrong interventions that could be harmful to the patient. A threat on WBAN can hide legitimate data, which could cause the wrong drug to be given by the actuator or the doctor to not be told about a life-threatening situation. Also, personal health data should not be available to people who aren't supposed to see it. Traditional cryptographic techniques can't be used in IoT-based WBAN, because the surrounding is very limited in terms of computing power, storage, and battery power. By analyzing the above limitations of WBAN, we propose multi-fractional triphase duplex data encryption (MTDDE) with ACO to reduce the computation cost while managing the patient's health data.

3. PROPOSED WORK

A process of encryption and decryption that uses an asymmetric key is slower and would need more energy and memory. This makes it unclear for WBAN, which has limited resources. When the patient's information is first gathered from the WBAN sensor nodes, it is stored in a personal data assistant (PDA). Before this, doctors and patients will sign up using a hash key algorithm. The patient's basic data profile can only be seen by doctors who have a patient identification number, or ID. The patients can see more than one doctor if they share their cloud data with them. Most of the time, patient data has information about different diseases. We proposed a moving target defense (MTD) with ACO technique to protect patients' health data and reduce the computation cost. Figure 1 represents an overview of our proposed method.

3.1. Data sample

This part is employed to gather both personal data and important symptoms of the disease. There are 493 COVID-infected people and 206 people who are not infected but have symptoms. A threshold routing algorithm model is created using the information provided by these individuals. Each new user then enters their personal information and symptoms, and to protect the privacy of COVID patient data [16].

3.2. Data normalization

Normalizing a dataset can be done in different ways, such as with min-max normalization, z-score normalization, decimal scaling, and standardized moment. Both min-max and z-score normalization are common and widely used [17]. The min-max method was used for our work. In min-max normalization, features in the range [0, 1] are normalized by using (1).

$$u' = \frac{u - min_B}{max_B - min_B} \tag{1}$$

The minimum and maximum values of feature B are shown here by min_B and max_B, respectively. The values u and u' indicate the attribute's original and normalized values, respectively [18]. The maximum and minimum feature values are transferred to 1 and 0, respectively, as can be seen from the (1).

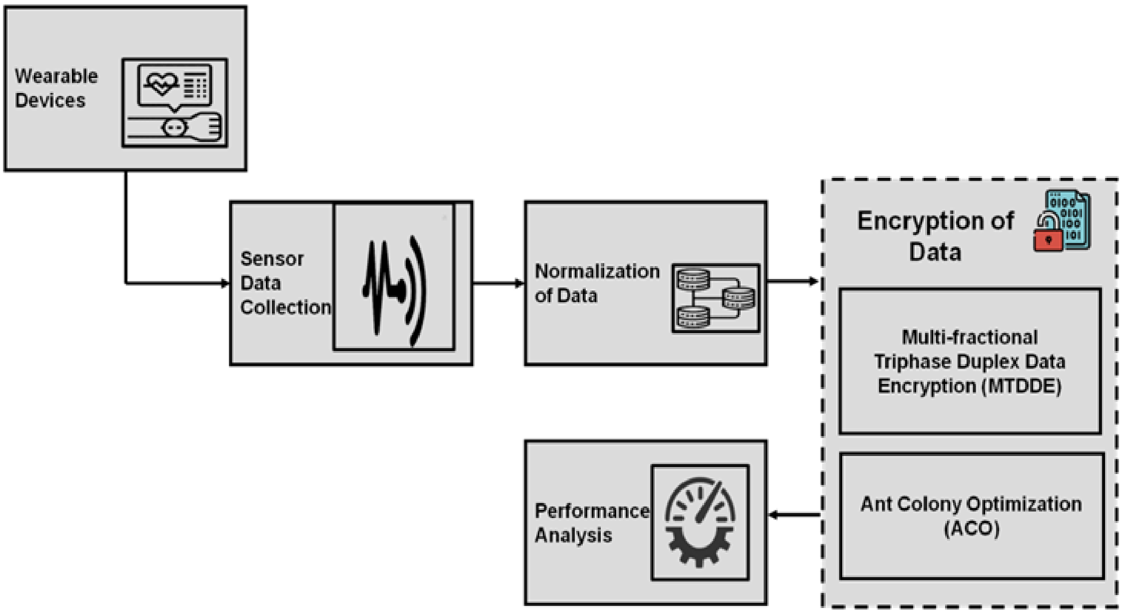

Figure 1. Representation of our proposed method

3.3. Encryption of data using multi-fractional triphase duplex data encryption
3.3.1. Multifractional encryption

For stationary time series, the standard partition function multifractal formalism was created. So, it doesn't offer exact results for time series that aren't stationary. More recently, a technique was made for the multifractal characterization of non-stationary time series. It is based on a generalization of the detrended fluctuation analysis (DFA) and is called the multifractal detrended fluctuation analysis (MFDFA). It has also been decided that the MFDFA must be suggested for the global detection of multifractal behavior. Also, the MFDFA doesn't take more work to put into place than the regular DFA. Just one extra step is needed. Because of these things, we chose the second method to find the multifractality of the information we want to study. We assume that a chaotic carrier with an embedded signal has a more complex structure than a chaotic carrier by itself, so the multifractality degree should be higher in the former case. So, this quantifier must be able to find a message and can be used to evaluate how well encryption schemes work. It was discovered that uncorrelated noise doesn't change the shape or location of the estimated multifractal spectrum using the MFDFA. But when there is correlated or ant correlated noise, this multifractal spectrum is narrower and centered on the noise's Hurst exponent value. Uncorrelated noise must be a natural part of real-world data. So, the MFDFA can be relied on for the multifractal quantification of noisy real data [19].

3.3.2. Duplex construction

For each block being processed, a duplex construction is a sponge function that enables you to retrieve specific bits from the intermediary chaining variables. According to rumors, the duplex's security level is equal to that of the sponge. The duplex construction is made up of two parts: the initialization phase and the duplexing phase. In the initial phase, the initial value (IV) has a size equal to the bitrate r on the outside and a size equal to the capacity c on the inside. Figure 2 denotes the duplex construction.

In the second phase, every M_i is padded using the function Pad and known one time. As a result, each padded block is guaranteed to be non-zero. The duplex construction, in contrast to the sponge function, accepts an input string for each call and returns an output string Z_i of length u_i that is based on all previous inputs. The duplex architecture can be transformed into a cryptographic keyed hash algorithm like the sponge function [20].

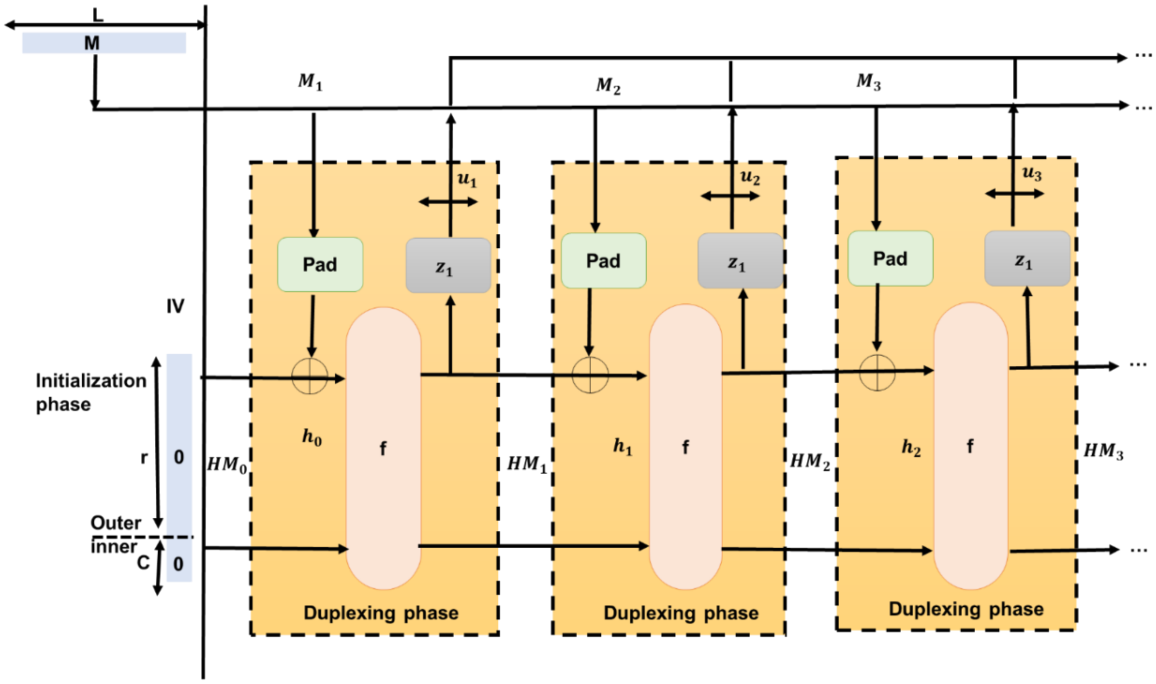

Figure 2. Duplex construction

3.3.3. Triphase encryption

The structure is highly emissive, which makes it possible to find all four of the organics in water at the nano molar level quickly and in a way that can be reused. Besides vapor and solid-state luminescence recognition. Liquid-phase fluorescence sensing proves that the framework is a flexible three-phase sensory scaffold for a wide range of dangerous organoaromatics [21]-[25].

3.4. Ant colony optimization

At regular intervals, each ant searches for the destination node using the pheromone update to find the shortest route. The WBAN nodes that are closest to the doctor's location are used to convey emergency notifications via the pheromone update. Using the shortest link from the sensor nodes, the gateway transmits the information to the doctor, who then receives the emergency signals. The ants remember the paths they take and the things that get in their way. When moving from one node to another, there will be a list of the nodes that have been visited and the amount of time it took to get there. In this way, decisions are made using a stochastic policy. The pheromone values are figured out by the ants' constant learning, which is based on both the current and past status of WBAN nodes. A part provides a concise description of the ACO method. Ants naturally choose the shortest way to get to their food, which led to the idea of ant colony optimization. In (2) gives the shortest route that ants are most likely to take to find food.

$$shortest\ path = \frac{\frac{n-ants^{pheromone}}{x-distance}}{\frac{Shortest\ distance}{-time}} \quad (2)$$

$$i_{dx} = \sqrt{(j_d - j_x)^2} + (e_d - e_x)^2 \quad (3)$$

The pheromone left behind on edge (i, j) at time t is given by $c(s)$. Each cycle updates the pheromone intensity by $\frac{O}{A}P$. This factor makes it possible to take the shortest path. the total of freshly deposited pheromones is given by $\Delta\tau_{dx}$. The pheromone is updated using (4).

$$\tau_{dx}(s + d) = k * \tau_{dx}(s) + \Delta\tau_{dx}(s) \quad (4)$$

p denotes the rate of pheromone decay per unit time and $\Delta\tau_{dx} = \sum\sum_{p=a}^{g} \Delta\tau_{dx}$.

The contributing components to the transition probabilistic approach are $i)\ \eta_{dx}\ and\ ii)\ \tau_{dx}$ which are provided by (4) and (5).

$$\eta_{dx} = \frac{1}{\eta = i_{dx}} \tag{5}$$

When the pheromone is changed, the subsequent iteration will begin by simultaneously modifying the ant path. Their weights are managed by α and β. The probabilistic transition function is given by (6).

$$K_{dx}^{p}(s) = \left\{\frac{[\tau_{dx}]^{\alpha}[\eta_{dx}]^{\alpha}}{\sum p} \in allowed\ p[\tau_{dx}]^{\alpha}[\eta_{dx}]^{\alpha}, if\ p \in allowed\ p\ ]\right\} \tag{6}$$

The ants will all learn if is close to 1, which causes a slight delay in the course. Delay is decreased if is close to 0, which indicates that l and are well balanced. There shouldn't be any loops to prevent latency because the route is found adaptively. If an ant visits a node that has already been reached, that data is erased from the ant's storage. If removed, the probabilistic transition equation stated was transformed into an ant colony system for balancing exploration and exploitation (7).

$$T = arg_{s\ ,otherwise\ i,e\ biased\ exploration}^{max\{[\tau(u,r)].[\tau(u,r)]^{\beta}\}, if\ o \leq o_q\ i.e\ exploitation} \tag{7}$$

Here, $r \in x_p(u), o_q =$ constant, $o -$ random variable and $T -$ result of probabilistic transition function. The procedure in (8) is used to upgrade the pheromone locally:

$$\tau(u,t) \leftarrow (1-\rho).\tau(u,t) + \rho\, \Delta\, \tau(u,t) \tag{8}$$

Ants' natural stigmergic behavior helps them find the shortest route and tell other ants about it. So, autocatalytic positive feedback algorithms are ACO methods. Each ant in the traveling salesman issue chooses a city depending on its proximity to the town and the amount of pheromone at each edge. It is essential to mention that the same town shouldn't be visited again. The ant will retrace its steps after reaching its destination. The probability of selecting a nearby ant is increased, altering the pheromone table. Data for the pheromone update is first gathered by WBAN nodes. Then, only makes other adjustments to ensure a decision at random. The WBAN node gains knowledge of the decision policy through pheromone updates. Therefore, to identify the shortest path, each node and the colony as a whole will understand the pheromone and act adaptively. In this research, WBAN is looked at from the perspective of ten nodes. In the suggested technique, the factor of fitness value is increased to reduce the time it takes to transmit emergency messages. When a patient requires critical care or has another medical problem, the WBAN will send an emergency message to the doctor's destination. Using ACO, the best and shortest way to send immediate messages to the doctor for quick treatment was found, and the lifetime of the network was reduced or increased based on a Bayesian game formulation.

4. RESULT AND DISCUSSION

The suggested experimental setup is used to simulate and evaluate the proposed MTDDE-ACO for WBAN. Comparisons are made between the proposed MTDDE-ACOs and the existing approaches, such as the identification key scheme (IKS), cooperative routing protocol (CRP), and energy efficient sustainable network using network optimization technique (EES-NOT). Based on parameters including throughput, computational cost, end-to-end latency, and packet loss, the performance of the network is assessed.

Table 1 compares the MTDDE-ACO to the IKS, CRP, and EES-NOT algorithms, which are currently utilized to address the issue of packet loss in WBAN, and reveals that the highest throughput average of the latter is 7045.705 kbps, depending on packet size. Figure 3 demonstrates that the MTDDE-ACO maximum throughput increases linearly about packet size. The throughput for the existing techniques, were IKS of 3349.2825, CRP of 2847.63, and ESS-NOT of 2002.6975. It indicates that the suggested system is more effective.

Table 1. Throughput of the MTDDE-ACO

Packet size (bytes)	IKS	CRP	EES-NOT	MTDDE-ACO [proposed]
10	2545.99	1659.74	1888.16	8343.01
20	4360.26	3213.71	2014.98	6027.16
30	3039.87	3730.84	1333.69	5370.55
40	3451.01	2786.23	2773.96	8442.1
Avg. of throughput	3349.2825	2847.63	2002.6975	7045.705

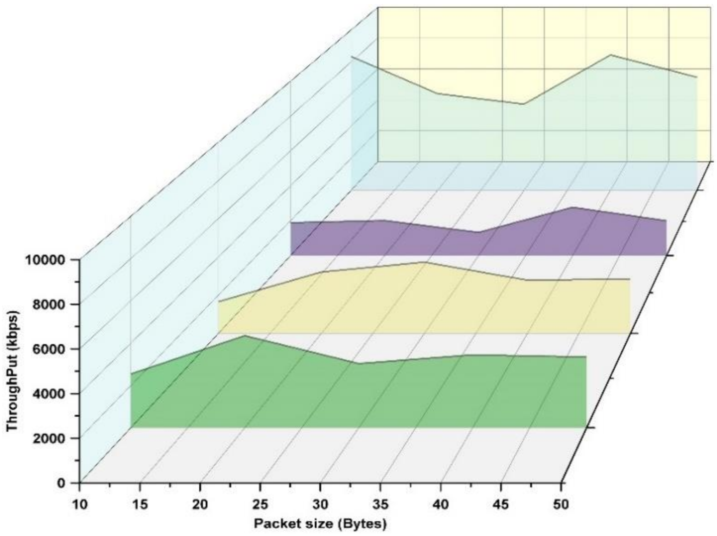

Figure 3. Maximum achievable throughput of MTDDE-ACO

The performance of MTDDE-ACO for end-to-end average packet delay at the various sites of data reception is shown in Table 2. In comparison to the IKS, CRP, and EES-NOT algorithms presently being utilized to address the issue of packet loss in WBAN, the least average end-to-end speed is 25.325 kbps for the MTDDE-ACO method. Figure 4 displays the end-to-end average packet delay performance for MTDDE-ACO at various data reception sites. The end-to-end delays for the presently used approaches were as follows: IKS 33.375, CRP 40.975, and ESS-NOT 42.675. It demonstrates the low suggested system performance.

Table 2. End-to-end delay performance of MTDDE-ACO

Packet size (bytes)	IKS	CRP	EES-NOT	MTDDE-ACO [proposed]
200	19.3	21.7	21.9	14.6
500	18.6	21.4	21.5	15.9
700	19.1	19.4	24.1	14.5
1000	76.5	101.4	103.2	56.3
Avg. of end-to-end delay	33.375	40.975	42.675	25.325

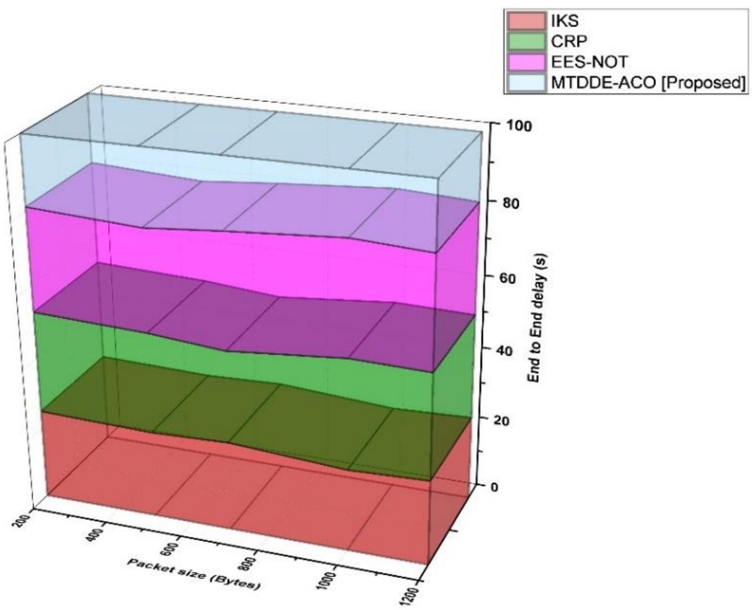

Figure 4. End-to-end delay performance for MTDDE-ACO

The performance results for MTDDE-ACOs of packet losses at various locations of data reception are shown in Table 3. When compared to the IKS, CRP, and EES-NOT algorithms that are presently being employed to address the issue of packet loss in WBAN, the MTDDE-ACO scheme has the lowest average packet loss of 3.25 kbps. Due to message transmission delays, the curve of several packet losses for MTDDE-ACOs grows at point one, however, they were smaller than the prior technique used to reduce the packet loss value. Figure 5 displays the upgraded scheme's lower packet loss value. IKS 6.5, CRP 8.25, and ESS-NOT 15 had the lowest Pocket loss among the currently used techniques. The low suggested system performance is shown.

Table 3. Packet loss performance for MTDDE-ACO

Packet size (bytes)	IKS	CRP	EES-NOT	MTDDE-ACO [Proposed]
1	6	6	17	3
2	5	10	12	4
3	7	8	16	3
4	8	9	15	3
Avg. of packet loss	6.5	8.25	15	3.25

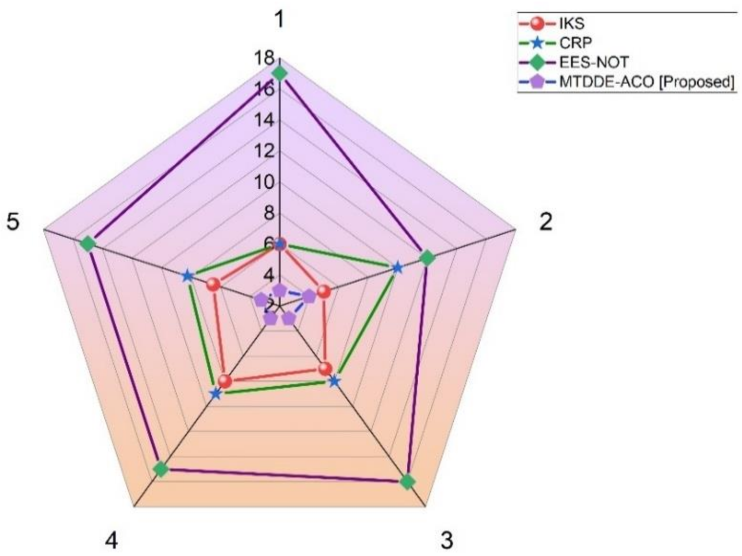

Figure 5. Number of packet loss in MTDDE-ACO scheme

Table 4 displays the MTDDE-ACO's computational cost performance at the different data receipt points. The MTDDE-ACO approach has a lower average computational cost of 30 than the IKS, CRP, and EES-NOT algorithms currently being used to handle the problem of packet loss in WBAN. The computational cost performance for MTDDE-ACO at different data-receiving points is shown in Figure 6. The currently used techniques have the following computing costs: IKS 58, CRP 61, and ESS-NOT 48. It indicates the low performance of the recommended system. IKS's capacity to provide effective network performance amongst devices for the WBAN application. The plan also offers a suitable transfer technique under optimal network performance circumstances. Only species that are included in the key may be identified using it, and since it is difficult, incorrect interpretations might result. In CRP, which is based on a multi-hop communication strategy, relays or sensors serving as forwarders are positioned along the communication path between the transmitter and the sink. Patients having wireless body sensors who were also congregated in a small area contributed to it. EES-NOT to improve the body area network's energy effectiveness and functionality. EES-NOT-based network performance assessment for renewable energy and smart grid systems. Each sensor node has a storage capacity problem as a consequence of the sensor's constant patient monitoring, which necessitates extra storage. MTDDE-ACO improves in preventing data breaches during transport and storage. Sensitive data may be sent across encrypted communication channels without running the risk of a security compromise. Compared to the other existing algorithms, this technique is superior.

Table 4. Computational cost performance of MTDDE-ACO

Packet size (bytes)	IKS	CRP	EES-NOT	MTDDE-ACO [proposed]
10	60	62	70	32
20	53	55	50	43
30	71	78	61	35
40	85	69	51	38
Avg. of computational cost	58	61	48	30

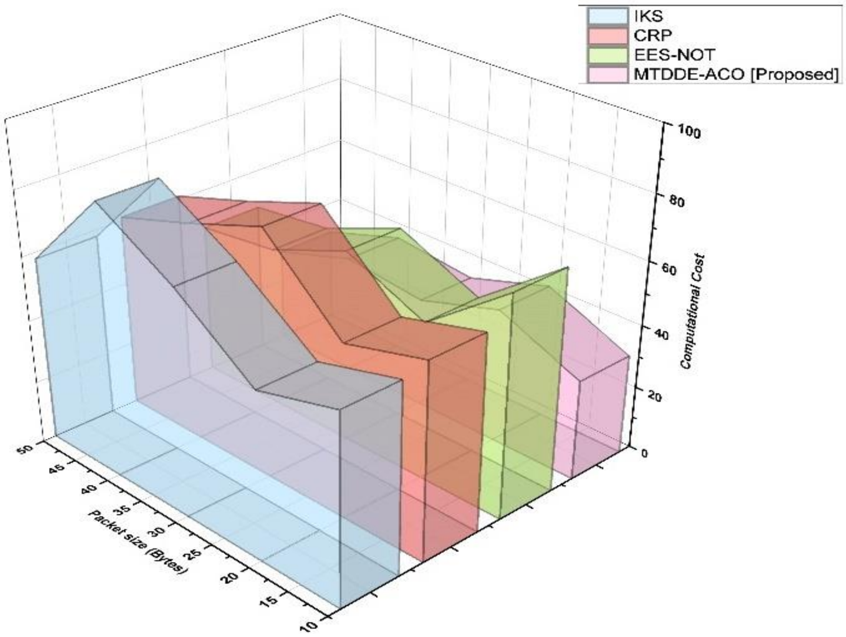

Figure 6. Computational cost performance for MTDDE-ACO

5. CONCLUSION

This paper's goal is to offer a WBAN that uses ACO and MTDDE. The simulation model shows how well the recommended approach protects the privacy and security of patient health data in WBAN. Wearable devices are utilized to first collect sensor data from the patient's body, and any redundant data is then normalized away. According to the findings, MTDDE-ACO was able to boost throughput while decreasing the amount of packet losses, computational cost, and end-to-end delay. This demonstrates MTDDE-ACO's capacity to provide effective network performance between devices for the WBAN application. Thus, by reducing the number of packet losses, this study addressed the need for efficient network performance and improved the efficient network performance of patient data transfer in the WBAN application. In the future, it is planned that the MTDDE-ACO will be able to link to an ambulance or another city and cover a broader medical environment area with other devices that support the MICS band.

ACKNOWLEDGEMENTS

The authors are grateful to the Iraqi Ministry of Higher Education and Scientific Research (MOHESR) for technically supporting the current research.

REFERENCES

[1] R. Nidhya, S. Shanthi, and M. Kumar, "A Novel Encryption Design for Wireless Body Area Network in Remote Healthcare System Using Enhanced RSA Algorithm," in *Intelligent System Design*, 2021, pp. 255–263, doi: 10.1007/978-981-15-5400-1_27.
[2] J. Iqbal *et al.*, "Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis," *Journal of Healthcare Engineering*, vol. 2022, pp. 1–19, Feb. 2022, doi: 10.1155/2022/9210761.
[3] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Computers & Security*, vol. 104, p. 102211, May 2021, doi: 10.1016/j.cose.2021.102211.
[4] A. D. V. and K. V., "Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications," *Personal and Ubiquitous Computing*, vol. 27, no. 3, pp. 875–885, Jun. 2023, doi: 10.1007/s00779-021-01546-z.

[5] M. Akhtar and T. Feng, "An Intelligent and Secured Privacy Preserving Framework For Wireless Body Area Networks (WBANs)," *EAI Endorsed Transactions on Creative Technologies*, vol. 9, no. 30, p. 173609, Mar. 2022, doi: 10.4108/eai.15-3-2022.173609.
[6] K. R. S. Bharathi and R. Venkateswari, "A novel security enhancement mechanism in wireless body area networks using quantum cryptography," in *7th International Conference on Computing in Engineering & Technology (ICCET 2022)*, Institution of Engineering and Technology, 2022, pp. 244–249, doi: 10.1049/icp.2022.0626.
[7] L. Zhong *et al.*, "Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey," *Sensors*, vol. 22, no. 9, p. 3539, May 2022, doi: 10.3390/s22093539.
[8] C. Rameshkumar and T. Ganeshkumar, "A Novel of Survey: In Healthcare System for Wireless Body-Area Network," in *Lecture Notes in Mechanical Engineering*, 2022, pp. 591–609, doi: 10.1007/978-981-19-0296-3_55.
[9] A. K. Ojelade, A. A. Ibrahim, and O. Ata, "Efficient Energy and QoS Based Routing Algorithm for Wireless Body Area Network," in *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, IEEE, Oct. 2021, pp. 110–115, doi: 10.1109/ISMSIT52890.2021.9604714.
[10] M. M. Kamruzzaman and O. Alruwaili, "Energy efficient sustainable Wireless Body Area Network design using network optimization with Smart Grid and Renewable Energy Systems," *Energy Reports*, vol. 8, pp. 3780–3788, Nov. 2022, doi: 10.1016/j.egyr.2022.03.006.
[11] S. Hussain, S. S. Ullah, M. Uddin, J. Iqbal, and C.-L. Chen, "A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks," *Sensors*, vol. 22, no. 3, p. 1072, Jan. 2022, doi: 10.3390/s22031072.
[12] G. Shanmugavadivel, B. Gomathy, and S. M. Ramesh, "An Enhanced Data Security and Task Flow Scheduling in Cloud-enabled Wireless Body Area Network," *Wireless Personal Communications*, vol. 120, no. 1, pp. 849–867, Sep. 2021, doi: 10.1007/s11277-021-08493-1.
[13] T. Bhardwaj, C. Reyes, H. Upadhyay, S. C. Sharma, and L. Lagos, "Cloudlet-enabled wireless body area networks (WBANs): a systematic review, architecture, and research directions for QoS improvement," *International Journal of System Assurance Engineering and Management*, vol. 13, no. 4, pp. 1531–1555, Aug. 2022, doi: 10.1007/s13198-021-01508-x.
[14] M. Ali and X. Liu, "Lightweight verifiable data management system for cloud-assisted wireless body area networks," *Peer-to-Peer Networking and Applications*, vol. 15, no. 4, pp. 1792–1816, Jul. 2022, doi: 10.1007/s12083-022-01313-8.
[15] F. Saleem *et al.*, "Ant Lion Optimizer Based Clustering Algorithm for Wireless Body Area Networks in Livestock Industry," *IEEE Access*, vol. 9, pp. 114495–114513, 2021, doi: 10.1109/ACCESS.2021.3104643.
[16] N. Bilandi, H. K. Verma, and R. Dhir, "An Intelligent and Energy-Efficient Wireless Body Area Network to Control Coronavirus Outbreak," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8203–8222, Sep. 2021, doi: 10.1007/s13369-021-05411-2.
[17] I. Albaeazanchi, H. R. Abdulshaheed, S. A. Shawkat, and S. R. B. Selamat, "Identification key scheme to enhance network performance in wireless body area network," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 7, no. 2, p. 895, Jul. 2019, doi: 10.21533/pen.v7i2.606.
[18] S. S. Oleiwi, G. N. Mohammed, and I. Al_Barazanchi, "Mitigation of packet loss with end-to-end delay in wireless body area network applications," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 1, pp. 460–470, Feb. 2022, doi: 10.11591/ijece.v12i1.pp460-470.
[19] S. R. Islam, S. Ullah, M. H. Kabir, M. A. Ameen, and K. Kwak, "A TR-UWB Downconversion Autocorrelation Receiver for Wireless Body Area Network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 516837, Dec. 2009, doi: 10.1155/2009/516837.
[20] I. Al Barazanchi, "An Analysis of the Requirements for Efficient Protocols in WBAN," *J. Telecommun. Electron. Comput. Eng.*, vol. 6, p. 43, 2014.
[21] H. B. Elhadj, J. Elias, L. Chaari, and L. Kamoun, "Multi-Attribute Decision Making Handover Algorithm for Wireless Body Area Networks," *Computer Communications*, vol. 81, pp. 97–108, May 2016, doi: 10.1016/j.comcom.2016.01.007.
[22] H. R. Bdulshaheed, Z. T. Yaseen, and I. I. Al-barazanchi, "New approach for Big Data Analysis using Clustering Algorithms in Information," *Jour Adv Res. Dyn. Control Syst.*, vol. 2, no. 4, pp. 1194–1197, 2019.
[23] I. Al Barazanchi, W. Hashim, A. A. Alkahtani, H. H. Abbas, and H. R. Abdulshaheed, "Overview of WBAN from Literature Survey to Application Implementation," in *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, IEEE, Oct. 2021, pp. 16–21, doi: 10.23919/EECSI53397.2021.9624301.
[24] I. Al-Barazanchi, H. R. Abdulshaheed, and M. S. Binti Sidek, "A survey: Issues and challenges of communication technologies in WBAN," *Sustainable Engineering and Innovation*, vol. 1, no. 2, pp. 84–97, Dec. 2019, doi: 10.37868/sei.v1i2.85.
[25 A. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, M. J. Singh and J. K. S. Paw, "Analytical Survey on the Security Framework of Cyber-Physical Systems for Smart Power System Networks," *2022 International Conference on Cyber Resilience (ICCR)*, 2022, pp. 1-8, doi: 10.1109/ICCR56254.2022.9995780.

BIOGRAPHIES OF AUTHORS

Othman Atta Ismael received the B.Sc. degree in Computer Science from High from Baghdad University in 2006. He received master degree from Mahamta Ghandi College in Computer Science in 2015. He can be contacted at email: othman.atta@aliraqia.edu.iq.

Ahmed Talal Kamil is a lecturer at the Department of Computer Engineering at Aliraqia University Baghdad. He received B.Sc. degree in Computer Science from Almustansryia University College of Science in 2006. He received Master degree in Information Technologies from KADIRHAS Univseriy Istanbul in 2015. He has publications in data mining. He can be contacted at email: AhmedScofeld8@gmail.com and ahmed.talal@aliraqia.edu.iq.

Layth A. Jasim received Bachelor in Computer Engineering from ALmamoun University, Iraq in 2010, he received Master of Computer Engineering Erciyes University in 2018, and Ph.D. Student in UNITEN University Malaysia. He can be contacted at email layth.jasim@aliraqia.edu.iq.

Poh Soon JosephNg graduated with a Ph.D. (IT), Master in Information Technology (Aus), Master in Business Administration (Aus), and Associate Charted Secretary (UK) with various instructor qualifications, professional certifications and industry memberships. With his blended technocrat mix of both business senses and technical skills, has held many multinational corporation senior management positions, global posting and leads numerous 24×7 global mission-critical systems. A humble young manager nominee twice, five teaching excellence awards recipient, numerous research grants, hundreds of citations, and mentored various students competition awards recipient. He has appeared in LIVE television prime time cybersecurity talk show and overseas teaching exposure. His current researches are on strategic IT infrastructure optimization and digital transformation. He can be contacted at email: joseph.ng@newinti.edu.my.