Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 12, Number 1, Spring 2023, pp. 52-60
Received: 05/02/2021, Revised: 09/19/2023, Accepted: 10/13/2023

A multi-objective secure routing method for wireless sensor network

Seyed Meysam Namazi [1], Hamid Barati[2*], Ali Barati[3]
1- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
2- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
3- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
[1]meysam.namazi@gmail.com, [2*]hbarati@iaud.ac.ir, [3]abarati@iaud.ac.ir

Corresponding author's address: Hamid Barati, Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.

Abstract- The wireless sensor network is a wireless network of self-organized sensors that are distributed at intervals. These sensors are used to group measurements of specific physical quantities or environmental conditions such as temperature, sound, vibration, pressure, motion, or pollutants at various locations. Energy efficiency to extend a wireless sensor network's lifetime should be considered in all network design areas, including hardware and software. Wireless sensor networks may be used in critical applications and transmit sensitive data, so they need methods to secure the data. Secure routing in wireless sensor networks is vital due to the need for data confidentiality, integrity, energy efficiency, authentication, and resilience against attacks. It ensures sensitive data remains private, prevents tampering, optimizes energy usage, verifies node authenticity, and defends against attacks. This paper presents a secure routing method in wireless sensor networks. In the proposed method, due to the nodes' processing limitations and to ensure the security of the exchanged messages, the lightweight columnar transposition cipher method is used. The routing process is done hop by hop, and the next hop is selected based on the parameters of remaining energy, distance to the base station, and node traffic. The proposed routing method is implemented by MATLAB and compared with SMEER and KID-SASR methods. The simulation results show a reduction of end-to-end delay of 50% and 38%, reduction of energy consumption of 39% and 20%, reduction of packet loss rate, and increased number of live nodes by 66% and 59% compared to SMEER and KID-SASR.

Keywords- Wireless sensor network, Routing, Columnar transposition cipher, Security.

I. INTRODUCTION

Wireless sensor networks are an example of distributed systems [1]. In these networks, the sensors are placed in a wireless environment at specific or random distances from each other and work to detect events, collect data and environmental information and transfer them to a monitoring center [2-3]. The sensors are equipped with a processor and communication facilities. They have different types to measure some physical quantities or environmental conditions such as temperature, light, humidity, sound, motion, or pollutants [4-6]. Some of these large network applications include monitoring and controlling industrial processes, health system monitoring, environmental monitoring, companies monitoring, centers and homes monitoring, health care monitoring, smart homes monitoring, and traffic control [7-10]. Sensor nodes have limited computing power, communication range, and storage capacity [11]. These sensor nodes' limitations have made routing in the wireless sensor network a challenging task [12]. Due to their wireless structure, these networks are prone to many attacks [13]. One way to deal with attacks is to use secure routing protocols in the wireless sensor network [14].

Wireless sensor networks (WSNs) play a crucial role in various applications. However, due to their distributed nature and resource limitations, ensuring secure communication in WSNs remains a significant challenge. Existing research has addressed different dimensions of security in WSNs, but there is still a need for efficient and lightweight secure routing methods. This paper aims to fill this gap by proposing a secure routing method that focuses

on maintaining data confidentiality, improving packet delivery rate, and reducing energy consumption. By utilizing the columnar transposition cipher, a lightweight encryption technique, the proposed method minimizes the overhead on the network while providing adequate security. The motivation behind this research is to enhance the overall security and performance of WSNs, enabling their reliable and secure operation in various real-world applications.

This paper aims to provide a secure routing method in a wireless sensor network so that data confidentiality is maintained, packet delivery rate is increased, and the energy consumption is reduced. Data transmission in the proposed method is done hop by hop from the source to the base station. The columnar transposition cipher method is used hop by hop to the base station in the proposed method. The columnar transposition cipher is a lightweight cipher method that imposes a small overhead to the network compared to many other methods. Therefore, due to the limited resources of nodes in the wireless sensor network, it is suitable for providing security in these networks. The data is encrypted by the source node by columnar transposition cipher with a specified key and sent to the next node. Then, according to the proposed routing algorithm, the packets are sent to the base station hop by hop. In each hop, the node encrypts the received data using its key and then sends it to the next hop. The proposed method will achieve a secure routing method by applying an effective and efficient routing method and cipher mechanism.

The innovations of proposed method are as follows:

- This paper focused on decreasing end to end delay and energy consumption on nodes that are at a farther distance from the base station by using multi-objective hop by hop routing.
- Enhancing the stability and lifetime of the network by conserving the energy of sensor nodes.
- Secure data transmission by a lightweight hop-by-hop encryption method.
- Experiment results demonstrate that our method can decrease packet lost rate, energy consumption and end to end delay significantly and increase the number of alive node.

The rest of the paper is organized as follows. In section 2, we will review the routing methods in the wireless sensor network. Then, in section 3, the network model is provided. In section 4, the proposed method, a secure routing method in the wireless sensor network using cryptography, is described in detail. In section 5, the proposed model is compared and evaluated, and the results are described. Then in section 6, conclusions and suggestions for future work are provided.

II. RELATED WORKS

This section provides an overview of routing methods in the wireless sensor network.

Viswanathan and Kannan [16] proposed a new secure routing algorithm using key management based on an advanced form of elliptic cipher to increase communication security in wireless sensor networks. In this method, an encryption key is formed from the Beta and Gamma functions in elliptic key cryptography. Using these values increases security and creates an extra layer for calculating the key, which increases the strength of the key.

Isaac Sajan and Jasper [17] provided security during data transmission using the Secure Atom Search Routing (SASR) algorithm, adopted from molecular dynamics behavior. This algorithm provides an effective solution for global optimization problems based on atoms' constraint and interaction force. Also, SASR performance is improved by providing a proper balance between exploitation and exploration. The route in this method is selected based on the best route ever found.

Paho and Tchendji [18] proposed a hierarchical routing protocol with geocasting over a wireless sensor network. This protocol is a fast and secure clustering and geographic protocol. The hierarchical clustering protocol is set to create a layered virtual architecture and it's based on a three-dimensional architecture. This protocol uses radio power modulation techniques to be eco-energetic and reliable. It also uses elliptic curves as secret key generators in an asymmetric process that secures communications.

Fang et al. [19] proposed a clustering-based routing method in the wireless sensor network. In this method, a trust management scheme for maintaining security in wireless sensor networks is presented. This method is presented in two phases. The first phase of the Lightweight Trust Management Scheme (LTMS) is presented using binomial distribution and adopting cluster head's recommendations with low computational complexity mitigate to reduce internal attacks. Multidimensional Secure Cluster Routing (MSCR) based on the trust value from LTMS, the environment domain, distance domain, energy domain, and security domain is presented in the second phase.

Dhand and Tyagi [20] proposed a hybrid method of K-means clustering algorithm with Ant Lion Optimizer to grouping nodes and optimal cluster head selection for better energy efficiency. In this method, security topographies are provided using the elliptic curve cryptographic method. Routing is also done using a multi-route spherical network routing method. This protocol is used to improve secure routing in a multilayer network.

Mutalemwa and shin [21] suggested two phantom-based source location privacy routing (SLP) protocols. They called the two-level phantom with the chase ring (PhaP) and the two-level phantom with the backbone route (PhaT). PhaP and PhaT protocols can be considered as modified versions of probabilistic source location privacy protection protocol (ProbR) protocol [22] and tree-based diversionary routing (TreeR) protocol [23], respectively. These protocols' two main purposes are to provide strong SLP protection across the wireless sensor network range and control the communication overhead by removing the fake packet on

the network.

Mitra and Sharma [24] proposed a meeting-based routing protocol. In this protocol, a virtual cross-shaped area with width w is created in the network's middle. This intersection acts as a meeting point for sensor node communications. The nodes in the meeting area are called the backbone nodes. In this protocol, the source nodes can send data to the sink whenever needed. The source node retrieves the sink location from the nearest tree node and transmits the data directly to the base station using the sink location information.

Mukhtar et al. [25] proposed a region-based wireless sensor network routing method. This protocol aims to reduce energy consumption and increase network lifetime. In this method, the network is divided into two regions. In this method, a number of mobile nodes are considered as routing nodes that do not participate in the sensing function and only collect the data of nodes in region two and send them to the base station. These nodes move on a specific route in the network, collect data from the cluster head node and send it to the base station.

He et al. [26] proposed a tree-based routing protocol in the wireless sensor network. This method combines virtual potential energy with the local density of nodes and the sleep-wake mechanism. This method allows nodes to dynamically join or exit the network, enabling nodes to transmit data in the shortest route to the destination automatically. Also, a sleep-wake mechanism is designed to reduce network traffic and save energy.

A summary and comparison of the mentioned methods presents in Table I.

III. NETWORK MODEL

The sensor network is considered as a connected graph G (V, E). In graph G, V represents the vertices and |V| indicates the set of sensor nodes' size. E is the graph edge, which represents the set of wireless connections between network nodes. Links are symmetrical. Each sensor node is equipped with a wireless receiver and sender that can be used to communicate with sensor nodes in its transmission range. The distribution of nodes is random and uniform. Nodes are homogeneous, and each node has a unique attribute. Each node can act as a desk or router. The base station and the nodes are all static. The energy of the nodes is limited, and the nodes are not rechargeable. The base station is static, and its energy is unlimited. The network in the proposed method is considered flat. The nodes are connected to the base station in a multi-hop manner. All nodes are equipped with a global positioning sensor. The network model is shown in Figure (1).

TABLE I
SUMMARY AND COMPARISON OF RELATED WORKS

Reference	Approach	Advantages	Disadvantages
Viswanathan and Kannan [16]	A secure routing algorithm with a novel encryption scheme using the cyclic group based Elliptic curve cryptography	enhanced security, reduce the computational complexity	Less throughput and delivery rate
Isaac Sajan and Jasper [17]	A routing algorithm called KID-SASR for security against the vampire attack and providing the shortest path for packet transmission.	Minimum delay and energy consumption, high throughput and network lifetime	Low detection of attacks in the topology discovery and packet forwarding phase.
Paho and Tchendji [18]	A secure clustering and fast geocasting protocol for a three-dimensional, hierarchical, GPS-free and low-density WSN	Well supports scalability, low energy consumption	Not supports of mobility and fault tolerance
Fang et al. [19]	A multidimensional secure clustered routing (MSCR) scheme by using dynamic dimension weight in hierarchical WSNs.	Prolonging the network lifetime and balancing energy consumption	The cluster heads are finally selected randomly
Dhand and Tyagi [20]	A Secure Multi-Tier Energy Efficient Routing (SMEER) Protocol with a technique called Miscegenation of Ant Lion optimizer	achieve a high security and reliability in the wireless communication system	High computational overhead
Mutalemwa and shin [21]	A two-phase quadrant-based routing scheme to address the source location privacy problem	Provides longer safety period and stronger privacy	Low packet delivery ratio, High energy consumption, High delay
Mitra and Sharma [24]	An efficient virtual grid based hierarchical routing approach suitable for delay bound applications, which reduces the overall energy consumption for multi-hop data communication.	Guarantees higher throughput and better network lifetime	Falls into a local optimum
Mukhtar et al. [25]	A region-based mobile routing protocol for the enhancement of network lifetime in WSN	Energy conservation and lifetime increased	Selection of cluster heads are randomly, Low PDR in low rounds
He et al. [26]	A routing protocol that combines virtual potential energy with local density of nodes and sleep-wake-up mechanism	Balanced energy consumption, high network lifetime	Do not support dynamic network of WSNs.

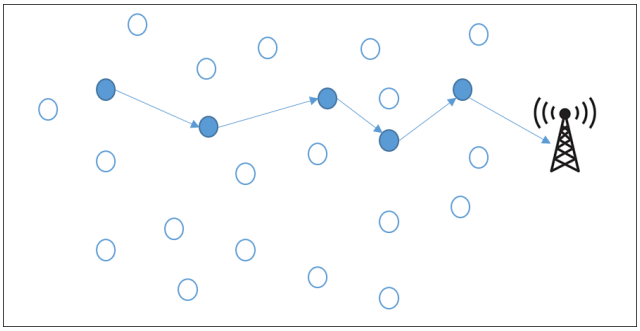

Fig1: Network model

IV. PROPOSED METHOD

The significant distance between the base station and the sensor nodes causes higher energy consumption for each node to transmit data to the base station. In the proposed method, routing operations are performed hop by hop to the base station between network nodes. Due to the nature of wireless communication in wireless sensor networks and these networks' sensitive applications, securing the exchanged messages is very important. In the proposed method, due to the nodes' processing limitations in the wireless sensor network, the lightweight columnar transposition cipher method is used. Details of each step of the proposed method are described below.

A. Routing

Routing between network nodes is based on the fitness function. The routing process is done hop by hop, and in each hop, the data is encrypted using columnar transposition cipher before sending to the next hop. During the route discovery process, the source node calculates a score for its neighbor nodes using parameters of remaining energy, distance to the base station, and node traffic. Neighbor nodes with the highest score will participate in the process of forming the route between the source node and the base station. Each node maintains a table to record the information of its neighbor nodes. The table of neighbor nodes is shown in Table II. This table contains the neighbor node ID, location, remaining energy, normal distance to the base station, normal energy, and normal traffic.

TABLE II
NEIGHBOR NODES

ID	remaining energy	location	normal distance to the BS	normal energy	normal traffic

The source node sends a "Hello" message to its neighbor nodes to select the next hop.

Neighbor nodes send the Replay packet to the source node after receiving the "Hello" message. The Replay packet is shown in Figure (2). This packet contains the node ID, remaining energy, node location, and the number of packets in the node buffer.

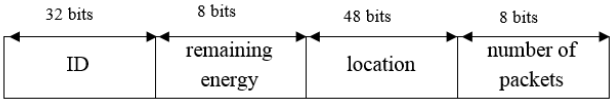

Fig2: Replay packet

After receiving the Replay packet, the source node performs the following operations.

- Calculating the energy ratio of neighbor nodes: Considering that energy is an essential and effective parameter in the routing process in wireless sensor networks, this parameter has been considered in choosing the next hop. Neighbor nodes with more energy are more suitable for sending data to get higher selection scores as the next hop. Since the next hop is selected based on the fitness function, the remaining energy in the range 0 to 1 is normalized according to Equation (1). Normalization causes correct and logical results by combining different parameters.

$$E_{Norm} = \frac{E_{current}}{E_{max}} \quad (1)$$

Where $E_{current}$ is the current energy of the neighbor node, E_{Max} is the initial energy of the network nodes and E_{Norm} is the normalized energy ratio.

- Calculating the neighbor node's distance to the base station: Network nodes are aware of the base station's location and can calculate their neighbors' distance to the base station based on the information stored in the neighbors' table. The source node calculates the distance from neighbor nodes to the base station according to Equation (2) and stores them in the neighbors' table.

$$D_{i\_BS} = \sqrt{(x_i - x_{BS})^2 + (y_i - y_{BS})^2} \quad (2)$$

Where (x_i, y_i) are the coordinates of the neighbor node i, (x_{BS}, y_{BS}) are the coordinates of the base station and D_{i_BS} is the distance of the neighbor node i to the base station.
The distance to the base station parameter is normalized according to Equation (3).

$$D_{Norm} = \frac{D_{i\_BS}}{L} \quad (3)$$

Where D_{i_BS} is the distance of the neighbor node to the base station, L is the size of the network diameter, which is equal to the maximum distance of a node to the base station, and D_{Norm} is the normalized distance, which is in the range 0 and 1. Neighbor nodes that are closer to the base station are more suitable for sending data. As a result, these nodes are more privileged and participate in the route formation process.

- Calculating the traffic in each neighbor node: The source node can estimate the amount of traffic in the neighbor nodes based on the number of data packets in the buffer of neighbor nodes. In the route formation process, it is better to use nodes with less traffic to avoid network congestion, data packet delivery delays, and data packet loss. As a result, nodes with less traffic have a higher priority for selection as the next hop. Equation (4) is used to normalize node traffic.

$$C_{Norm} = \frac{N_{current}}{BufferSize} \quad (4)$$

Where $N_{current}$ is the number of packets in the neighbor node buffer, $BufferSize$ is the size of the node buffer, which represents the maximum buffer capacity of the neighbor node. C_{Norm} is the normalized traffic of the neighbor node and is in the range 0 to 1.

- Calculating each node's score: In this step, the source node calculates its neighbor nodes' score. A node with more remaining energy, less distance to the base station, and less traffic will be a more desirable node to choose as the next hop. Therefore, the score of each node is calculated according to Equation (5).

$$Fitness_i = E_{Norm} + (1 - D_{Norm}) + (1 - C_{Norm}) \quad (5)$$

Where E_{Norm} is the normalized remaining energy of the neighbor node, D_{Norm} is the normalized distance of the neighbor node to the base station and C_{Norm} is the normalized traffic of the neighbor node. $Fitness_i$ specifies the score of the neighbor node i.

- Sending scores: After calculating the score, the source nodes will use the neighbor node with the highest score to send data packets to the base station. The source node encrypts the data before sending data packets to the neighbor node and then sends it to the next hop node. The steps of packet encryption are described in the next section.

B. Encryption and decryption of messages

After selecting the next hop to send the data, in this step, before sending the data, the source node encrypts the data using the columnar transposition cipher method with a specified key and sends it to the next node. In columnar transposition cipher, each node has a cryptographic key and a column read order. The base station randomly selects the cryptographic key for each node in the range of natural numbers 3 to 5. It is placed in the node memory before the nodes are distributed in the environment. The column read order is also randomly determined by the base station based on each node's cryptographic key and placed in the nodes' memory. The base station maintains a table to store the node ID and the cryptographic key of the columnar transposition associated with each node, as shown in Table III.

TABLE III
NETWORK NODES INFORMATION

ID	Key(number of columns)	Column order

The base station decrypts the data, and the network nodes do not know the encrypted data and the cryptographic key of the other nodes. The purpose of using different keys to encrypt in this route is that if one key is leaked, the whole route's security will not be compromised. So, the original data will not be revealed because several encryption steps are performed from the source node to the base station. The steps of encryption in the proposed method are as follows:

- After selecting the next hop node, the source node encrypts the data with the columnar transposition cipher method, and its key. Then sends encrypted data the to the next hop node. In this cipher method, the key is the number of columns and the column read order placed in the node memory.
- The source node first forms a table according to its key size to encrypt the data. The number of columns in the table equals the node key. The data is placed in a row in the formed table.
- In the columnar transposition cipher method, the data is written in a row and read as a column. The reading order indicates the order in which the data is read from the columns.
- After sorting the data in the columnar transposition table, the source node reads the data based on the reading order, and the original data is encrypted. The source node then sends the data to the next hop.
- After the data is received from the other node, the intermediate nodes encrypt the received encrypted data with their cryptographic key and send it to the next hop.
- Thus, in the proposed method, the data are encrypted in several steps according to the number of hops from the source to the destination.

Algorithm 1 shows the pseudo-code of the proposed method.

Algorithm 1: The pseudo-code of the proposed method

```
Initialization: (k: number of neighbor nodes, N: number of neighbor nodes)
for (i = 1; i <= N ; i++) do
   Base station randomly selects the cryptographic key and the column read order for node i
   Base station placed these keys in the memory of node i
End for
The base station maintains a network nodes information table to store the node ID and the cryptographic key
The source node sends a "Hello" message to its neighbor nodes
for (i = 1; i <= k ; i++) do
   Neighbor node i send the Replay packet to the source node
```

```
end for
while (data packet does not reach the base station)
   for (i = 1; i <= k ; i++) do
      Source node calculating the energy ratio of neighbor node i
      Source node calculating the neighbor node i's distance to the
         base station
      Source node calculating the traffic in neighbor node i
      Source node calculating node i's score
   end for
   Source node select the neighbor node with the highest score
   Source node encrypts the data with the columnar
      transposition cipher method
   Source node sends the data packet to the selected node
   The selected node is considered the source node.
end while
Base station extracts the node keys from the network nodes
information table.
The base station performs the decoding from the last hop to the
first hop.
```

An example of cryptography in the proposed method is shown below. For example, it is assumed that in a network based on Figure (3), node 5 intends to send a message with the content "*It is an emergency situation*" to the base station. The message route is shown in Figure (3).

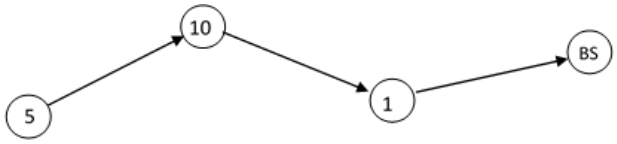

Fig3: The transmission path between node 5 and the BS

The properties of the nodes and their cryptographic keys are shown in Table IV.

TABLE IV
NETWORK NODES INFORMATION IN FIG 3

ID	Key(number of columns)	Column order
1	3	213
5	5	51243
10	4	1324

The following is a complete description of the encryption method using the node data.

Node 5 is the source node, and the plain text that intends to send is as follows:

IT IS AN EMERGENCY SITUATION

Node 5 forms a five-column table based on Table V to encrypt plain text, and the message text is placed in this table. The * parameter is used to indicate cells that contain spaces between words, and the empty columns of the last row are filled with asterisks.

TABLE V
KEY TABLE OF NODE 5

1	2	3	4	5
I	T	*	I	S
*	A	N	*	E
M	E	R	G	E
N	C	Y	*	S
I	T	U	A	T
I	O	N	*	*

In Table V, the plain text is written in a row in the form of five columns. Then the message is read as a column based on the reading order 51243. The text encrypted with the node 5 key will be as follows.

SEEST*I*MNIITAECTOI*G*A**NRYUN

The encrypted text is then sent to the node with ID 10.

Node 10 considers the message "*SEEST*I*MNIITAECTOI*G*A**NRYUN*" as a plain message, so it forms a four-column table based on its key. According to Table VI, it puts its plain text in the same way as node 5 in the code table.

TABLE VI
KEY TABLE OF NODE 10

1	2	3	4
S	E	E	S
T	*	I	*
M	N	I	I
T	A	E	C
T	O	I	*
G	*	A	*
*	N	R	Y
U	N	*	*

In Table VI, the encrypted text received from node 5 is written in a row in the form of four columns. In order to encrypt the message, according to reading order 1324, the text of the message is read as a column. The text encrypted with the node 10 key will be as follows.

STMTTG*UEIIEIAR*E*NAO*NNS*IC**Y*

The encrypted text is then sent to the node with ID 1.

Node 1 considers the message "*STMTTG*UEIIEIAR*E*NAO*NNS*IC**Y**" as a plain text, so it forms a three-column table based on its key. According to Table VII, it puts its plain text in the code table in the same way as the previous nodes.

In Table VII, the encrypted text received from node 10 is written in a row in the form of three columns. In order to encrypt the message, the text of the message is read in columns according to the reading order 213. The text encrypted with the node 1 key will be as follows.

TTUIAEAN***ST*II*N*SCYMGEER*ONI**

The encrypted text is then sent to the base station.

TABLE VII
KEY TABLE OF NODE 1

1	2	3
S	T	M
T	T	G
*	U	E
I	I	E
I	A	R
*	E	*
N	A	O
*	N	N
S	*	I
C	*	*
Y	*	*

The base station decrypts the message hop by hop. It examines the hops taken by the message to decrypt the incoming message. The base station then extracts the node keys. Decryption starts using the cryptographic key of the last node traversed and continues to the first node. According to the reading order, messages are recorded in columns in the node cryptographic table and are read in rows. Then the next hop decryption is done, and these steps continue until the message is completely decrypted.

V. SIMULATION AND RESULTS

In this section, the proposed routing method is simulated to evaluate its performance. Then, the simulation results will be compared with two routing methods. The proposed routing method is implemented by MATLAB software. In order to simulate the proposed routing method, it is assumed that the size of the wireless sensor network is 1000 × 1000 square meters. Also, the number of sensor nodes in the network is between 100 and 200 nodes, which are randomly and uniformly distributed in the network area. The simulation time is 180 seconds. The simulation parameters are summarized in Table VIII. The performance of the proposed routing method is evaluated in terms of end-to-end delay, energy consumption, packet loss rate (PLR) and number of live nodes.

TABLE VIII
SIMULATION PARAMETERS

Parameters	Values
Network size	1000*1000 (m^2)
Number of sensor nodes	100-200
Mac protocol	IEEE 802.11b
Data packet size	1000(byte)
Initial energy of the sensor node	0.5 (j)
Simulation time	2000 (S)

In Figure (4), the proposed routing method's performance is finally compared with the other two routing methods in terms of end-to-end delay. It should be noted that the end-to-end delay is defined as the length of time that the source node starts the route discovery process until the destination node receives the first data packet. As shown in Figure (4), the proposed routing method has a lower delay and performs better than other routing methods. This happens for several reasons. First, in discovering the route between network nodes, routes with less traffic are selected to send data packets, which will reduce delay in the network. Second, nodes with more energy have a higher priority to participate in forming the route between the source node and the base station. Increasing the number of nodes in the network increases the end-to-end delay. Because it increases congestion and increases the possibility of packet loss in the network, but in the proposed routing method, increasing the number of nodes in the network has less effect on increasing the end-to-end delay. This is because, in the proposed routing method, nodes with less traffic participate in the process of forming the route between a node and the base station. As a result, the proposed routing method can manage the increase in network congestion. Therefore, the end-to-end delay in the proposed routing method is less than the other methods in increasing the number of nodes.

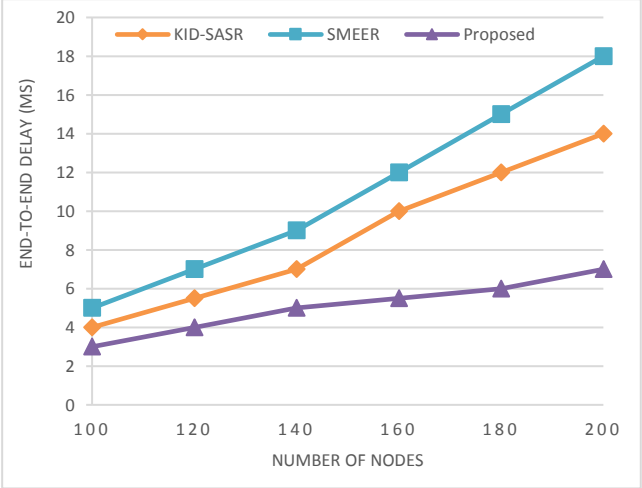

Fig. 4: End to end delay

Figure (5) shows the amount of energy consumed by sensor nodes in the process of sending data to the base station in different routing methods. As shown in Figure (5), the proposed routing method has the lowest energy consumption, which indicates an improvement in network lifetime. In the proposed method, the next hop is selected by considering the sensor nodes' remaining energy and the distance from the base station. As a result, energy is consumed in a balanced way, and nodes use less energy to send data to the base station.

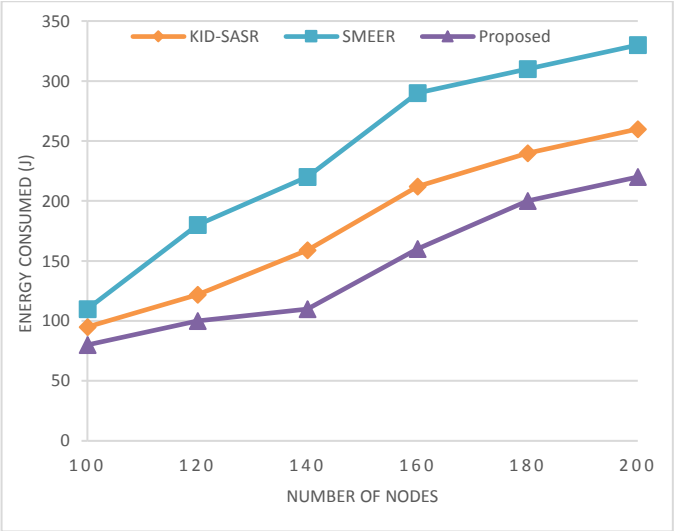

Fig. 5: Energy consumed

Packet loss rate means the ratio of total packets lost to total packets produced. In Figure 6, the performance of different routing methods is compared in terms of packet loss rate. As shown in Figure (6), the proposed routing method has a low packet loss rate due to the choice of routes with less traffic. Also, in the proposed routing method, the packet loss rate will increase slowly by increasing the number of sensor nodes in the network. This indicates the proper performance of the proposed method for networks of different sizes. As a result, the proposed routing method is scalable.

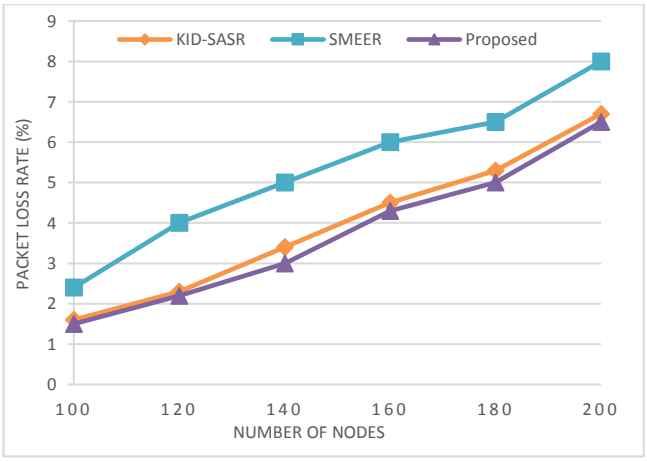

Fig. 6: Comparison of packet loss rate

A network with 200 sensor nodes is considered to evaluate network lifetime in different routing methods. Over time, the energy of some of the sensor nodes runs out and dies. Figure (7) shows the rate of decrease in the number of live sensor nodes based on time in different routing methods. As shown in Figure (7), the proposed routing method can adequately extend the network lifetime. In the proposed routing method, the time length until the death of the first node in the network is much better than other routing methods. This indicates that the proposed routing method can balance the energy consumption in the network in a desirable way; because the energy of the nodes in the routing processes in the network has been considered.

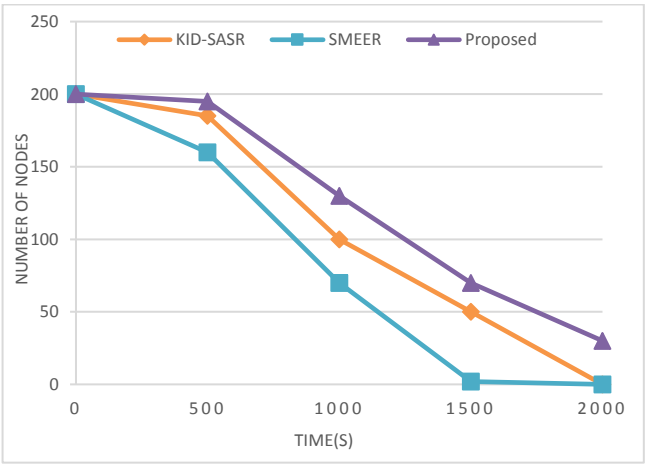

Fig. 7: Number of alive node

VI. CONCLUSION

In this paper, a routing method in the wireless sensor networks is presented. Also, due to the wireless communication in wireless sensor networks and their widespread applications, security is one of the key issues raised. Therefore, in the proposed method, an encryption method was used to secure the exchanged messages. In the proposed method, routing operations are performed hop by hop to the base station between the network nodes. Due to the nodes' processing limitations in the wireless sensor network, the columnar transposition cipher method is used. After selecting the next hop to send the data, in this step, before sending the data, the source node encrypts the data using the columnar transposition cipher method with a specified key and sends it to the next node. The proposed routing method is implemented by MATLAB software. The proposed routing method's performance was evaluated in terms of end-to-end delay, energy consumption, packet loss rate, and the number of live nodes.

REFERENCES

[1] BenSaleh, M. S., Saida, R., Kacem, Y. H., & Abid, M., "Wireless sensor network design methodologies: A survey", Journal of Sensors, pp. 1-13, 2020.

[2] Guillermo, J. C., García-Cedeño, A., Rivas-Lalaleo, D., Huerta, M., & Clotet, R., "Iot architecture based on wireless sensor network applied to agricultural monitoring: A case of study of cacao crops in ecuador". In Advances in Information and Communication Technologies for Adapting Agriculture to Climate Change II: Proceedings of the 2nd International Conference of ICT for Adapting Agriculture to Climate Change (AACC'18), pp. 21-23, 2018.

[3] Jabbar, S., Asif Habib, M., Minhas, A. A., Ahmad, M., Ashraf, R., Khalid, S., & Han, K., "Analysis of factors affecting energy aware routing in wireless sensor network", Wireless Communications and Mobile Computing, pp. 1-21, 2018.

[4] Karray, F., Jmal, M. W., Garcia-Ortiz, A., Abid, M., & Obeid, A. M., "A comprehensive survey on wireless sensor node hardware platforms", *Computer Networks*, Vol.144, pp. 89-110, 2018.

[5] Kumar, A., Zhao, M., Wong, K. J., Guan, Y. L., & Chong, P. H. J., "A comprehensive study of IoT and WSN MAC protocols: Research issues, challenges and opportunities", IEEE Access, Vol.6, pp. 76228-76262, 2018.

[6] Mihai, V., Dragana, C., Stamatescu, G., Popescu, D., & Ichim, L., "Wireless sensor network architecture based on fog computing". In 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), pp. 743-747, 2018.

[7] Verma, G., & Sharma, V., "A novel thermoelectric energy harvester for wireless sensor network application", IEEE Transactions on Industrial Electronics, Vol.66, No.5, pp. 3530-3538, 2018.
[8] Mohamed, R. E., Saleh, A. I., Abdelrazzak, M., & Samra, A. S., "Survey on wireless sensor network applications and energy efficient routing protocols", Wireless Personal Communications, Vol.101, pp. 1019-1055, 2018.
[9] Parween, S., & Hussain, S. Z., "A review on cross-layer design approach in WSN by different techniques", Adv. Sci. Technol. Eng. Syst, Vol.5, No.4, pp. 741-754, 2020.
[10] Samara, G., Besani, G. A., Alauthman, M., & Khaldy, M. A., "Energy-efficiency routing algorithms in wireless sensor networks: A survey" arXiv preprint arXiv: 2002.07178, 2020.
[11] Shinghal, D. K., & Srivastava, N., "Wireless sensor networks in agriculture: for potato farming", Available at SSRN 3041375, 2017.
[12] Singh, R., & Verma, A. K., "Efficient image transfer over WSN using cross layer architecture", Optik, Vol.130, pp. 499-504, 2017.
[13] Tharakan, L. A., Dhanasekaran, R., & Suresh, A., "Data Security in WSN-Based Internet of Things Architecture Using LDS Algorithm: WSN Architecture With Energy-Efficient Communication", In Edge Computing and Computational Intelligence Paradigms for the IoT pp. 170-195, 2019
[14] Bhasin, V., Kumar, S., Saxena, P. C., & Katti, C. P., "Security architectures in wireless sensor network", International Journal of Information Technology, Vol.12, No.1, pp. 261-272, 2020.
[15] Yu, J. Y., Lee, E., Oh, S. R., Seo, Y. D., & Kim, Y. G., "A survey on security requirements for WSNs: focusing on the characteristics related to security", IEEE Access, Vol.8, pp. 45304-45324, 2020.
[16] Viswanathan, S., & Kannan, A., "Elliptic key cryptography with Beta Gamma functions for secure routing in wireless sensor networks", Wireless Networks, Vol.25, pp. 4903-4914, 2019.
[17] Isaac Sajan, R., & Jasper, J., "Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network", International Journal of Communication Systems, Vol.33, No.8, pp. e4341, 2020.
[18] Paho, B. N., & Tchendji, V. K., "Secure and energy-efficient geocasting protocol for gps-free hierarchical wireless sensor networks with obstacles", International Journal of Wireless Information Networks, Vol.27, No.1, pp. 60-76, 2020.
[19] Fang, W., Zhang, W., Chen, W., Liu, J., Ni, Y., & Yang, Y., "MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, pp. 1-20, 2021.
[20] Dhand, G., & Tyagi, S. S., "SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks", Wireless Personal Communications, Vol.105, pp. 17-35, 2019.
[21] Mutalemwa, L. C., & Shin, S., "Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing", Sensors, Vol.19, No.5, pp. 1037, 2019.
[22] Mutalemwa, L. C., & Shin, S., "Routing schemes for source location privacy in wireless sensor networks: A survey", Journal of the Korean Society of Communication Studies, Vol.43, No.9, pp.1429-1445, 2018.
[23] Bradbury, M., Jhumka, A., & Leeke, M., "Hybrid online protocols for source location privacy in wireless sensor networks', Journal of Parallel and Distributed Computing, Vol.115, pp. 67-81, 2018.
[24] Mitra, R., & Sharma, S., "Proactive data routing using controlled mobility of a mobile sink in wireless sensor networks", Computers & Electrical Engineering, Vol.70, pp. 21-36, 2018.
[25] Mukhtar, M. F., Shiraz, M., Shaheen, Q., Ahsan, K., Akhtar, R., & Changda, W., "Rbm: Region-based mobile routing protocol for wireless sensor networks", Wireless Communications and Mobile Computing, pp. 1-11, 2021.
[26] He, Q., Mou, J., & Lin, B., "A robust self-organizing tree-based routing protocol for wireless sensor networks", Mathematical Problems in Engineering, pp.1-13, 2021.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۲، شماره ۱، بهار ۱۴۰۲، صفحه ۵۲-۶۰
دریافت: ۱۴۰۰/۰۲/۱۲، بازنگری: ۱۴۰۲/۰۶/۲۸، پذیرش: ۱۴۰۲/۰۷/۲۱

یک روش مسیریابی امن چند هدفه برای شبکه حسگر بی‌سیم

سید میثم نمازی[۱]، حمید براتی[۲*]، علی براتی[۳]
۱- گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
۲- گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
۳- گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
[1]meysam.namazi@gmail.com ،[2*]hbarati@iaud.ac.ir ،[3]abarati@iaud.ac.ir

آدرس نویسنده مسئول: حمید براتی، گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.

چکیده- شبکه حسگر بی‌سیم یک شبکه بی‌سیم از حسگرهای خودسازماندهی است که در فواصل زمانی مختلف توزیع می‌شوند. این حسگرها برای اندازه‌گیری‌های کمیت‌های فیزیکی خاص یا شرایط محیطی مانند دما، صدا، ارتعاش، فشار، حرکت یا آلاینده‌ها در مکان‌های مختلف استفاده می‌شوند. بهره وری انرژی برای افزایش طول عمر یک شبکه حسگر بی‌سیم باید در تمام زمینه های طراحی شبکه از جمله سخت افزار و نرم افزار در نظر گرفته شود. شبکه‌های حسگر بی‌سیم ممکن است در برنامه‌های کاربردی حیاتی استفاده شوند و داده‌های حساس را انتقال دهند، بنابراین به روش‌هایی برای ایمن کردن داده‌ها نیاز دارند. مسیریابی ایمن در شبکه های حسگر بی سیم به دلیل نیاز به محرمانه بودن داده ها، یکپارچگی، بهره وری انرژی، احراز هویت و انعطاف پذیری در برابر حملات حیاتی است. این تضمین می‌کند که داده‌های حساس خصوصی باقی می‌مانند، از دستکاری جلوگیری می‌کند، مصرف انرژی را بهینه می‌کند، صحت گره را تأیید می‌کند و در برابر حملات مقاومت می‌کند. در این مقاله یک روش مسیریابی ایمن را در شبکه‌های حسگر بی‌سیم ارائه می‌شود. در روش پیشنهادی، با توجه به محدودیت‌های پردازش گره‌ها و برای اطمینان از امنیت پیام‌های رد و بدل شده، از روش رمزنگاری انتقال ستونی سبک وزن استفاده می‌شود. فرآیند مسیریابی به صورت گام به گام انجام می‌شود و گام بعدی بر اساس پارامترهای انرژی باقیمانده، فاصله تا ایستگاه پایه و ترافیک گره انتخاب می‌شود. روش مسیریابی پیشنهادی توسط متلب پیاده سازی شده و با روش های SMEER و KID-SASRمقایسه شده است. نتایج شبیه‌سازی نشان دهنده کاهش تاخیر انتها به انتها به میزان ۵۰ و ۳۸ درصد، کاهش مصرف انرژی به میزان ۳۹ و ۲۰ درصد، کاهش نرخ تلفات بسته و افزایش تعداد گره های زنده به میزان ۶۶ و ۵۹ درصد در مقایسه با روش‌های SMEERو KID-SASR است.

واژه‌های کلیدی- شبکه حسگر بی‌سیم، مسیریابی، رمز انتقال ستونی، امنیت.