

A new method based on swarm intelligence with encrypted data in wireless sensor networks

Dhuha Kh. Altmemi, Basim Sahar Yaseen

Department of Computer Science, Shatt Al-Arab University College, Basra, Iraq

Article Info

Article history:

Received Oct 10, 2022

Revised Dec 22, 2022

Accepted Jan 1, 2023

Keywords:

GOARP

Lifetime network

Rivest cipher 5

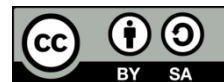
Routing

Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSNs) technology is one of the most essential Internet of things technologies. It is utilized efficiently in a variety of real-world applications, including healthcare, environmental monitoring, and tracking. WSNs are composed of sensor nodes with restricted resources. However, the communication between WSN components is not secure. Therefore, it is necessary to build efficient and lightweight cryptographic algorithms to secure shared data. Our paper comprises proposes a secure protocol called grasshopper optimization algorithm routing protocol (GOARP) with a lightweight encryption method in each sensor called rivest cipher 5 (RC5) to enhance network efficiency and simulation in terms of power consumption, required memory space, and computational time. Subsequently, the network lifetime result achieved in the proposed method is about (70%) more than in GOA elliptic curve cryptographic and Diffie Hellman (GOA-ECCDH).

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Dhuha Kh. Altmemi

Department of Computer Science, Shatt Al-Arab University College

Basra, Iraq

Email: duhakhalf@sa-uc.edu.iq

1. INTRODUCTION

Wireless sensor networks (WSNs) are decentralized or centralized sensing applications extensively employed in a variety of industries, including medical systems, smart mobility, ecological remediation, and military applications. The most common method for sending data between sensors is wireless transmission. Wireless connection systems are more vulnerable than cable connection systems to threats such as high traffic, forgeries, and accidents. Consequently, WSNs must have a strategy for risk prevention. A technique of cryptography that is both secure and efficient is the most significant of various security methods. WSN is comprised of an assortment of low-cost, low-energy sensing devices. Packets are moved from their source to their destination inside the system. Data packets are sent within a network with the use of sensing devices. Due to energy and bandwidth constraints, sensors can only collect a limited amount of data. The sink node is crucial because it receives data from other sensors and sends it elsewhere in the network for processing. The weaknesses of networks are the primary focus of this research. Due to their volatile nature and potentially hazardous environments, wireless sensor networks are very vulnerable [1].

The result is a choice among different approaches to safety. Security in WSNs is predicated mostly on cryptographic methods. Battery life and storage space are only two of the limitations of WSNs. As a result of these constraints, WSNs are unable to process typical encryption methods. There are two major issues with current WSN encryption methods. First, as much as possible should be done to reduce the burden that encryption systems have on messaging; the sensors' constant chatter uses up a lot of power and shortens the lifespan of the device with every bit sent [2]. To increase the efficiency of encrypted communication, it is

necessary to decrease both the storage capacity and the length of the key [3]. The actual world and cognitive systems can communicate thanks to the WSN that connects them. Sharing login information between users is a common practice, contributing to the rapid expansion of the internet. Confidentiality is particularly important when transmitting data over the internet using encryption. No unauthorized party will be able to access the information or change it in any way. In this way, an adversary can't change or send information. Data is encrypted by cryptographic techniques so that it may be read only by its creator and its intended receiver [4]. When calculating the efficiency of their routing behavior, these networks pay close attention to how long their components are expected to last. Researchers are focusing their attention on decreasing the amount of power required by networks by suggesting new routing techniques for WSNs. To gather and transmit the observed data, protocols have been proposed to choose the best path in the network. It was proposed by Sujanthi and Kalyani [5] that the hop distance of all routes should be minimized. This has resulted in a smaller hop distance relative to the shortest route. The energy required to receive and transfer data over a network was cut in half as a result of the proportional drop. To increase the lifespan of WSNs, Hung *et al.* [6] presented a transmission routing scheme. The A-star algorithm is used in the planning of this technique to obtain an optimal route beginning at the resource node and ending at the destination node. Ovasapyan and Moskvina [7], the authors used a high-weight version of the evolutionary genetic algorithm (GA). So, the current work proposes a new energy-conscious protocol for heterogeneous wireless sensor networks (HWSNs) protocol called grasshopper optimization algorithm (GOA-CR5). The new protocol can combine two approaches, grasshopper optimization algorithm routing protocol [8] with rivest cipher 5 (RC5) [9]. So, CR5 is used to encrypt the sensing data inside the clusters by the cluster heads to send by routing protocol through the optimal path to the sink for WSNs by using the GOA.

This paper is organized as follows: In section 2, previous work related to the research is briefly presented. In section 3, the security of WSN information is presented. Section 4, presented RC5 with GOARP proposed for WSNs. Section 5 introduces the performance evaluation of the proposed method with simulation results presented. Finally, the conclusion of this paper is presented in section 6.

2. RELATED WORKS

Several researchers have highlighted the problem of routing in WSNs. MBCC uses 13.44% less random access memory (RAM) for encryption and decryption, as well as 6.4 and 6.6 times less energy and time for encrypting 32-bit data, respectively, according to our comparative research. Increasing the length of the modified block cipher chaotic (MBCC) key, periodically generating the master key on the base station, and periodically generating the round key on the sensors are analyzed further to avoid brute-force assaults. A comprehensive evaluation of cipher approaches in terms of energy, time, memory, and security demonstrates that the MBCC algorithm is suitable for resource-constrained wireless sensors with security needs [10]. In this approach, the minimal number of active S-boxes must be determined for several rounds of the lightweight ciphers KLEIN, light emitting diode (LED), and advanced encryption standard (AES). We used the technique given in, in which the determination of the minimal number of active S-boxes is framed as a mixed integer linear programming (MILP) problem. Under the limitations given by differential propagation of the cipher, the goal function is to reduce the number of active S-boxes. In this study, the experimental findings are given and deemed promising [11].

Al Mazaidh and Levendovszky [12] developed a unique strategy for clustering HWSNs, one that makes optimal use of choosing the head of the cluster nodes, the degree of sensor nodes, and the remaining energy. As a bonus, the information package is gathered and sent via a chaining mechanism. In both the homogeneous WSNs, and the heterogeneous HWSNs [13], they suggested a swarm-based intelligence mechanism dubbed spider monkey optimization routing protocol (SMORP). The best route across the network may be determined using this technique. The IBchain technique allows smart objects to link securely with other smart items in a variety of scenarios. IBchain develops a new IoT-based blockchain processing setup. The IBchain might study blockchain concerning its primary competence or it could enhance the IoT's certification and credibility. It strengthens blockchain and the cloud to create an IoT-ubiquitous environment that facilitates safe communication between smart devices [14].

Kukkurainen *et al.* [15] investigations focus on the increase in computing time and energy consumption caused by the implementation of higher security features and levels. Hussain and El-Howayek [16], the authors suggest a novel routing protocol at the sea's surface, fusing two-dimensional underwater wireless sensor networks (UWSNs) with sleep-scheduling routing to detect and report oil traces to the sink as soon as possible. Reducing end-to-end time and energy usage was the goal of the routing strategy published in [17], which made use of the K-nearest neighbor (K-NN) algorithm and the clustering technique. In this proposal, we provide a least-distance-generation clustering strategy based on node categorization. To lower energy consumption in WSNs, Yu and Ku [18] introduced a novel balanced routing method with two

uncorrelated channels. With this concept in place, each node may choose between the two shortest pathways to the sink, thus halving the traffic burden on the network. Alshawi *et al.* [19] presented fuzzy Dstar-lite, a routing approach, to provide the best possible information routing for HWSNs. Along with illuminating the unbalanced energy dissipation (UED) issue in the network, it also highlights the need of going above and beyond the obstruction example. Nandan *et al.* [20], the authors suggest a routing strategy for WSNs. It enhances the network effect of the particle swarm method by enabling particles to make direct touch with each other throughout the network construction phase. They suggested a GA to choose the best cluster head (CH) [21]. Four different factors node density, distance, energy, and the capacity for heterogeneous nodes to build fitness functions re taken into account during GA-based CH selection. By considering them, it is possible to determine the cluster's total energy, the number of necessary hops, and the optimal nodes for CHs. Rajendran and Nagarajan [21] prevents premature network death due to disconnected sensors. The EFRP suggests that each node include a backup route to allow for quick rerouting between sources and destinations.

This work introduces RC5-based encryption and cipher block chaining-message authentication code (CMAC) authentication, which are utilized to ensure data privacy, freshness, replay protection, authentication, and integrity. Due to the increased computational and communication demands, these characteristics might impair the operability of sensor networks. By choosing an appropriate method and operating circumstances for encryption and authentication.

3. NETWORK SECURITY

WSN consisted of many nodes. These nodes have restricted capabilities and functions. In addition, these nodes have limited storage capacities and limited communication y of nodes is restricted because of their limited storage capacity and limited communication. Also contributing to the limitations of WSNs is the limited energy available to the nodes. In addition, the size of the nodes is modest. Due to the limits and limitations of WSNs, it is more difficult to directly optimize security methods. WSN is subject to several limitations. Energy limitation is the most important restriction in a WSN since the transmission of bits in a WSN requires a substantial amount of energy. Alkenani and Nassar [22] concludes that the amount of energy required to transport a bit is similar to 700-1000 instructions. As a result, the cost of transmission exceeds the cost of calculation. The energy limits have been separated into three categories: energy for the sensor transducer, energy for sensor transmission, and energy for microprocessor calculation. Memory limitations follow. Due to the sensor's diminutive size, the sensor's memory capacity is inadequate. Flash and RAM are the types of memory found in nodes. As a result, a threat actor may listen in on all communications, plant malicious packets, retransmit previously sent messages, or infect a sensor node. Preserving user anonymity and authenticating sensors are two of the biggest concerns for sensor nodes. To accomplish privacy, data confidentiality must be implemented under a security mechanism, and this in turn makes it possible for secure communications to take place in the network between sensor nodes and the management station. Additionally, a well-organized authentication method can guarantee that no rogue nodes may fraudulently join WSNs and get private data. Consequently, a variety of strategies for protecting data transmissions in WSNs have been suggested. Based on the underlying cryptographic methods, we divide them into three categories in this chapter: symmetric keys, asymmetric keys, and one-way hashing functions. The downloaded application codes are stored in the nodes' flash memory. In contrast, RAM stores application data. High latency is an additional limitation. Due to the existence of multi-hop routing in WSN, the high processing time of nodes and network congestion result in increased latency. Consequently, it might be challenging to establish synchronization at times. The following restriction is unattended operation. When nodes are put in distant areas, they are left unattended in the majority of situations. This renders them susceptible to physical assaults in a certain setting. Managing a distant WSN makes the detection of physical manipulation very challenging. Unreliable communication is another obstacle that must be overcome [23].

This limitation causes channel failures or channel dropping, which harms the packets. Routing is built on a connectionless mechanism, making it unstable. Due to the broadcasting nature of the transmission medium, the wireless network becomes susceptible to assault. As a result of its location in a hostile environment, the WSN's nodes are also physically unsafe. The assaults on the WSN may be divided into two distinct categories: attacks against the security mechanism and attacks against the fundamental mechanism. Denial of service (DoS) attacks constitute the remaining WSN assaults. In this specific form of assault, nodes malfunction unintentionally. The simplest DoS attacks aim to overwhelm the node by sending unnecessary packets, so depleting the node's energy. The dos attacks may also be categorized as Sybil assaults: in the Sybil attack, a single network node exposes numerous identities to other network nodes. This exploit allows the attacker to be present in many locations. The Sybil attack attempts to compromise the security and integrity of data. This attack also targets the fault-tolerant multipath routing system. Encryption of data and authentication of data are the countermeasures for the Sybil attack. These methods may aid in the elimination of the Sybil assault. Public key cryptography is also beneficial for preventing this attack, but it's a costly solution. In this assault, the physical layer is once again attacked. In this

attack, the node is taken and sensitive information, such as the public and private keys of the nodes, is retrieved. This kind of assault occurs at the data connection layer. In this scenario, two nodes simultaneously try to communicate on the same frequency, resulting in a collision [24].

Additionally, an attacker attempts to induce collisions in certain packets. The error-correcting codes serve as the anti-collision countermeasure. This assault, known as the "hello flood" attack, is a unique one against the WSN. The hello packets are used as the primary weapon to seize control of the WSN sensors. In this attack, the attacker attempts to squander a significant amount of the node's energy using laptop-class assaults which can cause a routing delay. Jamming: this sort of DoS attack targets the physical layer of the WSN. The radio frequency interference caused by the jamming leads to the disconnection of the established connection. It may disrupt the signal in two ways: first, if the source is strong, it can disrupt the whole network; second, if the portion is tiny, it can disturb just a piece of the overall network [25].

4. RC5 WITH GOA FOR WIRELESS SENSOR NETWORKS

The sensors have limited resources, such as limited processing speed, storage capacity, and communication bandwidth. The routing protocol is a method for selecting appropriate data pathways from source to destination. Depending on the kind of network, channel characteristics, and performance metrics, the technique faces a variety of challenges while determining the ideal route. Typically, the data collected by sensor nodes in a WSN is sent to the base station, which connects the sensor network to other networks, where it is collected, and evaluated, and action is taken appropriately. The proposed method represents the process of encryption and routing data for WSNs. The sensor node is first distributed at random throughout the network region. Using a grasshopper optimization technique, the routing route is determined by avoiding dangerous nodes while providing a secure routing path. The encryption and decryption procedure is then used to send the secure data through the network medium. Based on the routing criteria, the GOA decides which node the sensor will connect to next (maximum remaining energy, fewest hops, and lowest traffic load). This paper assumes: i) all sensors start with the same amount of battery life and the same transmission range; ii) all sensors know where they are and where their neighbors are; iii) the range of transmission and the initial battery power required for all sensors is the same; and iv) every sensor knows its relative position to the other sensors and the sink. This proposal is divided into two parts, in the first part, a security protocol called GOA is defined, while in the second part, an encryption algorithm is included to improve network performance and protect it from attacks using the RC5 algorithm.

4.1. Grasshopper optimization algorithm

Grasshopper optimization algorithm (GOA) is the newest population-based swarm algorithm. GOA takes into account the crucial characteristic of grasshopper swarms to seek food sources. Therefore, the process of locating food is separated into two categories: exploration and exploitation. During exploration, the search agent urges them to move quickly, but during exploitation, they prefer to wander locally. Exploration and exploitation are the two categories in which the grasshopper natural is conducted. The GOA mimics grasshopper swarm dynamics and social interaction. In addition, the mathematical model is used to promote the grasshopper's swarming tendency, which reduces the power consumption of sensor nodes and thus extends the life of the network. Algorithm 1 shows the pseudo code grasshopper optimization.

Algorithm 1. Grasshopper optimization algorithm

```

Generate the initial population of Grasshoppers  $P_i (i=1,2,\dots,n)$  randomly
Initialize  $c_{min}$ ,  $c_{max}$  and maximum number of iteration  $t_{max}$ 
Evaluate the fitness  $f(P_i)$  of each grasshopper  $P_i$ 
 $T =$  the best solution
while ( $t < t_{max}$ ) do
  Update  $c_1$  and  $c_2$  using,  $c = c - (max) - t \frac{(c_{(max)} - c_{(min)})}{t_{max}}$ 
  For  $i = 1$  to  $N$  (all  $N$  grasshoppers in the population) do
    Normalize the distance between grasshoppers in the range  $[1,4]$ 
    Update the position of the current grasshopper
    Bring the current grasshopper back if it goes outside the boundaries
  end for
  Update  $T$  if there is a better solution
   $t = t + 1$ 
end while
Return the best solution  $T$ 

```

When thinking about how to make WSNs last longer, the routing protocol is a crucial consideration. Information cannot be sent between sensor nodes if any of them die during the routing protocol because of a lack of power. Throughout their lifespan, this usually causes a deficiency in WSNs. Considering that the

lifetime of a WSN is proportional to the power it receives, sensors must be designed to minimize power consumption. In this regard, the GOA may increase the durability of WSNs by reducing power consumption and ensuring that it is distributed fairly throughout the network.

4.2. RC5 algorithm

Ron rivest designed the RC5 protocol. It is a technique for block encryption based on the symmetric key. The primary characteristic of this is its speed since it employs just basic computer functions. It permits a configurable number of rounds and variable bit size to increase adaptability. Using RC5 has the added benefit of requiring less RAM for execution. This capability allows RC5 to be used for a variety of reasons, including desktop operation and smart cards. The input plain text block size, number of rounds, and 8-bit bytes of the key are variable lengths in the RC5 method. Once the values of this have been determined, they will stay unchanged for each iteration of the cryptographic method. Plain text blocks may be 32 bits, 64 bits, or 138 bits in size. Key length may range from 0 to 2040 bits. The output of RC5 is cipher text with the same size as plain text. Figure 1, shows the RC5 algorithm.

This work discusses RC5-based encryption, privacy, freshness, authentication, and integrity. Due to the increased computational and communication demands, these characteristics might impair the operability of sensor networks. By choosing an appropriate method and operating circumstances for encryption and authentication, the data security of wireless sensor networks may be enhanced with minimal resource consumption. If the data transfer cannot be physically protected through wired transmissions or another mechanism, the only approach to increase security is to encrypt the message. These requirements restrict the utility of the application and are thus disregarded in WSNs. Encryption in WSN solutions is often performed using a symmetric cryptosystem such as RC5.

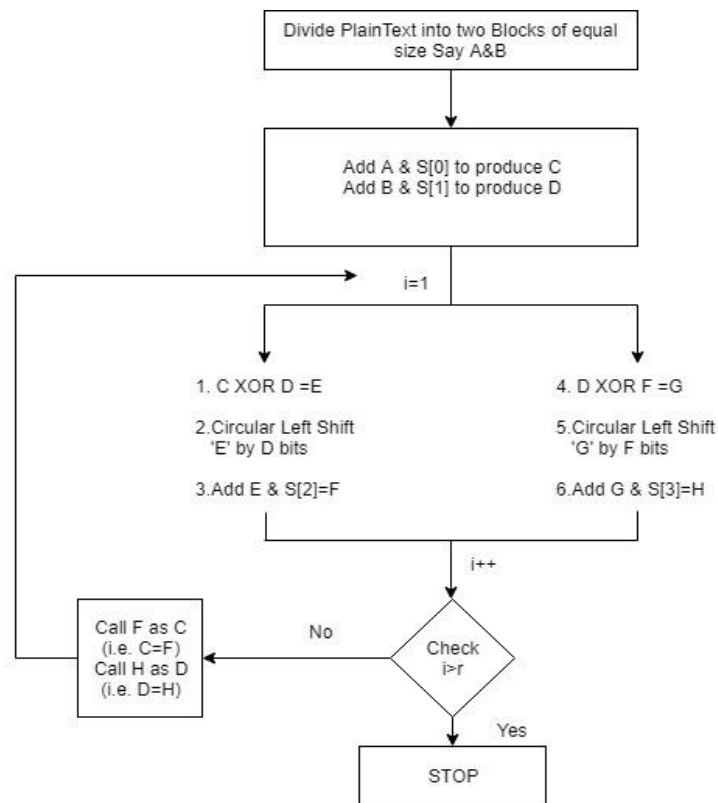


Figure 1. RC5 algorithm

4.2.1. Key expansion

The procedure for key expansion increases the user's secret key K to fill the extended key array S. The procedure for key expansion employs two magical constants. The key expansion method conducts a series of sophisticated operations on the secret key to generate the total subkeys denoted by t. Each subkey consists of a single word. Two subkeys are utilized in each round, and two subkeys are used in a non-round-specific addition operation, so $t=2r+2$. Techniques used to generate subkeys:

- The subkeys are stored in a t word array labeled S[0],S[1],S[t+1].
- The parameters r and were inputs.
- Then the b byte key, K[0, b-1] is converted into a c-word array L[0, c-1].
- This is performed on a little-endian computer by zeroing off the array L and immediately copying the string K into the memory locations indicated by L.
- If b is not an integer multiple of w, the rightmost component of L stays 0.
- Finally, a mixing operation is conducted by applying the contents of L to the initialized value of S to obtain the array S's final value.

4.2.2. Encryption algorithm

The input block of the RC5 encryption technique consists of two w-bit registers A and B, and the output is also stored in the same register. After round I has concluded, the variables LE_i and RE_i represent the left and right halves of the data, respectively. Algorithm 2 as shown in:

Algorithm 2. RC5 encryption algorithm

```

LE0 = A+S[0]; RE0 = B+S[1];
for i= 1 to r do
  LEi=( (LEi-1 XOR REi-1) <<<REi-1)+S[2*i];
  REi=( (REi-1 XOR LEi) <<<LEi)+S[2*i+1];
end for

```

The resultant ciphertext comprises the two variables LE_r and RE_r, and each of the r rounds consists of a substitution using both data words. A permutation is generated using both data words and a key-dependent replacement. Two rounds of DES are comparable to one round of RC5.

4.2.3. Decryption algorithm

The decryption algorithm may be simply derived from the RC5 encryption algorithm. The result of the encryption algorithm is 2w bits of cipher text. Initially, these bits are allocated to the single-word variables LD_r and RD_r. The variables LD_i and RD_i represent the left and right halves of the data before round I where the rounds are numbered from r to 1 inclusive. Algorithm 3 as shown in:

Algorithm 3. RC5 decryption algorithm

```

for i = r down to 1 do
  RDi-1=( (RDi-S[2*i+1] >>>LDi) XOR LDi); LDi
  l=( (LDi-S[2*i] >>>RDi) XOR RDi);
  B = RD0-S[1];
  A = LD0-S[0];
end for

```

This paper covers the RC5 encryption technique, a symmetric block cipher that may be implemented in hardware or software. A distinctive characteristic of RC5 is its extensive usage of data-dependent rotations. RC5 features a variable word size, variable rounds, and a variable secret key length. The encryption and decryption techniques are really simple. The RC5 algorithm should be a symmetric block cipher. Encryption and decryption both use the same secret cryptographic key. The plaintext and ciphertext are bit sequences of defined length (blocks). RC5, applicable to both hardware and software. This implies that RC5 employs just the computing primitives typically present in microprocessors. This almost indicates that RC5 is word-oriented, given the fundamental computing operations are operators that operate on complete words of data at a time.

5. EVALUATION OF PERFORMANCE

The main objective of this work is to create the GOA-ECCDH [26]. In this paper, we assume that many sensors send the events. Thus, the network is optimized by the encryption process in sensors. There is a comparison between the GOA-ECCDH and the simulation results for the suggested approach.

5.1. Simulation setting

Simulation processes are executed through the use of MATLAB because it provides powerful simulation and plotting tools in addition to a productive software environment. In this simulation, a WSN consists of one hundred sensor devices arbitrarily distributed over a square region that has an area of 10,000 m² (i.e., 100-meter x 100-meter dimensions). And each sensor is capable of wireless communication within a range of (30 meters). The simulated network has only one base station placed in the top-right corner of the area and its (x, y) coordinate is (90 m, 90 m). The initial energy amount of each sensor is (0.5 joule). Energy

consumption amounts are calculated using “first order radio model” which is frequently used to evaluate the efficiency of routing protocols and it is described. As demonstrated in this model, the energy amounts consumed by sending and receiving a data packet are $(E_{elec} * k + E_{amp} * k * d^2)$ and $(E_{elec} * k)$ respectively. Where E_{elec} is the energy exhausted for each bit in the circuitries of data transmitting and receiving, E_{amp} is the energy needed per each bit to the amplifier to produce an appropriate signal/noise ratio (SNR), k is the number of bits contained within each packet (i.e., packet size) and d is the distance of wireless communication between sender and receiver sensors. The values assigned for E_{elec} is (50 nJ/bit) and for E_{amp} is (100 nJ/bit/m²). The traffic load value specified to each node is an integer generated randomly within [1..10] value. Details of the parameters used in the simulations are given in Table 1.

Table 1. Simulation parameters

Parameter	Value
Area of topographical	100 m x 100 m
Location of the sink	(90, 90)
Length of control packets	2k
No. of transmission packets (rounds)	2×10^3
Number of nodes	1000
Limit of transmission distance	20 m
Initial energy	0.5 J
sensors	
E_{elec}	50 nJ/bit
E_{amp}	100 pJ/bit/m ²
Max. traffic in node's queue	10

5.2. Simulation results

The life of WSN can be extended by using an RC5 encrypted method with a routing protocol called GOA that has been optimized in to increase energy efficiency. To see how well it worked, it was tested in the amount of power left in each sensor and the number of sensors that survive during each cycle, if the same routing metrics and the same environment were used in both. By keeping track of how many sensors are still operational after each iteration of data, we can compare the two sets of findings collected for network longevity. At this point, Figure 2 shows the proportion of sensors, which are still alive in each method. As a result, the performance of the proposed method outperforms the performance of GOA-ECCDH. Based on the current number of functional nodes in the network, we find that GOA-ECCDH consumes more energy than the suggested approach. In this case, the network lifetime result attained in the suggested technique is around (70%) greater than in GOA-ECCDH after delivering (2000) packets to two sensors over the network. Depending on the system, the amount of energy still stored in the sensors decreases with each transfer cycle. When compared to the GOA-ECCDH technique, the GOA-RC5 performs better and uses fewer resources. As can be seen in Figure 3, the amount of power left over for the sensors changes depending on the transfer method. For obvious reasons, the GOA-RC5 approach is superior than the GOA-ECCDH in terms of preserving network stability for as long as feasible.

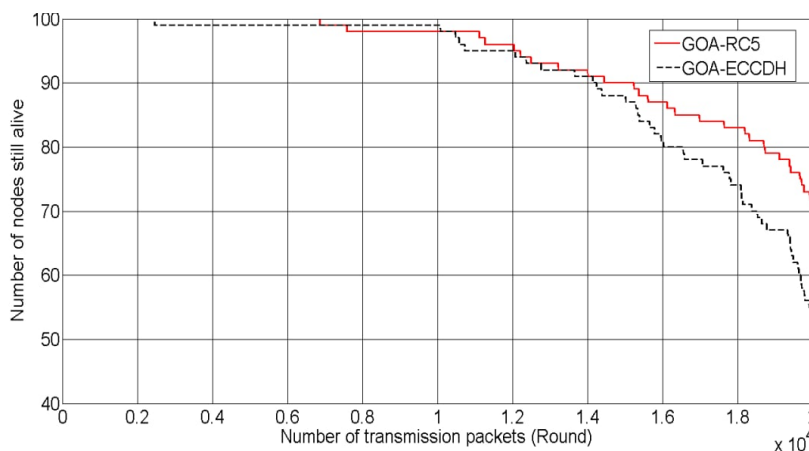


Figure 2. The sensors ratio remains alive

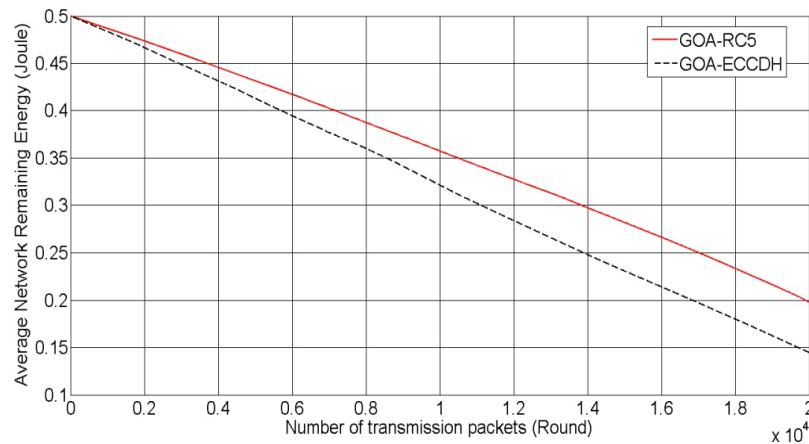


Figure 3. The ratio of leftover sensors' energies

6. CONCLUSION

WSN consisted of many nodes. These nodes have restricted capabilities and functions. In addition, these nodes have limited storage capacities and limited communication y of nodes is restricted because of their limited storage capacity and limited communication. Due to the limits and limitations of WSNs, it is more difficult to directly optimize security methods. WSN is subject to several limitations. Energy limitation is the most important restriction in a WSN since the transmission of bits in a WSN requires a substantial amount of energy. This paper comprises proposes a secure protocol, grasshopper optimization algorithm routing protocol (GOARP), with a lightweight encryption mechanism in each sensor, rivest cipher 5 (RC5), to improve network efficiency and simulation in terms of power consumption, needed memory, and computing time.




REFERENCES

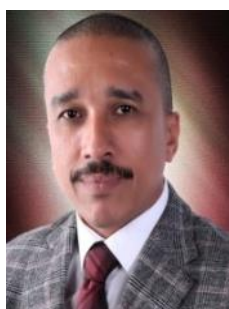
- [1] K. Shankar and M. Elhoseny, "Multiple share creation with optimal hash function for image security in WSN Aid of OGWO," in *Lecture Notes in Electrical Engineering*, vol. 564, 2019, pp. 131–146, doi: 10.1007/978-3-030-20816-5_9.
- [2] J. K. Alkenani and K. A. Nassar, "Network performance analysis using packets probe for passive monitoring," *Informatica*, vol. 46, no. 7, Nov. 2022, doi: 10.31449/inf.v46i7.4307.
- [3] N. Varela, O. B. Pineda Lezama, and H. Neira, "Information security in WSN applied to smart metering networks based on cryptographic techniques," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 6, pp. 8499–8506, Dec. 2020, doi: 10.3233/JIFS-189167.
- [4] J. Alkenani and K. A. Nassar, "Enhance work for java based network analyzer tool used to analyze network simulator files," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 2, pp. 954–962, Feb. 2023, doi: 10.11591/ijeecs.v29.i2.pp954-962.
- [5] S. Sujanthi and S. N. Kalyani, "SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT," *Wireless Personal Communications*, vol. 114, no. 3, pp. 2135–2169, Oct. 2020, doi: 10.1007/s11277-020-07469-x.
- [6] L.-L. Hung, F.-Y. Leu, K.-L. Tsai, and C.-Y. Ko, "Energy-efficient cooperative routing scheme for heterogeneous wireless sensor networks," *IEEE Access*, vol. 8, pp. 56321–56332, 2020, doi: 10.1109/ACCESS.2020.2980877.
- [7] T. Ovasapyan and D. Moskvina, "Security provision in WSN on the basis of the adaptive behavior of nodes," *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, pp. 81–85, 2020, doi: 10.1109/WorldS450073.2020.9210421.
- [8] L. Abualigah and A. Diabat, "A comprehensive survey of the Grasshopper optimization algorithm: results, variants, and applications," *Neural Computing and Applications*, vol. 32, no. 19, pp. 15533–15556, 2020, doi: 10.1007/s00521-020-04789-8.
- [9] A. Utama and R. F. Siahaan, "Application of cryptography for securing deposit transaction data on easy tronik with the RC-5 method (in Bahasa)," *Jurnal Ilmu Komputer dan Sistem*, vol. 3, no. 3, pp. 29–39, 2021, doi: 10.9767/jikomsi.v3i1.1.86.
- [10] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali, and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes," *IEEE Access*, vol. 7, pp. 8737–8753, 2019, doi: 10.1109/ACCESS.2018.2886384.
- [11] V. Tiwari, N. Jampala, A. N. Tentu, and A. Saxena, "Towards finding active number of s-boxes in block ciphers using mixed integer linear programming," *Informatica*, vol. 45, no. 6, pp. 77–87, Oct. 2021, doi: 10.31449/inf.v45i6.3427.
- [12] M. Al Mazaidh and J. Levendovszky, "A multi-hop routing algorithm for WSNs based on compressive sensing and multiple objective genetic algorithm," *Journal of Communications and Networks*, vol. 23, no. 2, pp. 138–147, Apr. 2021, doi: 10.23919/JCN.2021.000003.
- [13] I. S. Alshawi, Z. A. Abbood, and A. A. Alhijaj, "Extending lifetime of heterogeneous wireless sensor networks using spider monkey optimization routing protocol," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 1, pp. 212–220, Feb. 2022, doi: 10.12928/telkomnika.v20i1.20984.
- [14] T. Alam, "IBchain: internet of things and blockchain integration approach for secure communication in smart cities," *Informatica*, vol. 45, no. 3, pp. 477–486, Sep. 2021, doi: 10.31449/inf.v45i3.3573.
- [15] J. Kukkurainen, M. Soini, and L. Sydänheimo, "RC5-based security in wireless sensor networks: utilization and performance," *WSEAS Transactions on Computers*, vol. 9, no. 10, pp. 1191–1200, 2010.




- [16] A. Hussain and G. El-Howayek, "A sleep-scheduling oil detection routing protocol for smart oceans using internet of things," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, Jun. 2020, pp. 1–6, doi: 10.1109/WF-IoT48130.2020.9221438.
- [17] P. Tembhre and K. Cecil, "Low power consumption heterogeneous routing protocol in WSN," in *2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, Nov. 2020, pp. 310–314, doi: 10.1109/RTEICT49044.2020.9315644.
- [18] C. M. Yu and M. L. Ku, "A novel balanced routing protocol for lifetime improvement in WSNs," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, Jan. 2022, pp. 1–3, doi: 10.1109/ICCE53296.2022.9730409.
- [19] I. S. Alshawi, A.-K. Y. Abdulla, and A. A. Alhijaj, "Fuzzy dstar-lite routing method for energy-efficient heterogeneous wireless sensor networks," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 19, no. 2, pp. 906–916, Aug. 2020, doi: 10.11591/ijeecs.v19.i2.pp906-916.
- [20] A. S. Nandan, S. Singh, R. Kumar, and N. Kumar, "An optimized genetic algorithm for cluster head election based on movable sinks and adjustable sensing ranges in IoT-based HWSNs," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5027–5039, Apr. 2022, doi: 10.1109/JIOT.2021.3107295.
- [21] S. K. Rajendran and G. Nagarajan, "Network lifetime enhancement of wireless sensor networks using EFRP protocol," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1769–1787, Mar. 2022, doi: 10.1007/s11277-021-09212-6.
- [22] J. Alkenani and K. Nassar, "Network monitoring measurements for quality of service: a review," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 18, no. 2, pp. 33–42, Dec. 2022, doi: 10.37917/ijeee.18.2.5.
- [23] D. K. Altmemi, A. A. Abdulzahra, and I. S. Alshawi, "A new approach based on intelligent method to classify quality of service," *Informatica*, vol. 46, no. 9, Dec. 2022, doi: 10.31449/inf.v46i4.4323.
- [24] F. Afianti, Wirawan, and T. Suryani, "Lightweight and DoS resistant multiuser authentication in wireless sensor networks for smart grid environments," *IEEE Access*, vol. 7, pp. 67107–67122, 2019, doi: 10.1109/ACCESS.2019.2918199.
- [25] A. B. Feroz Khan and G. Anandharaj, "A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT," *Wireless Personal Communications*, vol. 119, no. 4, pp. 3149–3159, Aug. 2021, doi: 10.1007/s11277-021-08391-6.
- [26] G. Halidoddi and R. Pandu, "A GOA based secure routing algorithm for improving packet delivery and energy efficiency in wireless sensor networks," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 6, pp. 311–320, Dec. 2021, doi: 10.22266/ijies2021.1231.28.

BIOGRAPHIES OF AUTHORS



Dhuha Kh. Altmemi    is she holds a master's degree in wireless sensor networks, from the Computer Science Department, College of Computer Science and Information Technology, University of Basra, located in his hometown of Basra, Iraq. She received a B.Sc. degree in Computer Science at Shatt Al-Arab College, Basra, Iraq, in 2018. Recently, she has been interested in data mining and wireless sensor networks. She can be contacted at email: duhakhalf@sa-uc.edu.iq.



Basim Sahar Yaseen    is the Doctorate of Philosophy in the IT Department of Computer Science, Shatt Al-Arab University College, Basra, Iraq. He is interest in cryptography in computer science, computer security and reliability, skills, and expertise in security information security. He can be contacted at email: basimsahar@sa-uc.edu.iq, basim17814@gmail.com.