International Journal of Engineering

Journal Homepage: www.ije.ir

A Secure Routing Algorithm for Underwater Wireless Sensor Networks

M. Ahmadi[a], S. M. Jameii*[b]

[a] Department of Computer Engineering, Karaj Branch, Islamic Azad University, Karaj, Iran
[b] Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran

PAPER INFO

Paper history:
Received 11 February 2018
Received in revised form 28 April 2018
Accepted 17 August 2018

Keywords:
Underwater Wireless Sensor Networks
Security
Routing
Wormhole and Sybil Attack

ABSTRACT

Recently, underwater Wireless Sensor Networks (UWSNs) attracted the interest of many researchers and the past three decades have held the rapid progress of underwater acoustic communication. One of the major problems in UWSNs is how to transfer data from the mobile node to the base stations and choosing the optimized route for data transmission. Secure routing in UWSNs is necessary for packet delivery. A few researches have been done on secure routing in UWSNs. In this article, a new secure routing algorithm called Secure Routing Algorithm for Underwater (SRAU) sensor networks is proposed to resist against wormhole and sybil attacks. The results indicate acceptable performance in terms of increasing the packet delivery ratio regarding the wormhole and sybil attacks, increasing network lifetime through balancing the network energy consumption, high detection rates against the attacks, and decreasing the end to end delay.

doi*: 10.5829/ije.2018.31.10a.07*

1. INTRODUCTION

UWSNs include a large number of sensor nodes, distributed in the aquatic environment for collecting data. They generally provide solutions for various types of surveillance and monitoring applications that include environmental monitoring, health care, battlefield monitoring, etc. For example, the research presented in literature [1] provided a monitoring system for underwater oil exploration using acoustic sensor networks. The topologies of UWSNs are changing unpredictably and dynamically due to the resource limitations and complexity of the water environment in nodes; therefore, UWSNs would encounter a variety of attacks [2].

The current study presents an algorithm for secure routing in underwater sensor networks to make them resistant against wormhole and Sybil attacks and safely transfer the data from the underwater sensor nodes to the sink node.

The remaining of paper is organized as follows: In section 2, we overview the related works. In section 3, we present the proposed algorithm. Section 4 is simulation and experimental results. Finally, we conclude the paper in section 5.

2. RELATED WORKS

According to the studies, there are not many papers and research works on secure routing in underwater wireless sensor networks. The limited numbers of research works on secure routing in underwater wireless sensor networks are provided which have been reviewed in the following section:

Du et al. [3] have provided a secure routing scheme for underwater acoustic networks. The analysis determines that the proposed signature scheme can effectively prevent forgery attacks and improve communication security. This secure routing scheme manages network performance under the proven hypothesis.

Bharamagoudra et al. [4] proposed agent-based secured routing scheme for underwater acoustic sensor networks. This protocol is implemented by four agencies: security, routing, underwater gateway and vehicles that are embedded with static and dynamic agents. Agents facilitate flexible and adaptable services for secure routing. This secure routing scheme can handle wormhole and route poisoning and impersonation attacks.

*Corresponding Author Email Jamei@qodsiau.ac.ir (S. M. Jameii)

Dargahi et al. [5] presented a distributed approach to detect and reduce routing attacks in UWSNs. This protocol proposes a collaborative detecting strategy that detects and reduces routing attacks in UWSNs. This secure routing protocol is resistant against sinkhole, out-of-band wormhole and encapsulated wormhole attacks.

Ateniese et al. [6] introduced a Security Framework for underwater acoustic sensor networks (SecFUN). SecFUN presents data confidentiality, integrity and authentication using short digital signature algorithms and AES-GCM encryption. SecFUN to meet the security requirements of deploying underwater acoustic sensor networks with various features and levels of security is flexible and customizable. They implemented their security scheme on the CARP routing algorithm and compared it with original CARP method in terms of energy consumption and latency.

Basagni et al. [7] introduced the Channel Aware Routing Protocol (CARP). CARP prevents loops and can successfully routes around holes and can exit from shadow zones, applying ordinary topology information; the protocol is designed to use power control for choosing robust links. Although using shorter control packets increase transmission efficiency, but it means that the shorter control packet cannot include remote distance routing information with low power consumption, especially in environments are changing rapidly.

Gomathi1 et al. [8] presented an Energy Efficient Shortest Path Routing Protocol for Underwater Acoustic Wireless Sensor Network. This study furnishes an energy effective approach called SPR toward routing for underwater sensor networks. This algorithm aims at saving energy and enabling faster handling.

Bu et al. [9] proposed a fuzzy logic vector–based forwarding routing protocol (FVBF). This algorithm can achieves multi-parameters and fuzzy routing decision that utilizes a fuzzy logic inference system to calculate desirableness of adaptation time in the VBF protocol.

Taghizadeh et al. [10] introduced a Lightweight and Energy Balancing Routing Protocol for Energy constrained Wireless Ad Hoc Networks (LEBRP). The presented protocol does not impose a high computational load on the network and is suitable for energy constrained networks.

Pouyan et al. [11], introduced an Estimating Reliability in Mobile ad-hoc Networks. In this study, propose a basic way for estimating reliability in MANET based on enumeration method which is not commodious in Time Complexity.

3. THE PROPOSED ALGORITHM

In this section, we propose our secure routing algorithm for UWSNs called SRAU.

3. 1. Network Model

We assumed a common architecture of UWSNs which the sinks are on the water surface and sensor nodes are deployed underwater. Sensor nodes are deployed from the top to bottom at different depths of the employed area. We assumed an underwater acoustic network in a cubic area of 500m×500m×500m with duplex communication channels, consisting of 300 homogeneous sensor nodes randomly distributed where every node knows its location and has a fixed transmission range. In the proposed algorithm such as paper [12], it is assumed that the nodes are equipped with an array of hydrophone. Data packets are forwarded to the destination in a hop-by-hop fashion instead of finding end-to-end path to avoid flooding. The transmission range of each node is a sphere with radius R. The nodes might be active or unpredictable due to the current state of the underwater moves. Each node supports two types of communications, so acoustic communication is used for underwater communication and radio communications are used when the sink node on the surface, seeks direct communication with the coastal base station. To make it simple, a key distribution scheme was considered based on Identity-Based Cryptography (IBC) reported in literature [13]. Each node X, has an ID as ID_X that its public key and ID-based private key K_X^{-1}, has presented with a reliable authority prior to network deployment. In this algorithm, the need to transmit lengthy key information in public key distribution schemes is removed.

3. 2. Energy Model

Our energy model for sensor nodes is based on paper [14]. Each node has the same available initial energy to send a k-bit message over distance R, the consumed energy is calculated by Equation (1):

$$E(K,R) = E_{elec}K + E_{amp}Kd^2 \tag{1}$$

E_{elec} is the energy required for transceiver circuitry to deal with one bit of data. E_{amp} is the energy required to process one bit of data to the transmitter amplifier. d is equal communication radius of nodes.

3. 3. Description of SRAU

The SRAU consists of four stages: The first stage is secure neighbor discovery under wormhole attacks in underwater acoustic networks. The second stage is the primary route discovery process which selects next reliable sending node to the sink node, so it increases the packet delivery probability towards the sink, as a consequence, increasing the reliability. The third stage is the attack detection process during data distribution. This stage is based on state information of nodes to detect the Sybil attack. The fourth stage is discovery alternative safe route to detect malicious nodes.

In underwater acoustic network which sensor nodes are movable, neighbor discovery is a fundamental requirement. In the neighbor discovery process, each node discovers its neighbors and provides a list of its neighbors. When a node wants to find its neighboring nodes, it broadcasts a request message in its communication range. Each request message includes a digital signature private key/public key, unique identification number. Identification number that has been embedded in the request message would be recorded in the table after being received by destination node. By receiving broadcast packets, at first, the receiving node searches for its identification number in the table and if there, it removes the received packet. In this way, repeated attacks are prevented. If the nodes that are in the communication range of sending request packet node succeed in verifying public/private key in the receiving packet, they decide to send packet nodes which have valid public/private key and send reply packet to the request node. The reply message contains the direction of received acoustic signal and itself public key and digital signature private key. To find the direction of acoustic signal, each node is equipped with the array of hydrophone, which can estimate the sent acoustic signal direction.

If there is node mobility in the underwater acoustic network, its effect should be examined on the nodes. To manage mobile nodes, the negative effects of these movements should be minimized on the routing protocol performance. The most important mobility control method is predicting mobile nodes. In a real scenario, horizontal movements are not possible in the range of 2-3m/s and there will be only small fluctuations, while vertically, the node continuously moves at a speed of 2-3m/s with flowing of the water. For example, node *x* sends a request message, node *y* receives the message at L1, node *y* sends reply packet to node *x* at L2. Now, the sent signal direction from *y* to *x* has changed. In such a situation, node *x* after verifying node *y* digital signatures, first checks that equation (2) is established.

According to the movement of node *y* from L1 to L2 location, a triangle was created between node *x* and node *y* by drawing sent and received signals as it shown in Fig. 1. **a** is the distance from node *x* to node *y* in L1. **b** is the distance from node *x* to node *y* in L2.

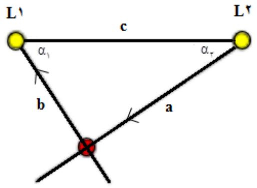

Figure 1. The effect of node mobility in the neighbor discovery process

c is the distance traveled from the previous node location to a new location.

$$\begin{aligned} &\frac{a}{\sin a_1} = \frac{b}{\sin a_2} = 2R \\ &a^2 = b^2 + c^2 - 2bc * \cos a_1 \\ &b^2 = a^2 + c^2 - 2ac * \cos a_2 \end{aligned} \qquad (2)$$

By obtaining an equal value of the above equation, the radius of triangle environment can be obtained. If the radius of triangle environment is greater than the communication range of node, node *y* is out of node *x* communication range and node *x* does not accept node *y* as its neighbor.

In case of establishing this relationship, node *x* updates previous location of node *y*. The direction of acoustic signal is calculated from *y* to *x*. Node *y* with receiving reply packet from node x, verifies the signature and then computes new received direction of the acoustic signal from node *x* and puts it in equation (3).

$$\left|\alpha_{yx} + \alpha_{xy}\right| - \pi \leq \delta \qquad (3)$$

δ is predetermined errors. α_{xy} is angles of direction xy.
If 180 degrees is subtracted from the sum of the acoustic signal of *x* to *y* and *y* to *x* is less than predetermined errors, node *y* can accept node *x* as a true neighbor and put it in its neighbors' list and then send the reply packet to node *x*.

In the reply packet, *x* and *y* node public key is put for the acoustic signal. By receiving reply packet by node *y*, signature is verified; if the signature is valid, then node *x* decides that node *y* has valid public/private key. Then it calculates the direction of the acoustic signal *y* to *x* and puts it in equation (3). In case of establishing of above relationship, node *x* can accept node *y* as a true neighbor and insert it in its neighbor's list.

After each node provides a list of neighbors, the real physical distance is calculated between two nodes to examine the relations of neighborhood nodes and detect the wormhole. If the measured distance is longer than the range of communication nodes, it is assumed that the nodes are connected via wormhole. In the SRAU, each sensor node calculates its distance to neighbors. Calculation of destination node is done using the energy of sent acoustic signal by the source node and receiving it by the destination node. That received energy is calculated as Equation (4):

$$E_{receive} = \frac{E_{send}}{4\pi R^2}\lambda \qquad (4)$$

E_{send} is the sent energy; *R* is communication range; and λ is the wavelength. We consider a fuzzy logic, so the input function is the distance and the consumed energy of node, the output function is node validation (Table

1). Actually, each node considers the neighbors that have low validation as wormhole attacks and removes it from its neighbors' list.

Routing is a fundamental issue for every network. Hence, routing should select the next forwarding node that increases the packet delivery probability towards the sink, consequently, increasing the reliability. Each node has a local routing table (Table 2).

When each sensor node sends a packet, attaches a unique ID to it.

In the routing process, first, a connect index is assigned to each node by sink node. Sink node first broadcasts a hello packet to assign the index to each node. Upon receiving the hello packets by sensor nodes, a connectivity index and hop count from the sink node, are assigned. Then, with receiving hello packets by nodes, their connectivity index and their hop count towards the sink are rebroadcasted, which may also receive this packet by their neighboring nodes. When a node receives a package from a neighboring node, first, the hop count of neighboring nodes is checked; if the hop count of neighboring nodes is less or equal than its hop count, its connectivity index increases one unit and keeps the ID, connectivity index and hop count of the neighboring nodes. Now, each node has a packet to send to the sink node and it should select the next forwarding node. First, that node sorts the neighboring list based on the highest connectivity index among its neighbors, whose neighboring list is obtained in the previous step. Now, the selected next forwarding node is based on the highest connectivity index, smaller hop count and more remaining energy. Then, the node sends a request packet to the next selected node that contains the node's position and the final destination and waits for the acknowledgement packet and sends its packet with received acknowledgement packet. A routing life depends on the deadline time or respective received acknowledgment such that each node is set with a timer and waits for the acknowledgment packet. If time expires or receives corrupted packet, it section is sent again.

TABLE 1. Validation

Distance	Energy consumed	Trust
Low	Low	High
Low	High	High
High	Low	Low
High	High	Low

TABLE 2. Local Routing Table (LRT)

#ID	Index connection to the sink	Hop number to the sink	Energy	Node lifetime

Neighbor node, receiving each part, checks data and resends the considered part to the destination.

During the data publication, a node often communicates with other nodes and each node consumes energy when sending and receiving packets. Then, the remaining node energy will be reduced. Some evaluation is done to detect Sybil attack during data publication. Sybil attacks are a serious threat in UWSNs. In such attacks, a malicious node creates several fake identities for itself and misleads the network nodes and reduces the remaining sensor nodes energy. So the network lifetime decreases. To find the suspicious node, each node data is examined.

(1) In a specified time period, node *x* starts to send packets to node *y*. Sent packets is displayed with P_{send}.

(2) Node *y* receives packets from node *x*. Sent packets is displayed with $P_{receive}$.

(3) Node *x* records connection time out after receiving a response from node *y*. Connection time-out is displayed with T_{end}.

4. SIMULATION AND EXPERIMENTAL RESULTS

In this section, we have simulated our proposed algorithm by NS2 and compared it with some other algorithms. The simulation network is composed of 300 nodes and 50 beacon nodes, randomly distributed in a 500m×500m×500m area. 20 Sybil and wormhole nodes were randomly placed. Each node had the same communication range of 100m. The evaluation of the SRAU was performed from some aspects, such as the detection rate, packet delivery ratio, average end-to-end delay, lifetime and energy consumption. The simulation parameters are presented in Table 3.

4. 1. Experiment 1: Detection Rate

The relationship between the detection rate and the number of nodes in the SRAU and other algorithm is shown in Figure 2. Detection rate is defined as a percentage of successful detecting of Sybil and wormhole nodes. By increasing the number of nodes, the detection rate of proposed scheme increases more compared with other algorithms.

TABLE 3. The simulation parameters

Parameters	Value
Simulation Area Size	500m×500m×500m
Transmission Range	100m
Traffic Model	CBR
δ	4°
Simulation time	300s

The proposed algorithm is better than the compared algorithm and only a minor part is getting worse. The proposed algorithm has a higher efficiency in comparison with other investigated algorithms at the detection rate of malicious nodes because other algorithms.

4. 2. Experiment 2: Packet Delivery Ratio Figure 3 shows packet delivery ratio in the different number of nodes for the proposed algorithm, [8-10]. By increasing the number of nodes, the connectivity index increases between the nodes, thus, enhancing the packet delivery ratio. When there are 75 nodes in the network, the packet delivery ratio is less unlike other states. This is because the number of nodes in the simulation space is low and the distance between nodes is usually greater than the radius of their relationship, thus the possibility of creating route is less. By increasing the number of nodes, delivery rate increases.

4. 3. Experiment 3: End-to-End Delay The average end-to-end delay increases in the proposed algorithm with increasing the number of nodes because after detecting malicious nodes, the nodes try to send data packets from the routes that get to destination properly (Figure 4). In most cases, the length of route increases to bypass the wormhole and Sybil nodes, which increases the end-to-end delay. However, it can be said that the proposed approach, by considering highest connectivity index and remained energy of forwarding node, sends the data packets as soon as it receives. Accordingly, the SRAU has a short end-to-end delay. In addition, the data packets are sent from the routes with higher reliability, comparing the lower end-to-end delay in the SRAU with other algorithms.

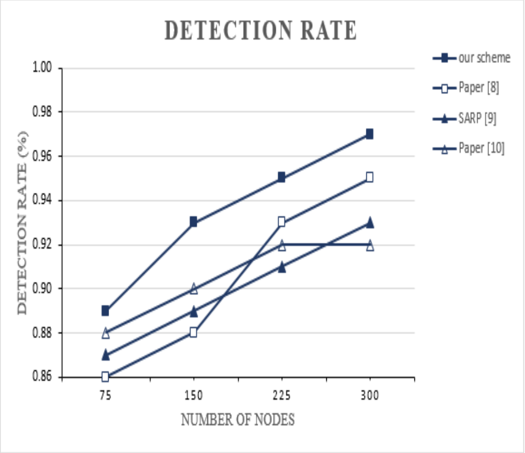

Figure 2. Detection rate. SARP indicates secure agent-based routing protocol

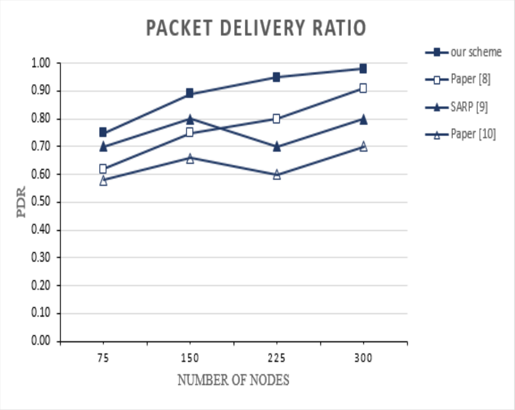

Figure 3. Percentage packet delivery with increasing number of nodes. SARP indicates secure agent-based routing protocol

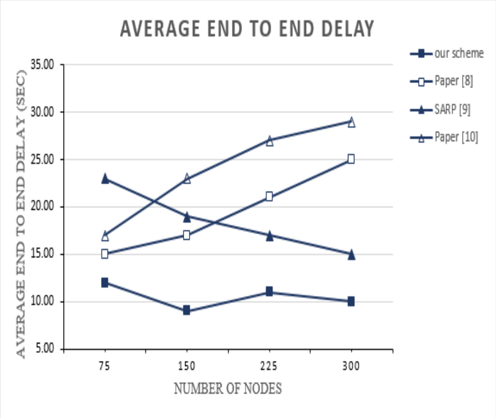

Figure 4. Average end-to-end delay with increasing number of nodes. SARP indicates secure agent-based routing protocol

4. 4. Experiment 4: Energy Consumption We measured the energy consumption of the proposed algorithm and compared it with some other protocols. As can be seen in Figure 5, the proposed algorithm consumed less energy than other algorithms. This is because the proposed algorithm considers the remaining energy of each node to select the next node for sending the packets. As the energy consumption in the network will be balanced, the network lifetime will be prolonged.

4. 5. Experiment 5: Network lifetime In the last experiment, we measured the Network lifetime of the proposed algorithm and compared it with some other protocols. Network lifetime is the time when the first node died in rounds. With these results in Figure 6, we can say that our schem is adaptable to different topologies and is more suitable for real underwater acoustic communication situations.

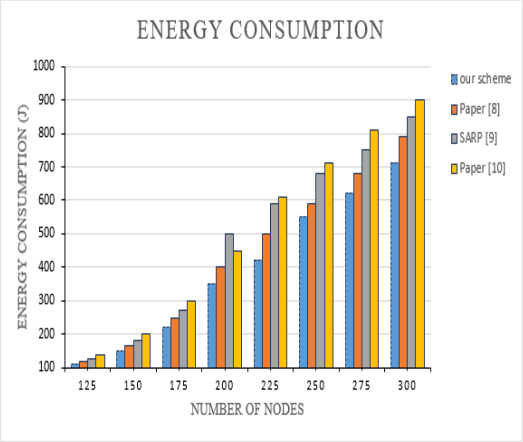

Figure 5. Energy consumption. SARP indicates secure agent-based routing protocol

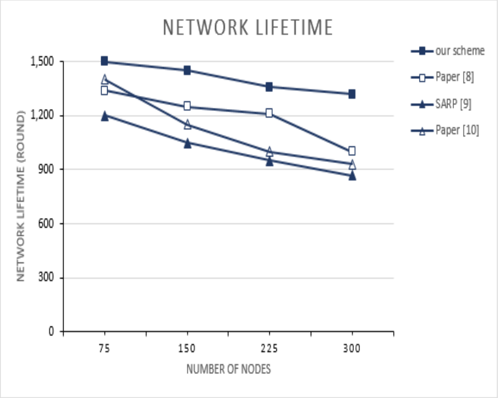

Figure 6. Network lifetime. SARP indicates secure agent-based routing protocol

5. CONCLUSION

Security and secure routing is an important issues in UWSNs, especially in applications requiring data validation, privacy and integrity. In this article, a new secure routing algorithm called SRAU (Secure Routing Algorithm for Underwater Sensor Networks) is proposed to resist against wormhole and sybil attacks. In the proposed algorithm, based on the new information, an alternative safe route was used for transferring packets properly to the destination. The results indicated acceptable performance in terms of increasing the packet delivery ratio regarding the wormhole and sybil attacks, increasing network lifetime through balancing the network energy consumption, high detection rates against the attacks, and decreasing the end to end delay.

6. REFERENCES

1. Ribeiro, F.J.L., Pedroza, A.d.C.P. and Costa, L.H.M.K., "Underwater monitoring system for oil exploration using acoustic sensor networks", ***Telecommunication Systems***, Vol. 58, No. 1, (2015), 91-106.
2. Li, X., Han, G., Qian, A., Shu, L. and Rodrigues, J., "Detecting sybil attack based on state information in underwater wireless sensor networks", in Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on, IEEE., (2013), 1-5.
3. Du, X., Peng, C. and Li, K., "A secure routing scheme for underwater acoustic networks", ***International Journal of Distributed Sensor Networks***, Vol. 13, No. 6, (2017), doi: 10.1177/1550147717713643.
4. Bharamagoudra, M.R. and Manvi, S.S., "Agent- based secure routing for underwater acoustic sensor networks", ***International Journal of Communication Systems***, Vol. 30, No. 13, (2017), e3281.
5. Dargahi, T., Javadi, H.H. and Shafiei, H., "Securing underwater sensor networks against routing attacks", ***Wireless Personal Communications***, Vol. 96, No. 2, (2017), 2585-2602.
6. Ateniese, G., Capossele, A., Gjanci, P., Petrioli, C. and Spaccini, D., "Secfun: Security framework for underwater acoustic sensor networks", in Proceedings of MTS/IEEE OCEANS. (2015), 1-9.
7. Basagni, S., Petrioli, C., Petroccia, R. and Spaccini, D., "Carp: A channel-aware routing protocol for underwater acoustic wireless networks", ***Ad Hoc Networks***, Vol. 34, (2015), 92-104.
8. Gomathi, R. and Manickam, J.M.L., "Energy efficient shortest path routing protocol for underwater acoustic wireless sensor network", ***Wireless Personal Communications***, Vol. 98, No. 1, (2018), 843-856.
9. Bu, R., Wang, S. and Wang, H., "Fuzzy logic vector–based forwarding routing protocol for underwater acoustic sensor networks", ***Transactions on Emerging Telecommunications Technologies***, Vol. 29, No. 3, (2018), doi: 10.1002/ett.3252.
10. Taghizadeh, S. and Mohammadi, S., "Lebrp-a lightweight and energy balancing routing protocol for energy-constrained wireless ad hoc networks", ***International Journal of Engineering-Transactions A: Basics***, Vol. 27, No. 1, (2013), 33-38.
11. Pouyan, A. and Yadollahzadeh Tabari, M., "Estimating reliability in mobile ad-hoc networks based on monte carlo simulation", ***International Journal of Engineering***, Vol. 7, No. 5, (2014), 739-746.
12. Zhang, R., Sun, J., Zhang, Y. and Huang, X., "Jamming-resilient secure neighbor discovery in mobile ad hoc networks", ***IEEE Trans. Wireless Communications***, Vol. 14, No. 10, (2015), 5588-5601.
13. Zhang, Y., Liu, W., Lou, W. and Fang, Y., "Location-based compromise-tolerant security mechanisms for wireless sensor networks", ***IEEE Journal on Selected Areas in Communications***, Vol. 24, No. 2, (2006), 247-260.
14. Heinzelman, W.R., Chandrakasan, A. and Balakrishnan, H., "Energy-efficient communication protocol for wireless microsensor networks", in System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on, IEEE., (2000), doi: 10.1109/HICSS.2000.926982.

A Secure Routing Algorithm for Underwater Wireless Sensor Networks

M. Ahmadi[a], S. M. Jameii[b]

[a] *Department of Computer Engineering, Karaj Branch, Islamic Azad University, Karaj, Iran*
[b] *Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran*

PAPER INFO

Paper history:
Received 11 February 2018
Received in revised form 28 April 2018
Accepted 17 August 2018

Keywords:
Underwater Wireless Sensor Networks
Security
Routing
Wormhole and Sybil Attack

چکیده

اخیرا شبکه های حسگر بی سیم زیر آب توجه بسیاری از محققین را به خود جلب کرده است و ارتباطات صوتی نیز در طی سه دهه اخیر پیشرفت سریعی داشته است. یکی از مسائل اصلی در شبکه های حسگر بی سیم زیر آب این است که چگونه داده از گره متحرک به ایستگاه پایه ارسال شود و مسیر بهینه برای ارسال داده انتخاب شود. مسیریابی امن در شبکه های حسگر بی سیم زیر آب برای تحویل بسته ها الزامی است. تحقیقات اندکی روی بحث مسیریابی امن در این نوع شبکه ها صورت گرفته است. در این مقاله، یک الگوریتم مسیریابی امن جدید بنام SRAU ارائه می شود که در مقابل حملات wormhole و sybil مقاوم است. نتایج شبیه‌سازی نشاندهنده کارایی قابل قبول روش پیشنهادی با توجه به معیارهای نرخ تجویل بسته، طول عمر شبکه و مصرف متوازن انرژی، نرخ تشخیص حملات و تاخیر انتها به انتها است.

***doi**: 10.5829/ije.2018.31.10a.07*