Secure Routing Protocol for WSNs Using Bacterial Foraging Optimization and Improved RC4

Hasan H. Al-badrei [1], Imad S. Alshawi[*2]
Email: hasanabohmod@gmail.com[1], emad.alshawi@uobasrah.edu.iq[2]
[*]Imad S. Alshawi
Department of Computer Science, College of Computer Science and Information Technology,
University of Basrah, Basrah, IRAQ

Keywords: Bacterial Foraging Optimization, IRC4, Network lifetime, Routing, Security, WSN

Received: July 8, 2022

Wireless sensor networks (WSNs) have recently received important sponsorship in various fields, such as medical treatment, emergency response, environmental monitoring, military monitoring, outer space research, etc. Sensor nodes are usually limited in capabilities, including batteries. These networks can handle critical data in hostile and uncontrolled environments. Sensor nodes are deployed in harsh, hazardous, or hard-to-reach environments, making it difficult to replace or recharge these batteries, so it is important to consider the security and energy consumption issues when designing such networks. Therefore, this paper proposed a new secure and energy-efficient routing protocol called Improved RC4 with Bacterial Foraging Optimization Routing Protocol (IRC4-BFORP) for WSNs. IRC4 has represented the improvement of RC4 to make the original algorithm safer and faster. The IRC4 is used to secure the sensing data sensed by the sensors before sending it to the sink. To demonstrate the effectiveness of IRC4 over the original algorithm, some numerical analyses are achieved. The results have shown that IRC4 is more secure than the original algorithm. Also, the BFORP has proposed to send the secure sensing data to the sink by selecting the preferred nodes in the transmission paths. The simulation results prove the effectiveness of the BFORP in reducing energy use and reducing delays on the one hand, compared with the well-known protocols that are used in routing.

Povzetek: Razvit in opisan je nov protokol za WSNje z imenom IRC4-BFORP, ki je v analizah pokazal določene izboljšave.

1 Introduction

Wireless Sensor Networks (WSNs) are leading the endeavors taken to construct and send frameworks planning to achieve definitive targets of the Internet of Things (IoT). They are self-designed and foundationless remote systems made of little gadgets outfitted with particular sensors and remote handsets, omnipresent detecting empowered by WSN advances cuts across numerous territories of cutting-edge living. The nodes, in WSN, can sense the environment, can communicate with neighboring nodes, and can, in many cases, perform basic computations on the data being collected. Therefore, the availability of WSNs has promised the development of a wide range of applications in both civilian and military fields. In these applications, a huge of low-price nodes are deployed over the monitoring area to report their sensed data to the central station called the sink [1-3].

Spreading sensor nodes in unfriendly and inaccessible environments makes networks unprotected from a diversity of probable attacks, and it mostly cannot perform continuous monitoring on the network [4]. So, one of the major challenges WSNs face today is security. In WSNs, sensor devices are generally of limited computational capabilities and are powered by small and inexpensive batteries. These limited resources of the sensors make conventional security solutions unfeasible, where the implementation of a strong security algorithm becomes difficult [1, 4]. Besides, sensitive information collected by WSN increased remote and unattended operation causing sensor nodes to be compromised by malicious attacks and intrusions. Moreover, wireless connections make it easier for the opponent to snoop on transmissions of the sensor. For instance, one of the foremost confronting security dangers is a denial-of-service attack, which aims to deactivate the proper operating of the network of sensors. Whilst there are many solutions and technologies for systems distributed that stop attacks or consist of the damage and extent of these attacks, they require much important computing, communications, and requirements of storage, that cannot frequently be met by nodes of the resource-restricted sensor [4]. So, the security issue in sensor networks is not easy compared with conventional desktop computers [5].

In symmetrical cryptography, there are two classes of encryption methods: stream and block ciphers. The stream ciphers method is the best choice for most security protocol designers for WSNs. It is faster and has less complex hardware circuitry than block ciphers [6, 7]; where a WSN may use thousands of sensor nodes. So, these need simple, adaptable, and scalable security protocols.

Several routing algorithms work the same behavior when it comes to minimizing the total energy consumption in the network while draining the network's regular energy [8]. The partition of the Network arises as a result of these behaviors, as nodes connected to several network parts waste battery energy more quickly than nodes connected to only one part of the network[9, 10]. As a result, the transmission delay is frequently reduced by using the same route in a protocol for all subsequent conversations. The nodes' energy in this route is therefore rapidly depleted[10, 11]. These algorithms frequently alter the energy usage of WSNs to reduce the total amount of power consumed. As a result, this algorithm owns the state of a division of the network damaging the advantages of the WSNs [12]. When some sensor nodes are hard to reach, the network part problem shows in Figure 1.

So, a WSNs lifetime is consumed immediately after the battery's energy is depleted in the "essential nodes". Critical sensor nodes are usually located on many route paths. Routes should reduce energy usage and distribute it more uniformly among nodes, such that all network nodes are drained at the same time[13]. Once the energy of the node's battery transfers for the segmentation of a WSN, the WSN life is ended. Therefore, the challenge is to suggest a set of procedures for each node to create a path so that it may transmit signals based on specific standards, or to an appropriate path that is configured for the signals sent by lengthening the WSN's life span [12, 14]. Then there's the "problem of optimization” which entails extending this duration, with parameters of the route as the variables. Therefore, this paper proposes a secure and energy-efficient routing protocol for WSNs using an improved RC4 (IRC4) encryption algorithm with a Bacterial Foraging Optimization Routing Protocol (BFORP). The proposed protocol is called IRC-BFORP) which first uses the IRC4 algorithm to secure the sensed data generated by the sensors before it is sent. After that, the BFORP is used to find the perfect path to the sink by some routing metrics (i.e., the remaining energy in the selected nodes, the distance to the sink, and the traffic load in the nodes).

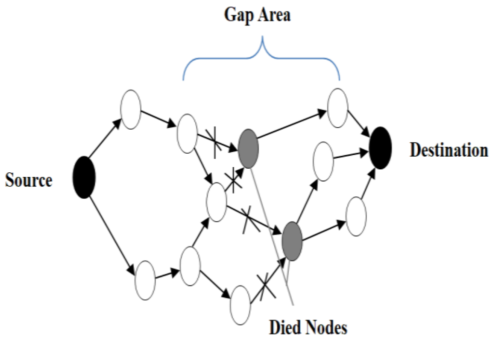

Figure 1 :Network field partitioned Because of the death of some nodes

The rest content of this paper is as follows. Section 2 delves into related work and concepts. Section 3 describes the proposed encryption technique IRC4 in detail with the simulation results. Section 4 goes into the BFORP proposed algorithm in detail with the simulation results. Section 5 addresses the IRC4-BFORP protocol resulting from the process of integrating both approaches in detail with the results. Finally, in Section 6, there is a succinct conclusion.

2 Related work

WSN security requires cryptographic protocols, and several cryptographic primitives have been developed particularly for WSNs. Sensors can generate cryptographic hash functions and perform symmetric key encryption or authentication systems. On the other hand, the energy savings issue requires finding an appropriate energy consumption protocol using a fair amount of their resources. In this section, relevant works addressing the most important authentication and encryption/decryption problems are discussed in addition to energy-efficient. In [15] Karlof et al. suggested a security mechanism known as "TinySec" in the link-layer for WSNs, performed on the operating system of TinyOS, To cope with processing, storage in sensor nodes, and energy constraints. TinySec exceeds the WSNs implicit constraints, such as limited channels for which kept the data secure and relatively short life, to select the cryptographic primitive's variables that are used. There are two operation modes in TinySec: authentication alone (TinySec-Auth) and authentication/encryption (TinySec-AE). During the mode of authentication-only, authenticates of protocol on the packet by using the MAC address. In the second mode (TinySec-AE), the protocol authenticates the entire packet with a Message Authentication Code (MAC) and encrypts the data portion. In [16] the Alliance of ZigBee introduced the standards of the network of ZigBee based on the standard IEEE 802.15.4. The system of security is distributed across the network layers as follows: 1) the sub-layer of MAC ensures reliable transmission of single-hop. The security level is determined in the top layers. 2) the manager of requests for routing, broadcasting, and processing is done by the network layer. 3) The application layer offers transport services and the key establishment to the applications and ZigBee Device Object (ZDO). The (AES) 128 bit is used by the media access control (MAC) layer as its basic cryptographic. The authors of [17] presented an algorithm that does a chaotic uniform cipher and a chaotic Feistel cipher. The goal is to investigate the connection between crypto components from both a cryptography standpoint and a dynamical system. M. Luk et al. [18] suggested a safe network layer protocol for WSNs known as MiniSec. There are two operating modes, the first for transmission of broadcast and the second used for transmission of unicast. The two approaches implement Offset Code Block OCB and Bloom filters. The protocol deal with AES keys of 128-

bit. Jiandong [19] proposed an algorithm for producing pseudorandom sequences and ideal uniform distribution. The plus and bit shift computation is used to generate the key using joined integral tent mapping algorithm and then consolidates the

Ref	Methodology	Performance/Results
(Wendi Rabiner et al(2000))	• Developed new energy efficient technique (LEACH) for WSNs	• The propose LEACH protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network. • LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station.
(Stephanie Lindseyet al(2002)	• Developed new energy efficient technique (PEGASIS) for WSNs	• The propose PEGASIS which is a near-optimal chain-based protocol that minimizes energy. • In PEGASIS, each node communicates only with a close neighbor and takes turns transmitting to the base station, thus reducing the amount of energy spent per round.
(Karlof et al,2004)	• Developed a new Secure technique (TinySec) for WSNs	• The Suggested a security mechanism known as "TinySec" in the link-layer for WSNs, performed on the operating system of TinyOS, To cope with processing, storage in sensor nodes, and energy constraints. • TinySec exceeds the WSNs implicit constraints, such as limited channels for which kept the data secure and relatively short life, to select the cryptographic primitive's variables that are used. • There are two operation modes in TinySec: authentication alone (TinySec-Auth) and authentication/encryption (TinySec-AE).
(Naoki Masuda et al (2006)	• Developed new Secure technique	• The proposed algorithm that does a chaotic uniform cipher and a chaotic Feistel cipher. • The goal is to investigate the connection between crypto components from both a cryptography standpoint and a dynamic system.
(M. Luk et al , 2007)	• Developed a new Secure technique (MiniSec) for WSNs	• The Suggested a safe network layer protocol for WSNs known as MiniSec. • There are two operating modes, the first for transmission of broadcast and the second used for transmission of unicast. The two approaches implement Offset Code Block OCB and Bloom filters. • The protocol deal with AES keys of 128-bit.
(Jiandong, 2008)	• Developed a new Secure technique for WSNs	• The proposed algorithm for producing pseudorandom sequences and ideal uniform distribution. • The plus and bit shift computation is used to generate the key using joined integral tent mapping algorithm and then consolidates the Feistel structure to create a block cipher for WSN.
(Raina et al,2011)	• Modify the security algorithms RC4 and AES	• The proposed many parameters for evaluating two prominent methods of encryption: RC4 and AES. • It is a primary motivator to utilize RC4 as the encryption on small memory and processing nodes to speed up the process and conserve available memory space.
(Wang et al ,2013)	• Developed a new Secure and energy efficient technique (EESSDA) for WSNs	• The Suggested Energy Efficient secures highly accurate and Scalable Scheme for Data Aggregation' protocol that protects data privacy for the nodes in the network.
(Chia-Hui Liu et al (2017))	• Developed new Secure and energy efficient technique for WSNs	• The proposed method a safe user authentication approach for healthcare-related WSNs. • The resource constraints of a WSN make the adoption of public-key encryption/decryption techniques difficult. Because these methods consume a lot of energy to encrypt and decrypt communications they are reduced the network's lifespan.
(Manisha Rathee, 2019)	• Developed newSecure and energy efficient technique (QEBSR) for WSNs	• The proposed a (QEBSR) QoS aware energy balancing secure routing technique for WSNs based on an ant colony optimization algorithm. • Better route determination was achieved by adapting ACO for QEBSR. The QEBSR applied upgraded models for estimating the delay of end-to-end and values of the trust factor.
(Khalid Haseeb et al (2020))	• Developed new Secure and energy efficient technique (SEHR) for WSNs	• The proposed SEHR protocol prioritizes secure data transfer, reliability, and energy efficiency. • To get the best data routing, the proposed protocol used artificial intelligence-based packet inferences. • The SEHR protocol utilizes hop count, aggregated residual energy, and network integrity factors to learn the routing decision.
(Xuanxia Yao et al (2020))	• Developed new Secure and energy efficient technique (ABE and ECC) for WSNs	• The proposed a cryptographic system based on ABE and ECC to address security and privacy challenges in IoT, according to the results, the suggested model had high productivity and low-level computational values.

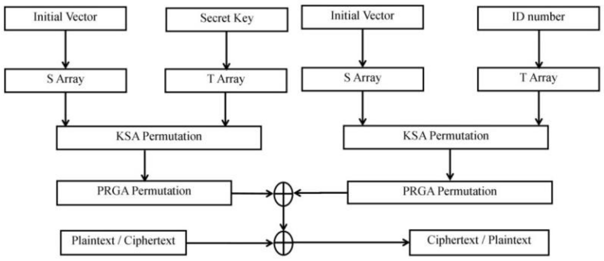

Figure 2: The improved RC4 algorithm

Feistel structure to create a block cipher for WSN. In [20] Raina et al. proposed many parameters for evaluating two prominent methods of encryption: RC4 and AES even though this experiment is conducted on workstations, the performance study opens the door to an alternative to AES when resources are restricted. This is critical because RC4 outscored AES in all criteria, including time of encryption and decryption, time of CPU process, and use of memory. It is a primary motivator to utilize RC4 as the encryption on small memory and processing nodes to speed up the process and conserve available memory space. Wang et al.[21] suggested (EESSDA) 'Energy Efficient secures highly accurate and Scalable Scheme for Data Aggregation' protocol that protects data privacy for the nodes in the network. The authors in [22] suggested a cryptographic system based on ABE and ECC to address security and privacy challenges in IoT, according to the results, the suggested model had high productivity and low-level computational values. In [23] the authors suggested a safe user authentication approach for healthcare-related WSNs. However, the resource constraints of a WSN make the adoption of public-key encryption/decryption techniques difficult. Because these methods consume a lot of energy to encrypt and decrypt communications they are reduced the network's lifespan. Manisha Rathee [24] suggested a (QEBSR) QoS-aware energy balancing secure routing technique for WSNs based on an ant colony optimization algorithm. Better route determination was achieved by adapting ACO for QEBSR. The QEBSR applied upgraded models for estimating the delay of end-to-end and values of the trust factor. Khalid Haseeb et al [25] present a secure and energy-efficient for WSN heuristic routing protocol. The SEHR protocol prioritizes secure data transfer, reliability, and energy efficiency. To get the best data routing, the proposed protocol used artificial intelligence-based packet inferences. The SEHR protocol utilizes hop count, aggregated residual energy, and network integrity factors to learn the routing decision. Table 1 summarizes the related works with their methodology, performance, and results.

3 Improved RC4 (IRC4) method

3.1 IRC4 proposed

The IRC4 proposed aims to provide a high level of randomness and complexity to bypass RC4 vulnerabilities by introducing improved RC4 key generation by entering the private ID number of each sensor node into KSA and PRGA algorithms and considering the output as a new key that is added with the encryption key by combining them using XOR function And use the output as the key for the encryption process as shown in Figure 2.

The encryption process of the proposed method includes, first, this process starts by entering the sensor ID as a key into the algorithms of Saudi Arabia and PRGA and using the output as a new key with a length of less than or equal to 16 bytes provided To be equal to the original key in terms of length. Second, combine the new key with the original key by using XOR to produce a new key of the same length. Finally, the XOR function is executed between the new key and the plaintext to get the cipher text.

Table 2. Statistical Test Suite

Statistical Tests	RC4	IRC4
Frequency Test	0.5959	0.8597
Binary Derivative D1	0.0624	0.4245
Binary Derivative D2	0.0325	0.2123
Change Point	0.2069	0.5069
Sub-block Test	0.0162	0.0780
Runs Test	0.5627	0.3112
Sequence Complexity	19	20
Linear Complexity	0.1659	0.5000

3.2 Performance analysis of IRC4

Several statistical tests are also available to evaluate the randomness features of cryptographic algorithms. The statistical analysis is evaluated using CRYPTX'98 tests[26], which are popular seven statistical tests designed to check randomness Based on the significance value, the CRYPTX'98 tests determine whether the sequence ratio is random. When the P-value is greater than 0.01, the sequence is considered random or vice versa and is called a non-random sequence.

Test results will also be discussed below.

- **Frequency Test:** Passing this test is required for all subsequent tests [32]. In this test, the IRC4 method is generally superior to the RC4, as shown in Table 2. IRC4 increases nearly 0.2638 more than the RC4 algorithm, according to CRYPTX'98 tests.
- **Binary Derivative Test (D1):** In this test, the IRC4 is generally superior to the RC4, as shown in Table 2. IRC4 increases nearly 0.3621 more than the RC4, according to CRYPTX'98 tests.
- **Binary Derivative Test (D2):** In this test, the IRC4 is generally superior to the RC4, as shown in Table 2. IRC4 increases by nearly 0. 1798 more than the RC4, according to CRYPTX'98 tests.
- **Change Point Test:** In this test, IRC4 is generally superior to the RC4, as shown in Table 2. IRC4 increases by nearly 0. 3 more than the RC4algorithm, according to CRYPTX'98 tests.
- **Sub-block Test:** In this test, IRC4 is generally superior to the RC4, as shown in Table 2. IRC4 increases nearly

0.0618 more than the RC4, according to CRYPTX'98 tests.

- **Runs Test:** In this test, RC4 is generally superior to IRC4, as shown in Table 2. RC4 increases nearly 0.2515 more than the IRC4, according to CRYPTX'98 tests.
- **Sequence Complexity Test:** IRC4 is generally superior to the RC4, as shown in Table 2. IRC4 increases nearly 1 more than the RC4, according to CRYPTX'98 tests.
- **Linear Complexity Test:** IRC4 is generally superior to the RC4, as shown in Table 2. IRC4 increases nearly 0.3341 more than the RC4, according to CRYPTX'98 tests.

4 Bacterial Foraging Optimization Routing Protocol (BFORP) for WSNs

4.1 Network model

In this model, the topology of WSN is built as only a G-directed diagram (N, A). The nodes have represented by N, and the collection of direct linkages between the nodes is represented by A. The sink is accountable for gathering data from all nodes located in its range of transmission [2]. The sink counts the entries in the routing table. The optimum routing table is calculated and broadcast. Each node has this table. Using this table, the process's best path for broadcast in the network is determined every time the data is sent from the node to the sink in each round. As a result, the routing technology used defines the routing path for the sensor node with the data to be sent to the sink.

4.2 BFORP proposed

In this subsection, we describe a Routing protocol for bacterial forage optimization (BFORP) as protocol energy-efficient which increases the lifespan of a WSN by limiting energy costs and ensuring that energy consumption is evenly distributed.

a. BFORP chooses the best path from the source node to the sink based on three routing factors. The maximum "residual power (RE)", the "minimum number of hops (MH)" to the sink, and the least "traffic load (TL)" are the node criteria.

b. The method used determines the optimal channel for transmitting data from the transmitter sensor to the sink based on the three criteria (MH, TL, and RE), then the specified path is used for routing in subsequent transmission procedure rounds, after each round, the status of each node running in that path is checked To see if the same path should be used for the next round.

c. The information in the base station relates to the current status of each node, including location coordinates, traffic load, and battery power.

1.) Knowing the coordinates (x, y) of each node in the network, the distance (d) between each node (n) and the sink can be calculated as follows:

$$d\,(n) \;=\; \sqrt{(x_s - x_n)^2 + (y_s - y_n)^2} \qquad (1)$$

The values (xs, ys) and (xn, yn) represent coordinates (x, y) for the sensor nodes n & the sink s.

2.) The value of fitness of the contiguous node (n) is obtained by using the (2):

$$(n)=\alpha*RE(n)+\beta*1/TL(n)+\gamma*1/d(n) \qquad (2)$$

The RE (n) represents the remaining energy of sensor node n; As for TL(n) it represents the current traffic load for sensor node n; and the integer coefficients (α, β, and γ) are defined by the user to controlling each variable's effectiveness (metric).

d. *BBC* then assesses the information collected from all nodes neighboring to the bacteria cell *BC* node and chooses the optimal node with the greatest probability P concerning probability provided by:

$P\ (ni)\ =$(3)

$$\frac{fitness\ (ni)}{\sum_J^N fitness\ (nj)}$$

The P (si) is representing the probability value of the sensor node (ni), the fitness value of the sensor node (ni) is the fitness (si), and N is the number of the neighbor nodes.

e. When a group of nodes is found during the same expansion process, they are successors and substitutes for the extended node. They are the extension node successors and each other's replacements. The packing pointer is assigned to the expanded node for each node identified throughout the extension procedure.

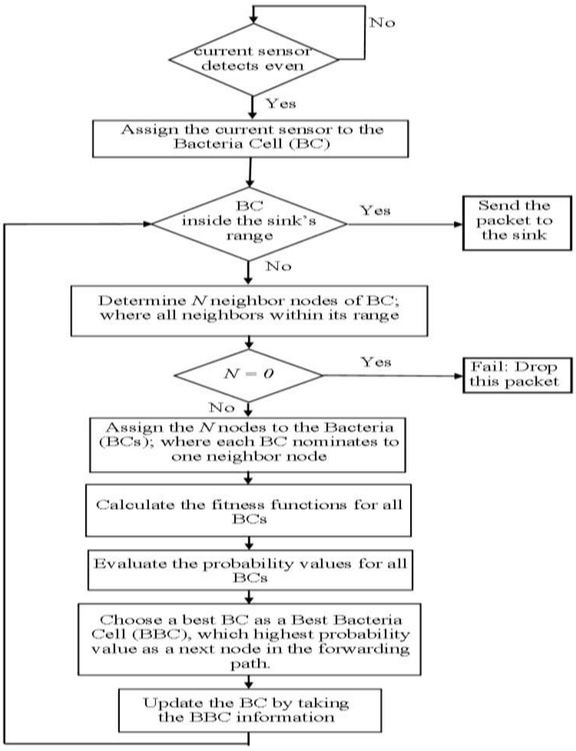
No
Current sensor detects even
Yes
Assign the current sensor to the Bacteria Cell (BC)
BC inside the sink's range
Yes
Send the packet to the sink
No
Determine N neighbor nodes of BC; where all neighbors within its range
N = 0
Yes
Fail: Drop this packet
No
Assign the N nodes to the Bacteria (BCs); where each BC nominates to one neighbor node
Calculate the fitness functions for all BCs
Evaluate the probability values for all BCs
Choose a best BC as a Best Bacteria Cell (BBC), which highest probability value as a next node in the forwarding path.
Update the BC by taking the BBC information

Figure 3: BFORP for WSNs

f. All of the steps from 1 to 4 are renewed until the sink is found, at which point all packets are transmitted to the sink by using the best path.

Figure 3 shows the flowchart of BFORP for WSN.

4.3 Performance results of BFORP

In respect of evaluating the performance of the BFORP maximizing network lifetime and balancing energy consumption, compared the recommended simulation results to the results of both known techniques, namely PEGASIS [27] and LEACH [28], all methods use the routing metrics namely, the residual energy, the shortest hop, and the traffic load to obtain a better pathway from the source node to the sink. A MATLAB program is utilized to carry out the system simulation processes. MATLAB is used to carry out the simulations. A hundred nodes are spread out in a topographical space with the (100 m100 m) dimension. The placement of sensor nodes is done at random. The perceived transmission is limited in the topographical area (20 m). This type of topographical area is used to test the performance of all approaches. A sink of data is placed at (90 m, 90 m). The beginning energy for all sensor nodes in the network is (0.5 J).In all methods, the first-order radio model is employed, which is widely used in the routing protocol assessment area in WSNs[28], In all techniques. In the model used in this work Receiving and transmission costs are defined by the formulas EnT(k)=Eelec•k+Eamp•k.d2 and EnR(k)=Eelec•k, respectively. K represents the amount of bit for each packet, the distance between the senders and receiver's nodes is represented by d, and Eelec and Eamp are bitting energy dissipation in receiving or sensing circuitry, and the energy required for each bit each square meter for the amplifier to achieve a sensible signal to noise ratio (SNR), respectively. Table 3 shows the parameters of the system in detail.

Figure 4 shows the number of live nodes for each round of sending using three distinct ways. The proposed BFORP preserves more nodes live than LEACH and PEGASIS techniques after the same amount of packets are transferred. When all 2000 packets are transmitted within the area, the suggested technique achieves a network lifetime that is almost nearly 60% higher than LEACH and higher than PEGASIS by nearly 50%. Additionally, Table 4 shows the difference in time associated with the first dead sensor node computed using three techniques distinguished in Table 4.

Since the number of delivered packets increases, the suggested technique In terms of values produces higher average energy residual than LEACH and PEGASIS techniques. The proposed way produces the best energy balance in a WSN, as shown in Figure 5. The delay induced by sending a packet of data is an essential factor.

Table 3. Simulation Parameters

Parameter	Value
Topographical Area (meters)	100 m × 100 m
Sink location (meters)	(90, 90)
Number of nodes	100
Limit of transmission distance (meters)	20 m
The initial energy of the node	0.5 J
Eelec	50 nJ/bit
Eamp	100 pJ/bit/m2
Packet	data size 2k bit
Number of transmission packets	2 x 103
Maximum traffics in node's queue	10

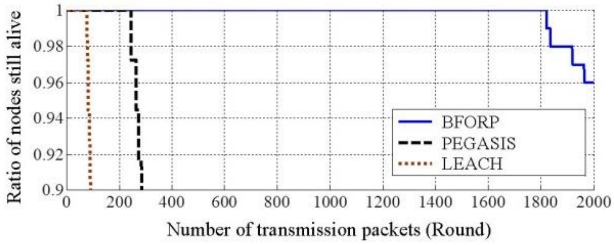

Figure 4: The sensor ratio is still alive in all methods

Table 4. First dead sensor based on all approaches

Approaches	LEACH	PEGASIS	BFORP	
The lifetime of the first Dead sensor (Rounds)	78	246	1820	

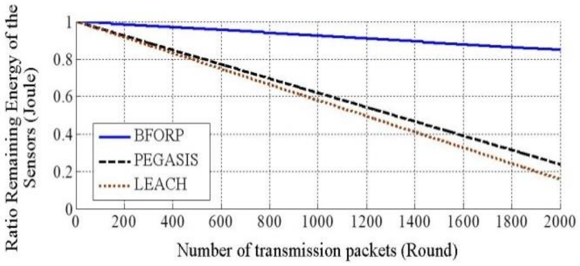

Figure 5: The ratio of residual power of nodes in each method

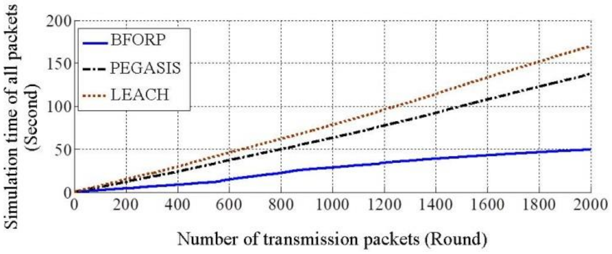

Figure 6: The time of Simulation in all methods

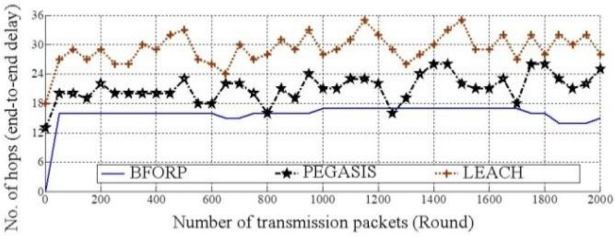

Figure 7: The delay of End-to-end in all methods

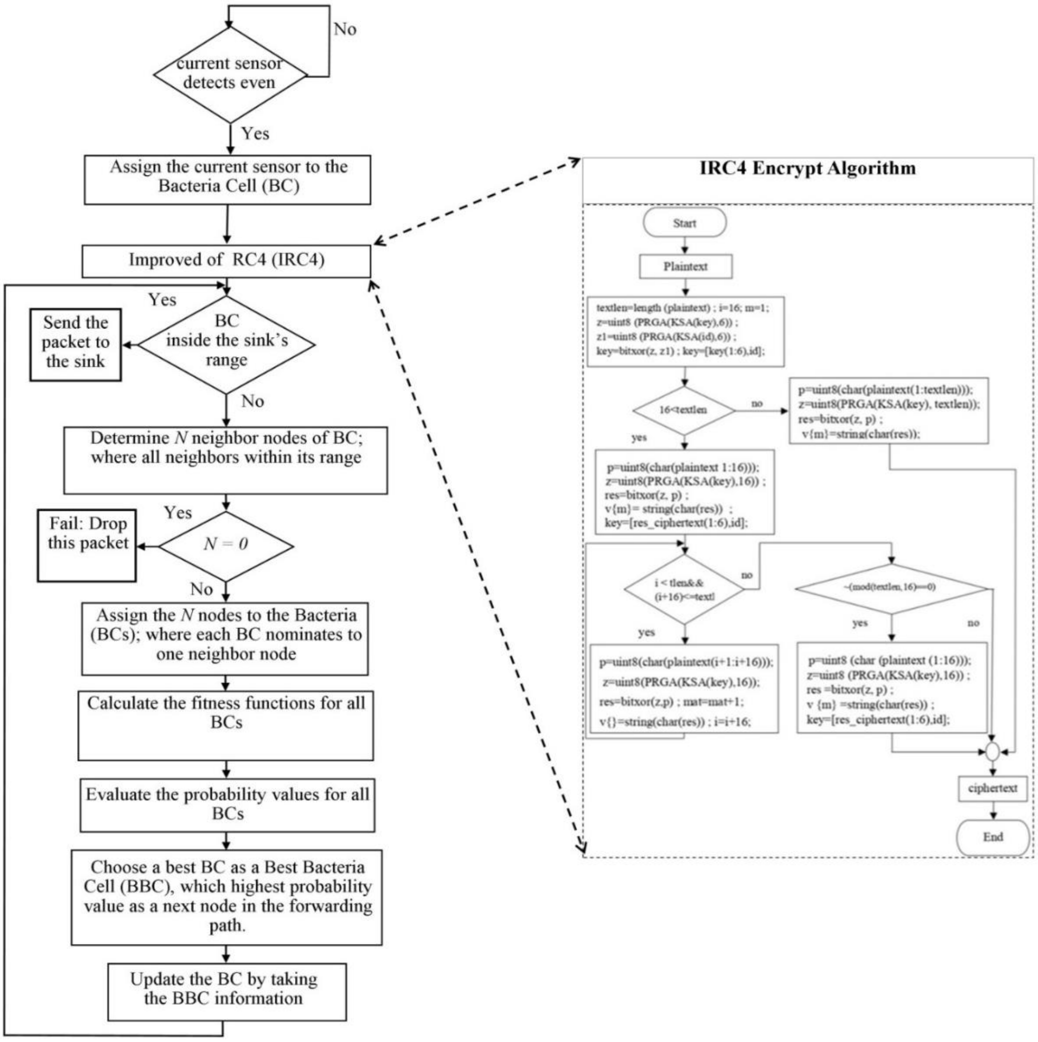
No
current sensor detects even
Yes
Assign the current sensor to the Bacteria Cell (BC)
Improved of RC4 (IRC4)
Yes
Send the packet to the sink
BC inside the sink's range
No
Determine N neighbor nodes of BC; where all neighbors within its range
Yes
Fail: Drop this packet
N = 0
No
Assign the N nodes to the Bacteria (BCs); where each BC nominates to one neighbor node
Calculate the fitness functions for all BCs
Evaluate the probability values for all BCs
Choose a best BC as a Best Bacteria Cell (BBC), which highest probability value as a next node in the forwarding path.
Update the BC by taking the BBC information
IRC4 Encrypt Algorithm
Start
Plaintext
textlen=length (plaintext) ; i=16; m=1;
z=uint8 (PRGA(KSA(key),6)) ;
z1=uint8 (PRGA(KSA(id),6)) ;
key=bitxor(z, z1) ; key=[key(1:6),id];
16<textlen
no
yes
p=uint8(char(plaintext(1:textlen)));
z=uint8(PRGA(KSA(key), textlen));
res=bitxor(z, p) ;
v{m}=string(char(res));
p=uint8(char(plaintext 1:16)));
z=uint8(PRGA(KSA(key),16)) ;
res=bitxor(z, p) ;
v{m}= string(char(res)) ;
key=[res_ciphertext(1:6),id];
i < tlen&&
(i+16)<=textl
no
yes
~(mod(textlen,16)==0)
yes
no
p=uint8(char(plaintext(i+1:i+16)));
z=uint8(PRGA(KSA(key),16));
res=bitxor(z,p) ; mat=mat+1;
v{}=string(char(res)) ; i=i+16;
p=uint8 (char (plaintext (1:16)));
z=uint8 (PRGA(KSA(key),16)) ;
res =bitxor(z, p) ;
v {m} =string(char(res)) ;
key=[res_ciphertext(1:6),id];
ciphertext
End

Figure 8: The flowchart of IRC4-BFORP for WSNs

Figure 6 compares the three ways. In addition, as demonstrated in Figure 7, the suggested BFORP has the smallest latency when compared to the other techniques. The reduced latency implies that the transmission is more effective and energy-efficient (particularly for important and protected information).

5 Routing protocol (IRC4-BFORP) for WSNs

In this section, a secure routing protocol (IRC4-BFORP) is proposed by combining the IRC4 with the BFORP protocol to create a new safe and energy-efficient protocol. IRC4-BFORP aims to ensure that the multi-hop routing of WSNs is not exposed to malicious attacks and to extend the network lifetime as much as possible by defining the optimal routing path for WSNs. Each node senses and segments the data to some of the segments that will be encrypted by the IRC4. Then, the encrypted segments will be reassembled and sent to the sink by the BFORP. The sink node collects and verifies messages, decrypting the entire information and data from the sensor domain.

5.1 IRC4-BFORP model

This subsection explains the IRC4-BFORP model work in the sensor node, which is to partition and encrypt the data and then collect it and send it to the sink node. The

data segmentation and encryption mechanism are summarized as, firstly the data packet is split into 16 parts, each part being 16 bytes (128 bits) long. Secondly, every piece of data is encrypted in IRC4, Finally assembled back to its original size to be sent. Figure 8 shows the flowchart of IRC4-BFORP for WSN.

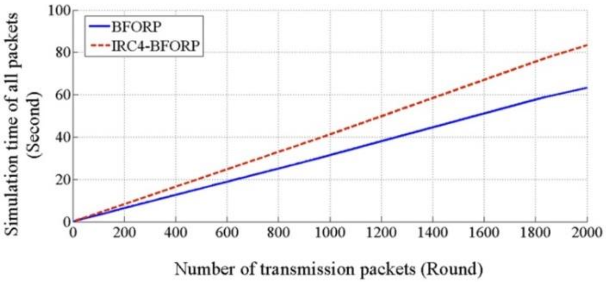

Figure 9: Processing Time BFORP with/without IRC4

5.2 Performance evaluation of IRC4-BFORP

To compare the performance of the IRC algorithm with and without the PFORP protocol, the results of IRC4-BFORP are the same as those of BFORP, except for the increase in the execution time in IRC4-BFORP, as shown in Figure 9. This is clear because the proposal uses packet encryption to protect it from hacking, and this requires additional time at the time of transmission. Therefore, in the proposed secure routing, we have obtained a secure routing of the data with a simple time addition that almost does not affect the network performance.

6 Conclusion

In WSNs, nodes have limited resources. Thus, it’s necessary to select techniques that perform the best use of available energy and data security. For performing the process transmission of data via a routing path that has been determined to be the best path to increase the network's total lifetime while minimizing the delay caused by the pathfinding process and securing the transmission of sensed data, in this paper, The IRC4 is used to secure the sensing data sensed by the sensors before sending it to the sink. Random cipher performance was tested using 7 cryptox'98 statistical tests, which were created to evaluate pseudo-random numbers of cryptographic applications and successfully bypass the randomness of the IRC4 algorithm, and a new protocol was proposed called Bacterial foraging optimization Routing Protocol (BFORP). The modern method is able of finding a path of optimal routing to be used in the transmission of data from the node of the source toward the sink. Comparing the suggested method with the other two methods, the results show that, performing the suggested method is much better than that of the two methods regarding the lifetime of the network and transmission delay. Then the proposed routing protocol (BFORP) was combined with the IRC4 optimization algorithm to obtain a safe and energy-saving routing protocol called (IRC4-BFORP). By comparing the new method with the (BFORP), the results showed that the implementation of the new method is identical, but there is difference a very small in time.

References

[1] I. S. Alshawi, L. Yan, W. Pan, and B. Luo, "Lifetime enhancement in wireless sensor networks using fuzzy approach and A-star algorithm," *IEEE Sensors Journal,* vol. 12, no. 10, pp. 3010-3018, 2012. https://doi.org/10.1109/JSEN.2012.2207950.

[2] A. S. Rostami, M. Badkoobe, F. Mohanna, A. A. R. Hosseinabadi, and A. K. Sangaiah, "Survey on clustering in heterogeneous and homogeneous wireless sensor networks," *The Journal of Supercomputing,* vol. 74, no. 1, pp. 277-323, 2018. https://doi.org/10.1007/s11227-017-2128-1

[3] I. Alshawi, L. Yan, W. Pan, and B. Luo, "Fuzzy chessboard clustering and artificial bee colony routing method for energy-efficient heterogeneous wireless sensor networks," *International Journal of Communication Systems,* vol. 27, no. 12, pp. 3581-3599, 2014. https://doi.org/10.1002/dac.2560.

[4] J. Zheng and A. Jamalipour, *Wireless sensor networks: a networking perspective*. John Wiley & Sons, 2009.

[5] C. N. Zhang and Q. Yu, "An RC4 based Light Weight Secure Protocol for Sensor Networks," in *Wireless and Optical Communications*, 2006.

[6] I. Mantin, "Analysis of the stream cipher RC4," *Master's Thesis, The Weizmann Institute of Science,* 2001.

[7] R. Venugopalan, P. Ganesan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis," in *Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems*, 2003, pp. 188-197. https://dl.acm.org/doi/10.1145/951710.951737

[8] M. D. Aljubaily and I. S. Alshawi, "Energy sink-holes avoidance method based on the fuzzy system in wireless sensor networks," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 12, no. 2, 2022. http://doi.org/10.11591/ijece.v12i2.

[9] U. Mahadevaswamy, "Energy efficient routing in wireless sensor network based on mobile sink guided by stochastic hill climbing," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 10, no. 6, 2020. http://doi.org/10.11591/ijece.v10i6.pp5965-5973

[10] M.-J. Tsai, H.-Y. Yang, and W.-Q. Huang, "Axis-based virtual coordinate assignment protocol and delivery-guaranteed routing protocol in wireless sensor networks," in *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, 2007: IEEE, pp. 2234-2242. https://doi.org/10.1109/INFCOM.2007.258.

[11] C. Wu, R. Yuan, and H. Zhou, "A novel load balanced and lifetime maximization routing protocol in wireless sensor networks," in *VTC Spring 2008-IEEE Vehicular Technology Conference*, 2008: IEEE, pp. 113-117. https://doi.org/10.1109/VETECS.2008.36.

[12] I. Daanoune, A. Baghdad, and A. Ballouk, "An enhanced energy-efficient routing protocol for wireless sensor network," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 10, no. 5, 2020. http://doi.org/10.11591/ijece.v10i5.pp5462-5469

[13] I. S. Alshawi and I. O. Alalewi, "Lifetime optimization in wireless sensor networks using FDstar-lite routing algorithm," *International Journal of Computer Science and Information Security,* vol. 14, no. 3, p. 46, 2016. https://dx.doi.org/10.6084/m9.figshare.3153868

[14] S. Savitha, S. Lingareddy, and S. Chitnis, "Energy efficient clustering and routing optimization model for maximizing lifetime of wireless sensor network," *International Journal of Electrical and Computer Engineering,* vol. 10, no. 5, p. 4798, 2020. http://doi.org/10.11591/ijece.v10i5.pp4798-4808.

[15] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, 2004, pp. 162-175. https://doi.org/10.1145/1031495.1031515.

[16] Z. Alliance, "Zigbee specification version 1.0," ed: April 2005.

[17] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 53, no. 6, pp. 1341-1352, 2006. https://doi.org/10.1109/TCSI.2006.874182.

[18] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in *2007 6th International Symposium on Information Processing in Sensor Networks*, 2007: IEEE, pp. 479-488. https://doi.org/10.1109/IPSN.2007.4379708.

[19] J. Liu, "One-way Hash function based on integer coupled tent maps and its performance analysis," *Journal of Computer Research and Development,* vol. 45, no. 3, p. 563, 2008. https://crad.ict.ac.cn/EN/Y2008/V45/I3/563.

[20] N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *International Journal of Computer Trends and Technology,* vol. 2, no. 6, pp. 177-181, 2011.

[21] T. Wang, X. Qin, and L. Liu, "An energy-efficient and scalable secure data aggregation for wireless sensor networks," *International Journal of Distributed Sensor Networks,* vol. 9, no. 12, p. 843485, 2013. http://dx.doi.org/10.1155/2013/843485.

[22] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Generation Computer Systems,* vol. 49, pp. 104-112, 2015. https://doi.org/10.1016/j.future.2014.10.010.

[23] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers & Electrical Engineering,* vol. 59, pp. 250-261, 2017. https://doi.org/10.1016/j.compeleceng.2016.01.002.

[24] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks," *IEEE Transactions on Engineering Management,* vol. 68, no. 1, pp. 170-182, 2019. https://doi.org/10.1109/TEM.2019.2953889.

[25] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and energy-aware heuristic routing protocol for wireless sensor network," *IEEE Access,* vol. 8, pp. 163962-163974, 2020. https://doi.org/10.1109/ACCESS.2020.3022285.

[26] E. Dawson, A. Clark, H. Gustafson, and L. May, "CRYPT-X'98,(Java Version) User Manual," *Queensland University of Technology,* 1999.

[27] S. Lindsey, C. Raghavendra, and K. M. Sivalingam, "Data gathering algorithms in sensor networks using energy metrics," *IEEE Transactions on parallel and distributed systems,* vol. 13, no. 9, pp. 924-935, 2002. https://doi.org/10.1109/TPDS.2002.1036066.

[28] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd annual Hawaii international conference on system sciences*, 2000: IEEE, p. 10 pp. vol. 2. https://doi.org/10.1109/HICSS.2000.926982.