https://doi.org/10.33261/jaaru.2019.26.1.015 *Association of Arab Universities Journal of Engineering Sciences (2019) 26(1): 113–120*

Association of Arab Universities Journal of Engineering Sciences
مجلة اتحاد الجامعات العربية للدراسات والبحوث الهندسية

Secure Mobile Sink Node location in Wireless Sensor Network using Dynamic Routing Protocol

Ahmed R. Zarzoor [1,*], ***Mahmood Z. Abdullah*** [2], **and** ***Nadia A. Shiltagh*** [3]

[1] *Institute for Post-graduation Studies, Iraqi Commission for Computer and informatics, Baghdad, Iraq, ahmed.arjabi@gmail.com*

[2] *Department of Computer Engineering, Al-Mustansiriyah University, Baghdad, Iraq, drmzaali@uomustansiriyah.edu.iq*

[3] *Department of Compute Engineering, University of Baghdad, Baghdad, Iraq, dr.nadiaat123@gmail.com*

** Corresponding author: Ahmed R. Zarzoor, ahmed.arjabi@gmail.com*

Published online: 31 March 2019

Abstract— The important device in the Wireless Sensor Network (WSN) is the Sink Node (SN). That is used to store, collect and analyze data from every sensor node in the network. Thus the main role of SN in WSN makes it a big target for traffic analysis attack. Therefore, securing the SN position is a substantial issue. This study presents Security for Mobile Sink Node location using Dynamic Routing Protocol called (SMSNDRP), in order to increase complexity for adversary trying to discover mobile SN location. In addition to that, it minimizes network energy consumption. The proposed protocol which is applied on WSN framework consists of 50 nodes with static and mobile SN. The results havw shown in each round a dynamic change in the route to reach mobile SN, besides prolong the network lifetime in compare with static SN.

Keywords— Wireless Sensor Newark (WSN), Sink Node (SN), Traffic analysis Attacks.

1. Introduction

Nodes in a WSN deployed in wide geographical area to collect data such as temperature, humidity and pressure. These data are sent from sensor nodes or clusters to Sink Node (SN) either in a single or multi-hop route. The SN analyses the collected data and connect the WSN to the cloud server or higher authority. Therefore, any failure in SN would make the entire WSN useless. Also, it can be a reason to lose a remarkable amount of data that cannot be transmitted to end users. Thus, the significant role of SN in a WSN may attracts opponent's attention .

The opponents usually use robust laptops and strong antennas capabilities to observe the traffic patterns. They monitor patterns for long periods of time and try to estimate the SN position. Since, all the nodes send their sensory data to SN using a single-hop or multi-hop route, which makes the traffic near SN region be congested. Thus, the opponent can implement the traffic analysis in this region and can be able to reach the SN position. So, one of the solutions is using a mobile SN to increase the hardness in tracing the path to SN for adversary. Furthermore, it divides the traffic on different parts of the WSN, in order to maximize complexity for adversary to specify SN location [4].

On other hand, there are some challenges on using mobile SN such as: designing the routing path to the mobile SN. Also, changing the SN position continually could cause loss of some data packets for nodes that are located in an appropriate position to the new SN location. In, [6] researchers proposed AERO and free AERO and they used transition time of SN within the new location to enhance the network lifetime. Another solution which takes into account decreasing the distance between Cluster Head (CH) and SN in order to reduce the communication energy consumption [13]. Furthermore, in [9], the study suggested that CH must be deployed in a way that it covers all of the network nodes. Thus, each node can find at least one cluster to communicate with it .

However, in this study a mobile SN is used to maximize complexity for adversary in tracing the path to SN location. Also, a new dynamic routing protocol developed in order to specify the path between CHs and SN based on location and residual energy of each CH in the network. The proposed protocol specifies a new position for mobile SN by taking the mean of all CHs locations in each round. Although, to reduce the traffic near the SN only one CH can send all aggregate data from other clusters head on the path to SN. In addition to that, it must have the highest residual energy and closest distance to the SN in

comparison with other CHs in each round. In this study, both static and mobile SNs are used. The implementation results have shown an improvement in the network lifetime when using the protocol with mobile SN in comparison with the static SN. As will be seen the method increased the complexity in specifying SN position for adversary. The rest of this paper's arrangement is as follows: Section 2 review of related works, Section 3 shows the study method which demonstrates the proposal WSN framework three phases (initial, setup and process) phase and SMSNDRP protocol constructing steps. Section 4 discusses simulation results of the proposed protocol on WSN framework consisting of 50 nodes with static and mobile SNs and finally Section 5 includes study conclusions.

2. Related Works

In the last few years, hiding the SN location, ID and role of nodes has a great attention of WSN researchers. In [2,3] researchers study supporting the SN anonymity through organizing nodes inside the clusters. These clusters are connected to each other using mesh topologies. Thus, the mesh provides more than one path to send the collected data to the SN, which increases the complexity for attackers to trace the path to SN position. Also, they used the Hamiltonian cycle to make the SN appears as a normal node in the cycle. In [14] the researchers used a ring nodes around the mobile SN to store its location information. Thus, all the nodes can communicate with the SN via this ring. Also, in [15] used a blast node that acts as endpoint around the SN. Consequently, when any node in the network sends its collected data to the SN it must selects the first one of the blast nodes. Which in turn sends the data to the area that coveres all the range of endpoints around SN and perform a mask to its ID.

On the other direction, Baroutis and Younis showed in their study [5] how the attackers perform traffic analysis using three kinds of attack models: GSAT Test, Entropy and Traffic Volume (TV) and Evidence Theory (ET). In the GSAT Test, the attackers follow a number of steps until they discover the SN location. They start by observing the activities of radio transmission for a random number of nodes and their neighbors during a particular time. In case not reaching to the SN position, they refer to this case as local maxima and start again but also take into account the previous local maxima's. While in model TV and Entropy, the attackers follow the traffic distribution in the whole network. So, when there is more traffic in one region in the network, it means that the attacker determines the SN location. In ET, the attackers collect evidence about network, such as transmission time and receive time, location information, strength of received signal, etc. In order to increase the confidence about the path that they follow to reach SN location. Another technique, Lightfoot and Ren, injected fake data in order to create fake area and high traffic in the network [8]. Thus, the attacker cannot know the SN position, but using this technique cause increasing in energy consumption and reduce the networks lifetime.

Another approach to protect sink node ID was proposing in Haakensen and Thulasiraman, study [12] they used k-anonymity. In which there must be at least one node in the network acting as a SN. Thus, any changes in the SNs behavior and its neighbors, must be done in the same way by node that acts as SN. This is performed in order to make the same changes in the network traffic. As a result, increasing the number of nodes that behave in the same way as the SN would maximize the protection of the SNs ID. Also, to secure the SN location, Ying, et. al used IATA to make some fake SNs behave similarly as SN [16]. In addition, nodes around fake SN generate fake messages in order to generate more traffic in the whole network which causes confusion to the opponents .

In this study, an SMSNDRP protocol is proposed to protect the mobile SN location. The data collected from the nodes is sent to its cluster head, which in turn forward sensory data to the next CH on the path until it reaches the SN. Only CH with highest remaining energy and minimum distance in comparison with other CHs is able to send sensory data to the SN directly. The routing protocol is dynamically altered in each round. This is due to the CHs and mobile SNs locations being changed based on the mean of CHs locations. Consequently, this adds more difficulties for opponents to analyze traffic patterns and discover the SN position

3. Study Method

This paper proposes a SMSNDRP protocol to secure mobile SN location against a traffic analysis attack. Also, it provides an efficient way to enhance the energy consumption and prolong the networks lifetime. The study method is divided into three phases. These are: initial phase, setup phase and the process phase as will be shown below in details.

3.1 *Initial Phase*

The WSN is divided into small sub areas by using “Delaunay Triangulation” method [1,10] in order to increase its coverage. This is executed to deploy the sensor nodes in an efficient way and to avoid the case of hot spots. In Delaunay Triangulation, the locations of all nodes are the set points that are used to define the numbers of triangular in a way to make a circumcircle passes via end points and ensuring no else points of data sets. In this study, 50 nodes are deployed into a 1000x1000m2 area using Delaunay Triangulation as shown in Figure 1.

In Figure 1, the blue points represent the nodes location in the area that is used to specify blue dash triangles in a way that plots polygon edges in red in order to represent the best coverage area of each node in WSN.

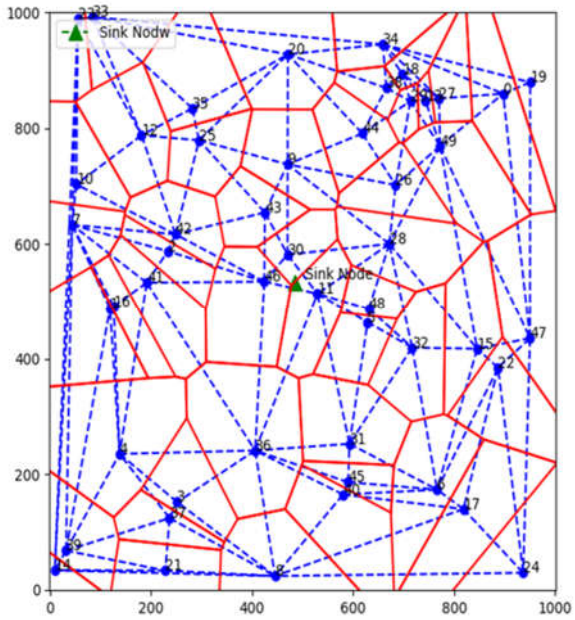

Figure 1: Coverage Area in WSN using Delaunay Triangulation [1].

3.2 *Setup Phase*

After dividing the WSN area into sub areas in the initial phase, the WSN framework will then be constructed. The SMSNDRP is implemented on hierarchal clustering WSN. The DECAR [4], algorithm is used to select the cluster head in order to reduce the hot spot problem through the process of transmission aggregate data to SN. The algorithm organized the CHs in a way that puts the CHs with higher remaining energy closer to the SN and CHs with lower residual energy far away from SN. In SMSNDRP, a mobile SN is used rather than the static SN that was used in the DECAR. Also, the new position of mobile SN is specified according to the mean of all CHs locations in one round. This will ensure the best position for mobile SN that minimizes the distance between CHs and SN beside prolonging the network lifetime. For instance, Table (1) shows the location of 15 clusters, distance between (CHs and SN) and the residual energy for each cluster. The mobile SN new position is calculated using the mean Eq. (1) and Eq. (2) [7]:

$$X_{PostionSN} = \frac{\sum_1^N X}{N} \qquad (1)$$

$$Y_{PostionSN} = \frac{\sum_1^N X}{N} \qquad (2)$$

Where N is the number of clusters in each round and $X_{PostionSN}$, $Y_{PostionSN}$ is the new location coordination that mobile SN is moved to it in the current round.

The distances between the CHs and SN are calculated by using Euclidean distance Eq. (3). Where d is the distance between SN and CH

$$d(SN.CH) = \sqrt{\sum_{i=1}^{N} (SN - CH)^2} \qquad (3)$$

So, the new SN position according to the shown routing details in Table (1) is ($X_{PostionSN}$ =471.0797609, $Y_{PostionSN}$ 599.965588) using Eq. (1) and Eq. (2).

For energy model, the radio model [11], was used in this study. Which consists power amplifiers, receiver energy and transmitter energy. Eq. (4) is used to calculate the transmission of Z bits at distance (d).

$$E_{Tx}(m.n) \begin{cases} (\alpha Tx + \varepsilon fs d^2)Z & D(m,n) < d_0 \\ (\alpha Tx + \varepsilon fmp d^4)Z & D(m,n) \geq d_0 \end{cases} \qquad (4)$$

Where D(m,n) is the distance between nodes m and n, *fs* is the free space used for single path loss power d^2 , fmp is the free multi-path, the loss power is d^4 , and d_0 is the energy threshold calculated using Eq. (5).

$$d_0 = \sqrt{\frac{\varepsilon fs}{\varepsilon fmp}} \qquad (5)$$

Eq. (6) is used to calculate the usage energy to receive Z bits.

$$E_{Rx}(m) = Z\alpha_{Rx} \qquad (6)$$

Where
αTx and αRx are the transmisstion and recivied electronic energy in Eq (4), εfs *and* εfmp are the amplifier energy in in Eq. (4) and Eq. (5), E_{Rx} is the usage energy for $Z\alpha_{Rx}$ in Eq.(6) and αTx, αRx, εfs *and* εfmp are measured by Joules units.

3.3 *Process Phase*

After setting up the WSN framework, in this phase the SN moves in each round to a new location based on the locations of the new selected CHs. In order to protect the SN position from the traffic analysis attack, the SMSNDRP allowed only one CH to send aggregate data to SN. So, in that way the SN will appear as a normal node in the network. Also, the SMSNDRP sort the elected CHs in each round in descending order according to their residual energy and in ascending order according to their distance from mobile SN position, given in Table (1).

Table 1: SMSNDRP routing path to the mobile SN in one round.

Cluster	X Position	Y Position	Residual Energy Joules (J)	Distance from Sink node Meters (M)
1	950.7618578	878.9863309	94.88030189 J	671.5183571 M
2	236.7718757	123.9605385	93.58023478 J	207.5788199 M
3	43.99340942	632.8745278	92.87681447 J	460.095624 M
4	470.5109358	737.3991075	88.4890678 J	231.3657215 M
5	666.2712095	869.1947348	80.81448647 J	456.8593495 M
6	471.0797609	927.1944225	80.37791917 J	595.2334731 M
7	684.387865	701.6916831	78.09178587 J	539.2435395 M
8	766.4149401	173.2677225	78.02580034 J	435.3124149 M
9	671.8028445	599.9655885	77.66520141 J	277.9587957 M
10	137.9038006	235.111987	71.35386816 J	441.7647806 M
11	445.6636064	23.65610903	51.59057076 J	484.6410634 M
12	743.7496701	847.2104491	48.33353494 J	426.9064958 M
13	191.7300314	532.8801492	28.77882363 J	404.7675446 M
14	529.6031372	513.6488076	28.4883356 J	43.76157647 M
15	228.4420448	33.04829679	11.95280705 J	420.893193 M

4. SMSNDRP Protocol Steps

1. In round one let R=1, Where R is counter of the round number.
2. Forming clusters using DECAR algorithm to elect CHs. In this algorithm each node has a time latency (t) before its start a CHs election. The node with higher residual energy will be selected as CH. However, the higher remain energy will be measured based on the overlapping area between the nodes and maximum distance between the current node and SN. Thus CHs with higher remain of energy become closer to the SN and CHs with lower residual become far away from SN
3. After forming clusters in the network, the next step is specifying the new position for mobile SN using Eq. (1) and Eq. (2) in order to calculate $X_{PostionSN}$, $Y_{PostionSN}$ of the new location coordination that a mobile SN is moved to it in the current round.
4. Subsequently, computing the distance between each elected CH and new SN position using Eq. (3)
5. In this step, used CHs residual energy and their distance from the mobile SN. In order to define the routing path to the mobile SN as follow:
   a. Arrange the CHs according to their residual energy from largest to smallest and
   b. Arrange the CHs according to their distance from SN (smallest to largest).
6. Calculate the energy consumption for transmitter, receiver and amplifier using Eq's. (4, 5 and 6).
7. If one or more of CHs total residual energy on the routing path to SN is less than the value of energy threshold d0 that is calculated using Eq. (5), then the number of round R is incremented by one and go to step 2 otherwise go to step 6.

5. Results

The WSN framework and SMSNDRP protocol implemented using Python programming language version 2.7. The number of node 50 deployed in area range 1000x1000m2 see Table (2). The protocol applied using static SN in two positions: corner and center of the network. When the static SN is placed in the corner, the network drained all its energy in two rounds. While it is extended to 12 rounds when place the static SN in the center of the network.

Table 2: Simulation Parameters.

No	Parameter	Unit
1	Number of nodes	50
2	Area	1000x1000 Meters
3	Packet size	3000 bits
4	Energy dissipated at the transceiver electronic (E _ELEC)	50e-9 Joules
5	Energy dissipated at the data aggregation (E_DA)	5e-9 Joules
6	Energy dissipated at the power amplifier (supposing a multi-path Emp	0.0013e-12 Joules
7	Energy dissipated at the power amplifier (supposing a line-of-sight free-space channel E_FS	10e-12 Joules

However, the proposes protocol are implemented with mobile SN in the network. In each movement of SN, the path that leads to the SN is changed in each round. In addition, the first CH on that path has the lowest residual energy and maximum distance from SN than other clusters head on the same path. While, the last CH has the largest remaining energy and minimum distance to SN. So, it cans only send the aggregate data that received from other CHs

on the path to the SN. In Figure (2), the number of clusters is 35, the first position of mobile SN is (474.24342213, 512.61998603) and network lifetime becomes exhausted in 14 rounds. In Figure (3), the number of clusters is reduced to 25, the SN moves to the second location (473.73628537, 499.79405746) and the network lifetime is extended to 78 rounds. Within Figure (4), the SN moved to third position (486.41612648, 506.58073298). The number of clusters is reduced to 19 and the network lifetime depleted in 24 rounds. In Figure (5), the fourth location of SN is (482.60579928, 522.00603031) and the number of clusters is reduced to 15 and number of rounds is 32, see Table (3).

So, the path to SN was changed dynamically based on the locations of elect clusters head. Each path is completely different from other paths in Table (3). Beside the location of SN node is changing in each round. In order to increase the anonymity of SN position.

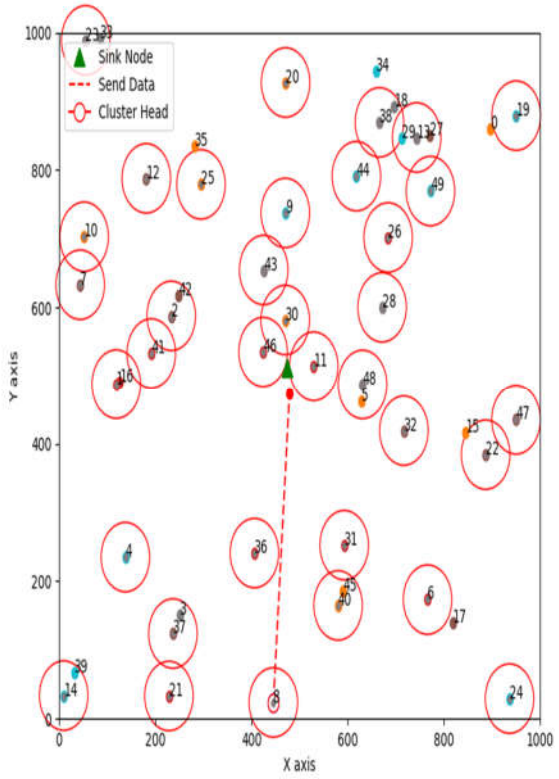

Figure 2: Mobile SN first location, number of cluster 35

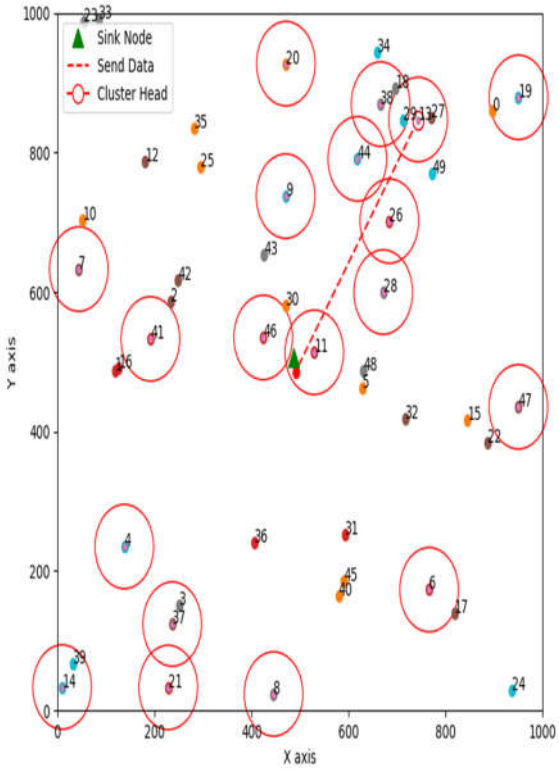

Figure 3: Mobile SN location 2, number of cluster 25.

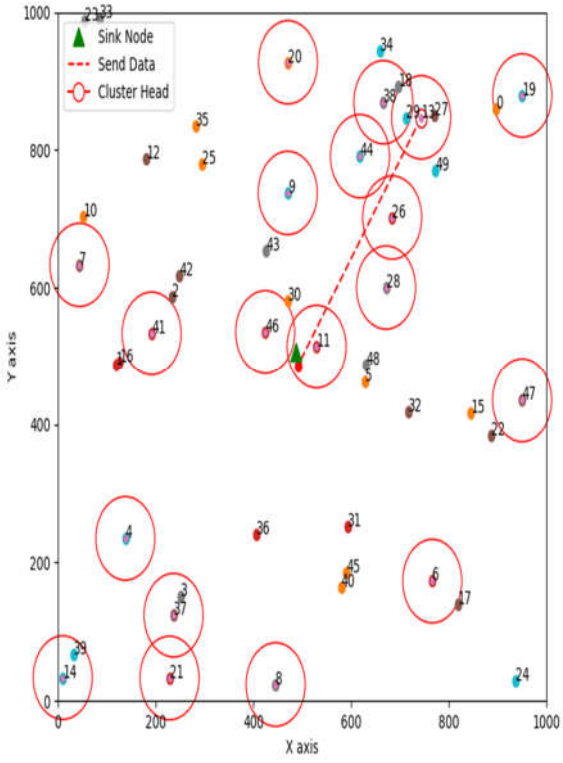

Figure 4: Mobile SN Location 3, number of cluster 19

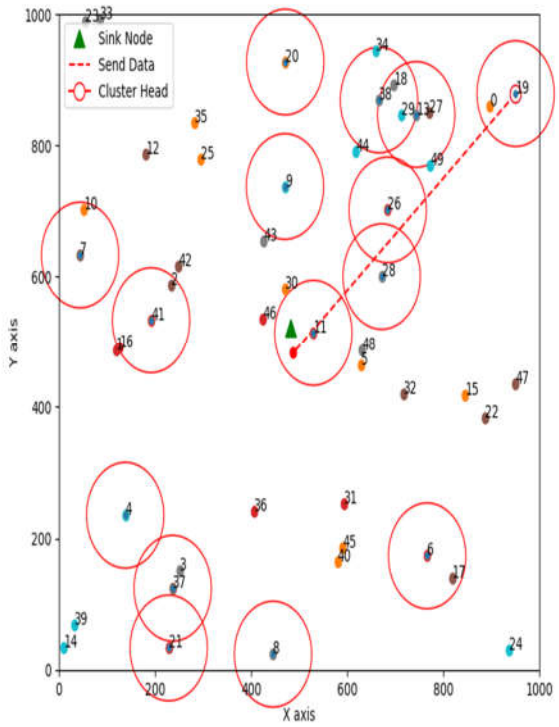

Figure 5: Mobile SN Location 4, number of cluster 15.

6. Consolations

The SN is the most substantial device of the whole WSN because all sensor nodes send their sensory data to it (in order to store and analyze it). Besides, SN proved interface to communicate entire network with outside clients' servers. Therefore, attackers target it, through tracing the path that lead to its location .

In this paper the SMSNDRP protocol is proposed to secure mobile SN location from being discovered by the attackers. In addition to that, the protocol is extending the networks lifetime. Also, the position of mobile SN is changed in each round based on the calculation of the mean of elected clusters head locations. The path to the SN is dynamically changed and derived from clusters head locations through ordering them in ascending order according to their residual energy and in descending order according to their distance from the SN. The result of this study shows that the network lifetime is extending in each round in comparison with the Static SN. Also, the routing path to the mobile SN is dynamically changed, which in turn adds more confusion to the adversary to specify SN position in the network.

Table 3: Mobile Sink Node in four locations.

Mobile Sink Node location	No. of Cluster	No. of rounds	Path to Sink node
[474.24342213, 512.61998603]	35	14	CH23->CH10->CH7->CH12->CH1->CH41->CH2->CH12->CH25->CH4->CH14->CH37->CH20->CH9->CH43->CH46->CH30->CH11->CH36-> CH38->CH13->CH44->CH49->CH26->CH28->CH48->CH32->CH31->CH40->CH6->CH24->CH22->CH47->CH19->CH8->SN
[473.73628537 499.79405746]	25	78	CH12->CH7->CH2->CH41->CH4->CH14->CH37->CH21->CH20->CH9->CH30->CH46->CH36->CH8->CH31->CH6->CH47->CH28->CH26->CH44->CH38->CH13->CH19->CH11->SN
[486.41612648, 506.58073298]	19	24	CH7->CH41->CH4->CH14->CH37->CH21->CH8->CH6->CH47->CH9->CH20->CH38->CH44->CH11->CH46->CH26->CH19->CH28->CH13->SN
[482.60579928, 522.00603031]	15	32	CH7->CH41->CH4->CH37->CH21->CH8->CH6->CH20->CH9->CH38->CH29->CH26->CH28->CH11->CH19->SN

Acknowledgements

We would like to appreciate all the excellent suggestions of anony-mous reviewers to enhance the quality of this paper.

References

[1] A. Soundarya and V. Santhi, "An efficient algorithm for coverage hole detection and healing in wireless sensor networks", IEEE 1st International conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech), Kolkata, pp. 1-5, 2017.

[2] S. Alsemairi and M. Younis, "Forming a cluster-mesh topology to boost base station anonymity in wireless sensor networks", Proc. of IEEE Wireless Communications and Networking Conference, pp. 1-6., 2016

[3] Alsemairi S and Younis M., "Cross-layer technique for boosting base-station anonymity in wireless sensor networks". Int J Commun Syst.; pp. 1-16, 2017.

[4] Amgoth, Tarachand & Jana, Prasanta, "Energy-aware routing algorithm for wireless sensor networks". Computers & Electrical Engineering, Vol. 41, pp. 357-367, 2014.

[5] Baroutis, N., and Younis, M., "A novel traffic analysis attack model and base-station anonymity metrics for wireless sensor networks". Security Comm. Networks, Vol. 9, pp. 5892–5907, 2016.

[6] Chen, J.I.Z. and Lin, C.H., "Algorithms for promoting anonymity of BS and for prolonging network lifetime of WSN", Peer-to-Peer Networking and Applications, Vol. 7, pp.710-722, 2014.

[7] Dâmaso, Antônio; Rosa, Nelson; Maciel, Paulo., "Integrated Evaluation of Reliability and Power Consumption of Wireless Sensor Networks." Sensors, Vol. 11, pp. 1-27, 2017.

[8] L. Lightfoot and J. Ren, "R-STaR destination-location privacy schemes in wireless sensor networks", IEEE International Conference on Communications, pp. 7335-7340, 2015.

[9] M. Samanta and I. Banerjee, "Optimal load distribution of cluster head in fault-tolerant wireless sensor network", in Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-7, 2014.

[10] S. Saha, "Sensor Node Placement Methods Based on Computational Geometry in Wireless Sensor Networks: A Review", International Research Journal of Engineering and Technology (IRJET), Vol. 05, pp. 799-804, 2018.

[11] Sohal, A.K., Sharma, A.K. and Sood, "Enhancing Coverage Using Weight Based Clustering in Wireless Sensor Networks", Wireless Pers Commun., Vol. 98, pp. 3505–3526, 2017.

[12] T. Haakensen and P. Thulas-iraman, "Enhancing sink node anonymity in tactical sensor networks using a reactive routing protocol", IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 115-121, 2017.

[13] V. Biradar, S. R. Sawant, R. R. Mudholkar, and V. C. Patil, "Multihop routing in self-organizing wireless sensor networks", International Journal of Computer Science Issues (IJCSI), Vol. 8, pp. 155-164, 2011.

[14] V. Kumar, A. Kumar and M. Singh, "Boosting anonymity in wireless sensor networks", 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, pp. 344-348, 2017.

[15] V.P.V. Gottumukkala, V. Pandit, H. Li, and D.P. Agrawal, "Base station location anonymity and security technique (blast) for wireless sensor networks", in Proc. of IEEE International Conference on Communications (ICC), pp. 6705–6709, 2012.

[16] Ying D., Makrakis D., Mouftah HT., "Anti-traffic analysis attack for location privacy in WSNs". EURASIP Journal on Wireless Communications and Networking, Vol. 1, pp. 131-143, 2014.

حماية موقع عقدة الحوض المتحركة في شبكة الاستشعار اللاسلكية باستخدم نظام المراسم للمسار الحركي

احمد رشيد زرزور[1،*]، محمود زكي عبدالله[2]، نادية عدنان شلتاغ[3]

[1] *معهد المعلوماتية للدراسات العليا، الهيئة العراقية للحاسبات والمعلوماتية، بغداد، العراق، Ahmed.Arjabi@gmail.com*

[2] *قسم هندسة الحاسبات، الجامعة المستنصرية، بغداد، العراق، drmzaali@uomustansiriyah.edu.iq*

[3] *قسم هندسة الحاسبات، جامعة بغداد، بغداد، العراق، dr.nadiaat123@gmail.com*

[*] *الباحث الممثل: احمد رشيد زرزور، Ahmed.Arjabi@gmail.com*

نشر في: 31 آذار 2019

الخلاصة – تعد عقدة الحوض او المحطة الرئيسية اهم جهاز في شبكة الاستشعار اللاسلكية حيث تستخدم لتخيزين وجمع البيانات من كل نودات الاستشعار في الشبكة. هذه الوظيفة الرئيسية للسنك نود في شبكة الاستشعار اللاسلكية تجعلها هدفاً رئيسياً لهجوم تحليل الترفك .لهذا حماية مكان عقدة الحوض يعد امراً مهم. في هذه الدراسة نقدم طريقة لحماية عقدة الحوض المتحركة باستخدام نظام المراسم (SMSNDRP) بغية حماية موقع عقدة الحوض من مهاجمين تحليل ترفك الشبكة بالاضافة الى ان هذا نظام المراسم يستخدام طاقة اقل في الشبكة حيث في كل حركة عقدة الحوض يتغير مسار الوصول اليها بالاعتماد على الوسط الحسابي لمواقع رؤوس الكلاستر في كل جولة . نظام المراسم المقترح تم تطبيقة على شبكة الاستشعار اللاسلكية مؤلفة من 50 عقدة مع عقدة الحوض ثابتة ومتحركة النتائج اظهرت تغير المسار بشكل حركي للوصول للشبكة مع زيادة مدة استخدام الشبكة عقدة الحوض المتحركة بالمقارنة مع عقدة الحوض الثابتة.

الكلمات الرئيسية – شبكة الاستشعار اللاسلكية ، عقدة الحوض ، هجوم تحليل ترفك الشبكة.