A Novel Approach for Boosting Base Station Anonymity in a WSN

Vicky Kumar
Department of E&CE
NIT, Hamirpur
Himachal Pradesh, India

Ashok Kumar
Department of E&CE
NIT, Hamirpur
Himachal Pradesh, India

***Abstract*—Nodes in a wireless sensor network scrutinize the nearby region and transmit their findings to the base station (BS) using multi-hop transmission. As the BS plays an important role in a wireless sensor network, therefore an adversary who wants to interrupt the operation of the network would avidly look for the BS location and imposes maximum damage by destroying the BS physically. The multi-hop data transmission towards BS makes a prominent pattern of the traffic (huge traffic near the BS region) that indicates the presence of BS in the nearby region and thus the location of the BS may expose to the adversaries. This work aims to provide a novel approach which will increase the BS anonymity. For this purpose, a randomly roamed BS and the special nodes are proposed to achieve the above mentioned objective. The special nodes produce a large number of high traffic regions, which are similar to the BS region. Now, there are many regions which look like BS region and hence the probability to get the BS region using traffic analysis is very low. Therefore, this approach increases the effort of adversaries in order to find the exact BS position. We have used a standard entropy model to measure the anonymity of the base station and the GSAT test is used to calculate the number of steps required to find the base station. The results show that the proposed technique provides better results in terms of anonymity compared to the existing techniques.**

Keywords*—Anonymity; network lifetime; wireless sensor networks

I. INTRODUCTION

Nodes of the wireless sensor networks (WSNs) are cost effective, small in size and are capable of sensing temperature, pressure and motion. But they are commonly constrained in energy, computational capacity and communicating capabilities. These nodes are randomly deployed in large numbers over a vast geographic area [1]. The nodes scrutinize the nearby environment and transmit their observations to the base station (BS) or sink node. If BS becomes faulty due to some reasons, then the whole network becomes inoperable. This makes the BS an important device in the network and therefore, an adversary can stop the functioning of a WSN by damaging the BS. Basically, nodes use multi-hop path for data transmission and hence each node transmit its data to a neighboring node which is one hop near to the BS. When these data packets arrive near the BS they will follow the same path.

This pattern produces a noticeable traffic and expose the BS location. An adversary can perform traffic analysis on such regions (comparing the sending time of the packets) and by doing this he/she can reach near to the BS [2]. The powerful antennas and a laptop with vigorous computing capabilities are commonly used for analyzing the traffic flow.

To conceal the position of the BS, various techniques have been proposed in literature using anonymity [3]-[7]. Identifying the role of the node and the position of the BS in itself is a clear statement of anonymity [8]. Various algorithms were taken on to estimate how anonymity can be used directly in the existing WSNs. The authors have proposed methods like K-anonymity and BAR to increase the BS anonymity [9]-[11]. These methods have been used a random or periodic packet transmission in order to distribute the traffic in the network and thus make it difficult to find the region near to the BS. These random or periodic packet transmission methods consume more energy and due to which the network lifetime is reduced. In recent years, mobile sink is used by many researchers in order to increase the network lifetime [12], [13]. Mobile sink is placed in a moving vehicle and redeployed to a new position whenever required. However, a mobile sink changes the routing paths regularly and hence WSNs will require generation of new routing paths frequently [12]. A mobile sink has mainly two advantages: Firstly, tracking of a mobile BS is difficult compared to the static one and secondly, it helps in enhancing network lifetime by distributing traffic. However, the relocation (moving) of the BS is a difficult decision as it should have the ability to increase the network lifetime and BS anonymity. When the BS starts moving, the nodes are not aware about the new position of the BS and hence there is packet loss in this interval. The retransmission of the lost packets will consume extra energy. To overcome this problem, two algorithms AERO and free-AERO have been proposed in the literature [14]. These algorithms have highlighted the importance of the BS relocation in order to increase the lifetime and anonymity (BS) of the network. But AERO and free-AERO algorithms have assumed that there is no packet transmission until the BS is reached at its new position and the energy consumed during this interval is not added in total energy consumption (since many packets may be transmitted towards the old BS position and the energy consumption to recover or retransmit these packets is not considered). In the proposed approach, some special nodes are introduced in order to provide the location of the mobile BS to each source node continuously. Now each source node is able to transmit its data to the BS without any interruption. Therefore, the packet loss probability during the

BS movement is reduced. In addition, this approach is also able to increase the anonymity of the BS by producing the similar hot spot regions in the different parts of the network.

This paper is organized as follows: In Section 2 work related to BS protection is discussed. Detail of the proposed scheme is given in Section 3. The simulation results and performance evaluation of the proposed scheme is presented in Section 4. Section 5 concludes the paper.

II. Related BS Privacy Protection Works

Earlier wireless sensor network research had only focused towards the energy saving. But with the passage of time, the secrecy of the data transmission has become the first priority. The privacy protection in WSNs is a challenging issue as it uses wireless radio for transmission/reception of the data. In [2] authors have categorized the privacy protection into different types. But data privacy and privacy context are mostly applied in the WSNs. Data-oriented privacy protection provides privacy for the data content. Data contains information as well as queries and received acknowledgments. For example, when a WSN is applied for monitoring the patient in a hospital, the sensed information includes patient's heartbeat, blood pressure, sugar level and body temperature. If this information is intercepted by malicious attackers who are interested in the patient, the safety of the patient can be in peril.

Malicious attackers are divided into two types. The first type of attackers eavesdrops on a radio and they are called as outside enemy. This type of attackers can be blocked using cryptographic schemes. The second type of attackers cracks sensor nodes for receiving the information and they are called as internal enemy. The cryptographic techniques fail to stop such type of attacks.

Context-oriented privacy protection intercepts the oppression of the WSNs characteristics from the attackers. These characteristics comprise BS location and time of the events. The WSN comprises important devices like BS, cluster head, source nodes that require privacy protection (hiding their positions and event happening time) in order to maintain the secrecy of the network. The existing research has concentrated on protection against external enemies. Enemies can be external or internal depend upon their ability or power to analyze a network. External enemies are very powerful and are able to analyze a wider region or a complete network. On the other hand, internal enemies are only able to analyze small span and they are less powerful than external enemies. The BS is used for collecting the information from all sensor nodes and also acts as a gateway to the external network. Generally, all security schemes consider that the BS is secure for simplifying the analysis [12]. Therefore, it becomes necessary to hide the BS from the enemies.

Many approaches have been proposed to resolve the hot spot problem near the static BS. But mobile sink is proved to more energy efficient and it also improves the security of the BS [15]. A mobile sink and tree-based topology had overcome the hot spot problem [15]. The experimental results demonstrate that mobile BS is better than static BS for increasing anonymity of BS. The proposed scheme have also used a mobile BS with some special nodes (SP) in order to overcome the hot spot and BS anonymity problem. The brief discussion regarding proposed scheme is given in the next section.

III. Proposed Mobile BS Scheme

A. Model for Analyzing BS Anonymity

A WSN follows many to one traffic pattern in which all nodes send data to the BS. Therefore, traffic near the BS region is large compared to other parts of the network. The attackers divide the network into many squared cells and start analyzing the traffic intensity in each cell (Fig. 1). The cell which has maximum traffic intensity, the probability of finding the BS is also large in that cell.

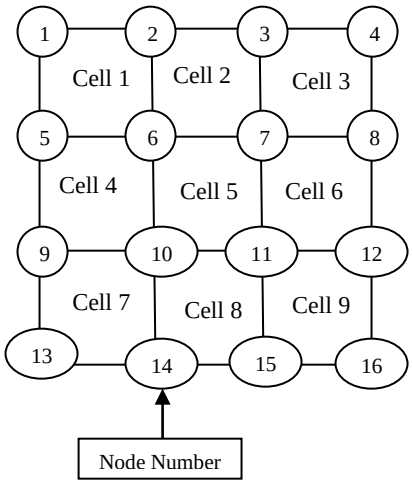

Fig. 1. Observing packet transmission in the network.

B. Mathematical Model of Entropy

In 1948, Shannon proposed a mathematical model (entropy method) for analyzing the randomness in a network [16]. This model is referred by many researchers to find the anonymity [4], [5]. The entropy measure shows the traffic distribution in the network. An attacker can split networks into N cells and start sensing each cell independently for the traffic analysis. After a time span, the attacker provides each cell a probability P_i, where i = 0,1,2,…., N-1, which indicates the chance of BS present in the i-th cell. An entropy value H(x) can be calculated by the equation given in [17].

$$H(x) = -\sum_{i=0}^{N-1} P_i \times [\log_2(p_i)] \quad (1)$$

At initial point, the probability of finding the BS is 1/N and therefore, maximum entropy H_{max} can be attained by substituting P_i with 1/N in (1).

$$H_{\max}(x) = -\sum_{i=0}^{N-1} 1/N \times [\log_2(1/N)] \quad (2)$$

To calculate the anonymity, we combined (1) and (2) which is considered as the ratio degree in this paper.

$$\text{Ratio Degree} = \frac{H(x)}{H\max(x)} \quad (3)$$

C. Determining BS Anonymity using the Entropy Method

This study assumes an external attacker who can eavesdrop on the whole network and deduce the BS location from the packets reached at each cell. After analyzing the network for some time, the attacker calculates the total number of packets transmitted in the network and the number of packets reached at i-th cell. The BS anonymity can be calculated using (1) and given in (4) and (5).

$$H(x) = -\sum_{i=0}^{N-1} \frac{p_i}{M} \times \left[\log_2 \left(\frac{p_i}{M} \right) \right] \quad (4)$$

$$H(x)/H_{\max}(x) = -\sum_{i=0}^{N-1} \frac{p_i}{M} \times \left[\log_2 \left(\frac{P_i}{M} \right) \right] \Big/ \log_2 (N) \quad (5)$$

Where, M is the total number of packets transmitted in the whole network and the P_i represents the number of packets transmitted from i-th cell.

D. Increasing BS Anonymity using Mobile Sink (Proposed Scheme)

If the BS is static, the attackers can easily estimate the position of BS after the WSN operation has been run for a short time. In this paper, we assume that the attacker can analyze the packet transmission information using eavesdrop method. A static BS in WSN can be easily identified by attackers because high intensity traffic shows the vicinity of the BS. Therefore, it is observed that a mobile BS will be beneficial to minimize the finding probability of the BS. An external (distant) user cannot detect the motion and direction of the mobile sink. Hence, mobile BS can be utilized to increase the randomness of BS in the sensing field. Some crucial problems like BS position advertisement and designing of new routing paths to all nodes arose when mobile BS is used in the WSNs. If BS floods location update messages regularly to the nodes, the most of the energy of these nodes will be consumed in order to complete this process. This reduces the network lifetime and hence it becomes compulsory to select a method which provides the BS location update in an energy-efficient way. To fulfill this requirement, we propose a novel algorithm in which the location of the mobile BS is stored in some specific nodes called as special nodes (SP) (Fig. 2) and all the nodes contact SP nodes for knowing the BS location. These SP nodes are also utilized to generate the hot spot in the network, which increases the BS anonymity.

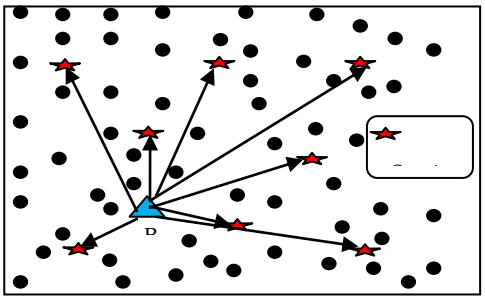

Fig. 2. A WSN scenario for the proposed method.

a) Selection of special nodes

After dispersing the nodes in the sensing field, the process for the selection of SP nodes is started. The SP node selection process is divided into two steps. In the first step, each node gathers some important information like distance from the sink and the number of neighboring nodes (n_i). Each node counts its neighboring nodes in a defined radius (RSP). The RSP radius decides the number of SP nodes required for the operation (large RSP value provides the small numbers of SP nodes and vice-versa). This information is shared within the nodes and now each node calculates its degree ($deg_i = n_i$ / max [n_1, n_2, n_3,…….n_N]). The maximum number of neighboring nodes is the first condition in order to check the suitability of the node to become a SP node. These suitable nodes are called as candidates for SP nodes. The probability of a node (P_i) to become the candidate for SP node is given by (6).

$$p_i = \begin{cases} \dfrac{(E_{resi} \times \deg_i)}{p_{total}} & E_{resi} \geq E_{avg}(1-\mu) \\ 0 & \text{else} \end{cases} \quad (6)$$

$$p_{total} = E_{avg} \times \sum_N \frac{\deg_i}{2k_{SP}} \quad (7)$$

Where,

In the above mentioned equation, K_{sp} is the required number of SP nodes to perform the operation and K_{sp} is equal to the $\sqrt{N}$ [17]. E_{avg} is the average residual energy of the nodes in the ongoing round which is calculated by the SP nodes in the last round. E_{resi} is the residual energy of i-th node and μ is a number between 0 and 1. μ is fixed to 0.8 in the proposed technique. This helps to stop the participation of low energy nodes in the SP nodes selection process. The (6) shows that the value of P_i (probability to become a SP node) mainly depends upon the node degree (deg_i) because residual of many nodes may be similar but the number of neighboring nodes for each node is different. The nodes, which have calculated its p_i value, generate a random number between 0 and 1. If the generated random number is less than the p_i value, the node considers itself a suitable candidate for the SP node selection. Now all such candidates announce its role to all other candidates by broadcasting a SP-CANDIDATE message in a particular order. This message contains the information of the sender like ID, residual energy and node degree. After receiving this message, each candidate calculates its distance from the sender and counts the number of those candidates who have already announced the candidacy for the SP role. The eligible candidates which have higher candidate density in their vicinity are removed to gain appropriate distribution (see, Fig. 3). For this purpose, all candidates score once and the candidate who has scored minimum is removed from the competition. This score is actually the multiplication of its distances from the other candidates. Hence, the dense candidates will score low as compared to those candidates who are situated at large distances. The procedure is stopped when the remaining number of candidates becomes equal to the needed number of candidates (K_{sp}).

b) Selection of special nodes

When each SP node advertises its role in the network, the neighboring nodes receive these messages from SP nodes. Now each node checks the RSSI value or number of hops for the received message and based upon these parameters, every node decides its special node. Each node replies to a specific SP node by sending a joining request message. The SP node acknowledges for the request and now the node becomes the member of a SP node. Each source node sends a BS position query message to its special node and SP node replies with the current position of the mobile BS. Now the source node has the information of the BS and now it is able to transmit data to the BS using greedy geographic routing [18].

1. **While** Low energy nodes > 0 **do**
2. **If** $|K_{CSP}| > K_{SP}$ **then**
3. Remove a candidate of SP node (K_{CSP}) which has the lowest energy;
4. **End**
5. Low energy nodes ← Low energy nodes – 1;
6. **End while**
7. **While** $|K_{CSP}| > K_{SP}$ **do**
8. **for** i = 1 to $|K_{CSP}|$ **do**
9. $Score_i = \prod_{Kcsp}^{i \neq j} d(i, j)$;
10. **end**
11. Find node i which have lowest $Score_i = \min\{ score_1, score_2, \ldots\ldots score_{Ksp} \}$;
12. Delete i-th node from the K_{CSP} list;
13. Score ← 0;
14. **end while**
15. $K_{SP} \leftarrow K_{CSP}$;
16. **Return** K_{SP} ;

Where d(i,j) is the Euclidean distance between i-th and j-th node. K_{CSP} candidates for SP node selection. K_{SP} needed number of SP nodes.

Fig. 3. SP node selection procedure.

c) Increasing BS anonymity and providing fresh location of the mobile sink to SP nodes

Each SP node sends a message to the BS which include their ID's , locations and role in the network. The BS replies to these nodes with its fresh location. Each SP node stores this message and compares its distance from the BS. If the distance between SP node and the sink node is greater than a threshold value (half of the network length), the SP node transmits a fake message to its member nodes and generates a hot spot in its vicinity. The SP node which has distance less than the threshold distance will not generate any traffic. In this way, many hot spots are generated in different parts of the network and it makes the traffic uniform in the network. The attacker eavesdrops the different regions and it becomes difficult for him to find the real BS region. This type of traffic pattern generates the possibility of finding the BS in each region equally and hence it becomes very difficult for the attackers know about the exact BS location. This approach increases the number of steps required to search the BS location and thus increases the BS anonymity.

d) GSAT Test

GSAT test executes a greedy local search for the evaluation of the BS anonymity [10]. GSAT test is used to measure the number of steps required to find the BS location. An attacker initially analyzes the traffic at a random location and finds the flow of the traffic in the nearby region. After analyzing for some time, the attacker detects a node which is transmitting/receiving the packets most frequently. The attacker continuously monitors that node until he/she is able to get the information regarding the BS position. The number of nodes/areas that changed by the attacker for monitoring before getting the BS location is called as GSAT score. This score represents the effort required to get the BS position and a large score provides the more BS anonymity in the network.

IV. Simulation Parameters and Performance Metrics

A. Simulation Parameters and Setup

The various parameters used for performing the simulation are mentioned in Table 1. The BS moves randomly in the network. The network is divided into 3×3 and 5×5 cells. The number of nodes deployed is 100 and 256 respectively. These nodes are uniformly distributed in the network. Initially, the BS starts moving from the center of the network. The events are randomly generated with a frequency of one hundred events per minute.

B. Performance Metrics

The first performance metrics is the anonymity of the BS and it is observed with respect to the moving time of the BS.

To estimate the anonymity, the entropy of the network is calculated after a certain interval of time and this information is used to show the variation in the anonymity of the BS.

The second performance metrics is the network lifetime and observed with respect to the moving time of the BS. The number of random events generated (without any node died) is considered to evaluate the network lifetime.

V. Simulation Results and Discussion

A. Results for 3×3 Network Area (Case 1)

The BS anonymity for the static BS case (BS placed in the central region of the network) is shown in Fig. 4. The results show that the anonymity of BS is decreasing with the passage of the time because the traffic near the BS region is increasing as compared to the other parts of the network. To determine the effect of the proposed technique, the anonymity and network lifetime is examined at different time intervals (30 and 60 minutes).

Fig. 5 and 6 showing that the anonymity of the proposed techniques is better than AERO because it is able to distribute the traffic uniformly. In AERO, the BS is relocated to a new position after a fixed time interval and shift traffic to different regions. AERO provides good anonymity (0.99) when it relocates BS more frequently, but due to the continuous motion of the BS in the proposed technique it provides better anonymity (0.995) than AERO. When the relocation of BS is very frequent in AERO, a large number of packets are lost because until the BS moves to the new position no data packet is able to reach its destination (BS).This deficiency is overcome in the proposed technique. Fig. 7 shows the effect of a randomly roamed BS on the network lifetime. For fixed BS, the first node gets out of the energy after performing 12701 randomly generated events and AERO performs 50336, 34931 and 27909 randomly generated events (when BS is relocated after 30, 60 and 90 minutes, respectively). On the other hand, the proposed technique performs 47,498 randomly generated events (BS is moving continuously). The network lifetime of the proposed approach is less than AERO because it utilizes some energy in the location update of the mobile BS and also consumed some energy for generating hot spots at the different regions to maintain the anonymity of BS in the network. We may say that the proposed technique provides connectivity of the mobile BS with each sensor node through special nodes (SP) and increases anonymity of the BS as compared to AERO approach.

B. Results for 5×5 Network Area (Case 2)

This subsection includes the experimental results for 5×5 network area. Fig. 8 shows that the results of 5×5 network area are different from the results obtained in the 3×3 network area. The anonymity of the static BS decreases steadily at the initial stage of the operation, but it may instantly decrease in the later stage. This may happen because in a large area network the events may generate at the distant places and the traffic near the BS region may indicate the position of the BS.

Fig. 9 and 10 shows the impact of mobile BS on the anonymity of BS for the proposed technique and shows the comparison with AERO techniques. The anonymity of the proposed technique is better than the AERO when the relocation time interval of the BS is 30 and 60 minutes.

Fig. 11 shows the effect of mobile BS on the network lifetime. For the static BS case, the first node dies after 12,626 events generated in the given network. AERO provides maximum of 57,098 events when BS relocates to a new position after each 30 minutes of time and the network lifetime of AERO is decreasing continuously with the increase in the relocation time of the BS. On the other hand, the proposed technique provides 56,765 events generation before dying the first node in the network. The proposed technique provides low network lifetime than AERO because the special nodes consume some additional energy for providing the mobile BS location updates to the source nodes. The proposed technique does not provide any packet loss while the BS is moving. The results show that for a larger network area (compared to 3×3 cell) the network lifetime is enhanced by the proposed approach.

C. GSAT Test Results

Fig. 12 shows that the mobile BS increases the efforts of the attackers for searching the BS location. The above results show that a large network area provides more security for the BS. In a 3×3 network area the attacker is able to find the exact position of the BS in 535 steps using the AERO technique (relocation of the sink is after every 30 minutes). For the proposed technique, the attacker needs 683 steps for the confirmation of the BS position.

In a 5×5 network area, the attacker needs 1178 steps using proposed approach and it needs 980 steps using the AERO approach to confirm the location of the BS. Hence the proposed technique gives better anonymity than AERO.

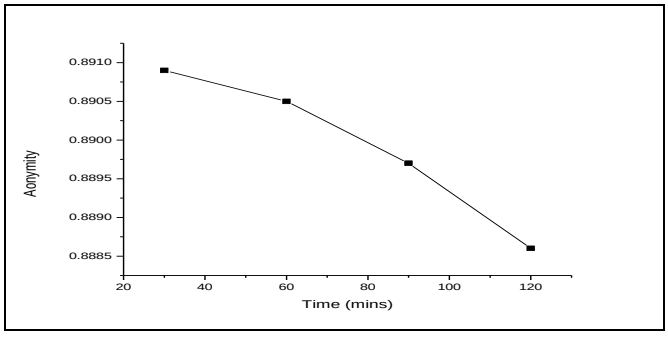

Fig. 4. Anonymity with respect to for fixed BS (3×3).

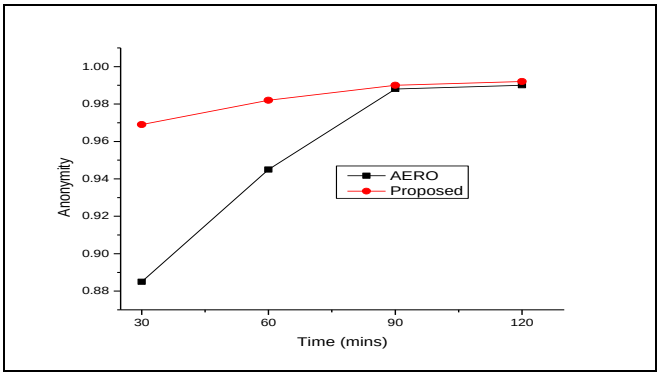

Fig. 5. Anonymity with moving time of the BS (after each 30 minutes).

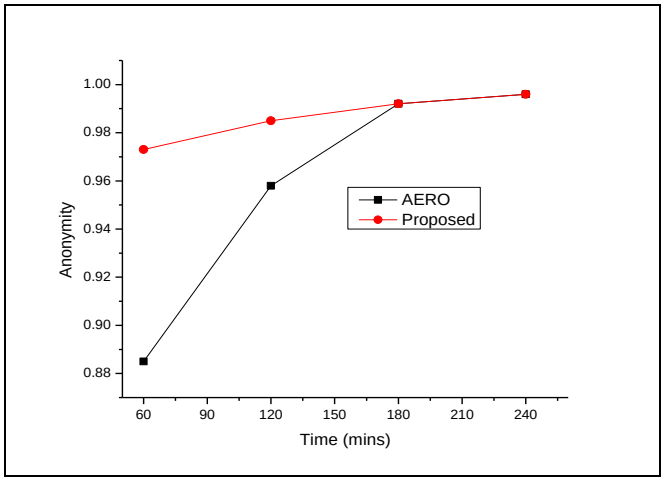

Fig. 6. Anonymity with moving BS (after every 60 minutes).

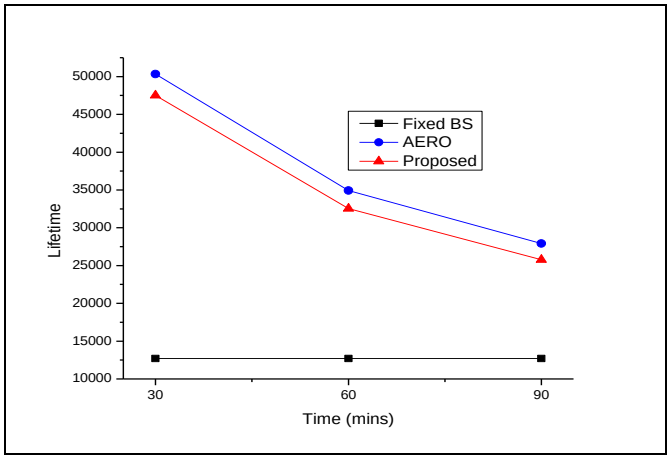

Fig. 7. Network lifetime with moving time of the BS (3×3).

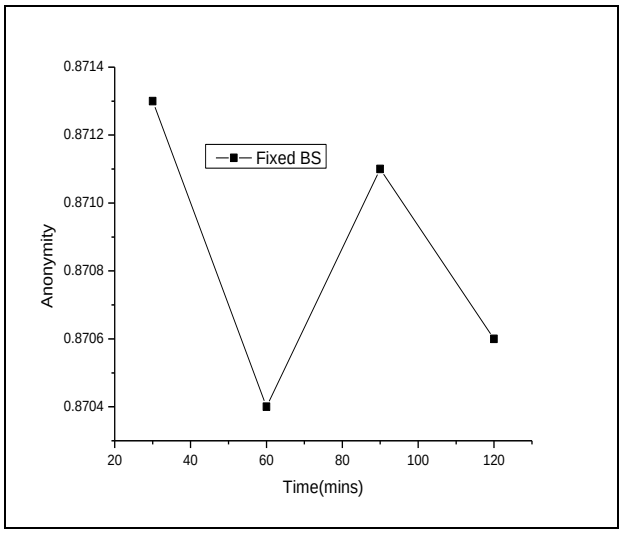

Fig. 8. Anonymity with respect to for fixed BS (5×5).

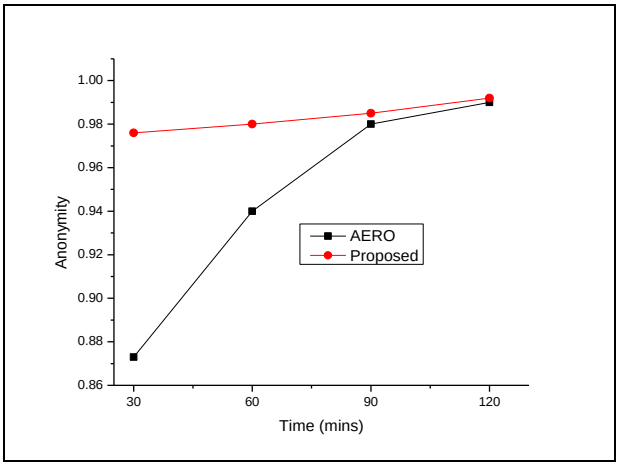

Fig. 9. Anonymity with respect to mobile BS (after every 30 minutes for 5×5).

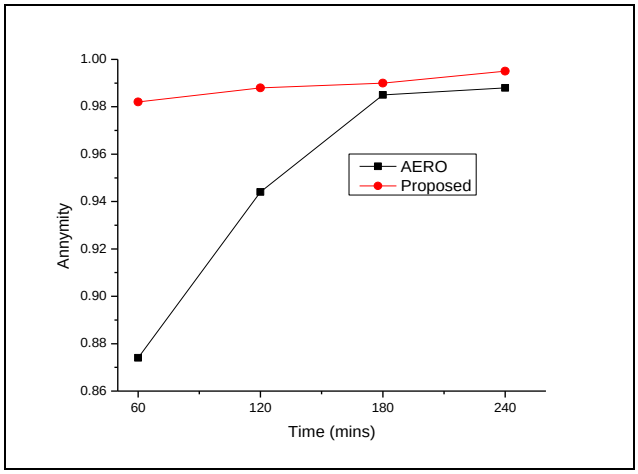

Fig. 10. Anonymity with respect to moving BS (after every 60 minutes for 5×5).

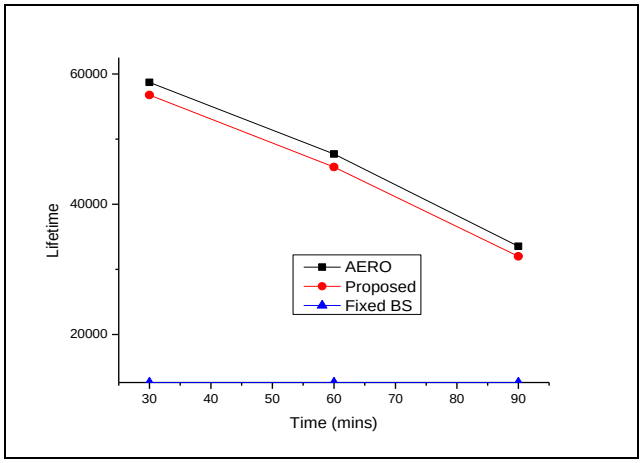

Fig. 11. Network lifetime with moving BS (5×5).

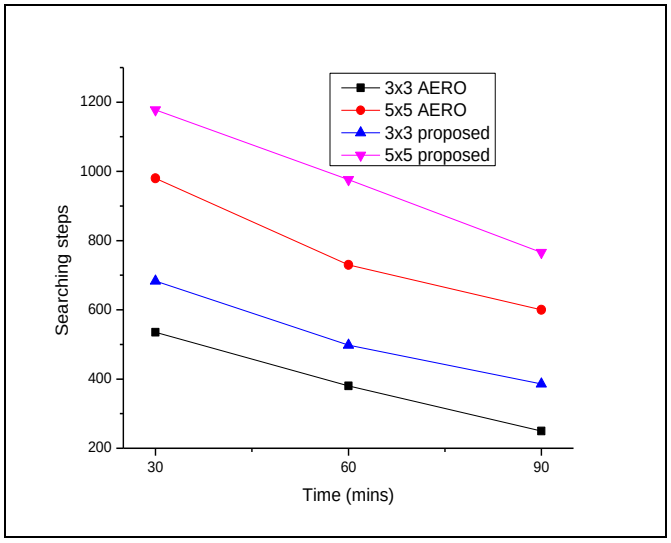

Fig. 12. Seacrhing steps with respect to time.

TABLE I. SIMULATION PARAMETERS

Parameters	**Values**
Network grid	3×3, 5×5 (cells)
Number of nodes	100,256
Initial BS location	Center point of the area
Events occur	Random
Frequency of events	100 (per minute)
Initial energy of the nodes	8 J
Packet size	128 (byte/packet)
Energy needs to transmit a packet	0.0006341 J
Energy needs to receive a packet	0.0006341 J
RSP	30, 50 m

VI. CONCLUSIONS

The proposed technique has used a randomly roamed BS to increase the anonymity and the SP nodes are proposed to provide the location of the mobile BS to each source node. These location updates about BS avoids the packet loss while the BS is moving and provide a continuous data transmission in the network. The SP nodes also generate hot spot regions in different parts of the network and hence increase the BS anonymity as compared to AERO. The network lifetime of the proposed technique is four times better than the fixed BS approach and comparable to the AERO approach. The results show that a large (5×5) network span provides better anonymity and network lifetime as compared to the smaller one (3×3) for the proposed technique.

REFERENCES

[1] Banerjee, Indrajit, Prasenjit Chanak, Hafizur Rahaman, and Tuhina Samanta. “Effective fault detection and routing scheme for wireless sensor networks.” Computers & Electrical Engineering 40.2, pp. 291-306, 2014.

[2] Raji, Fatemeh, and B. Tork Ladani. “Anonymity and security for autonomous mobile agents.” IET information security 4, no. 4, pp. 397-410, 2010.

[3] Gu, Y., Ren, F., Ji, Y. and Li, J. “The evolution of sink mobility management in wireless sensor networks: A survey.” IEEE communications surveys and tutorials no. 18(1), pp. 507-524, 2016.

[4] Acharya, Uday, and Mohamed Younis. “Increasing base-station anonymity in wireless sensor networks.” Ad Hoc Networks 8, no. 8, pp. 791-809, 2010.

[5] Deng, Jing, Richard Han, and Shivakant Mishra. “Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks.” Pervasive and Mobile Computing 2, no. 2, pp. 159-186, 2006.

[6] Nezhad, Alireza A., Ali Miri, and Dimitris Makrakis. “Location privacy and anonymity preserving routing for wireless sensor networks.” Computer Networks 52, no. 18, pp. 3433-3452, 2008.

[7] Wang, Haodong, Bo Sheng, and Qun Li. “Privacy-aware routing in sensor networks.” Computer Networks 53, no. 9, pp. 1512-1529, 2009.

[8] Pfitzmann, Andreas, and Marit Hansen. “A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.” 2010.

[9] Deng, Jing, Richard Han, and Shivakant Mishra. “Enhancing base station security in wireless sensor networks.” Technical Report CU-CS-951-03, Department of Computer Science, University of Colorado, 2003.

[10] Deng, Jing, Richard Han, and Shivakant Mishra. “Countermeasures against traffic analysis attacks in wireless sensor networks.” 2005 first IEEE International Conference Security and Privacy for Emerging Areas in Communications Networks,. pp. 113-126. 2005.

[11] Jian, Y., Chen, S., Zhang, Z., & Zhang, L. (2007, May). “Protecting receiver-location privacy in wireless sensor networks,” 2007, 26th IEEE International Conference on Computer Communications, pp. 1955-1963

[12] Basagni, Stefano, et al. “Controlled sink mobility for prolonging wireless sensor networks lifetime.” Wireless Networks, 14.6, pp. 831-858, 2008.

[13] Yang, Yinying, Mirela I. Fonoage, and Mihaela Cardei. “Improving network lifetime with mobile wireless sensor networks.” Computer communications, Vol.3, no. 4, pp. 409-419, 2010.

[14] Chen, Joy Iong-Zong, and Chu-Hsing Lin. “Algorithms for promoting anonymity of BS and for prolonging network lifetime of WSN.” Peer-to-Peer Networking and Applications 7, no. 4 , pp. 710-722, 2014.

[15] Kim, Hyung Seok, Tarek F. Abdelzaher, and Wook Hyun Kwon. “Minimum-energy asynchronous dissemination to mobile sinks in wireless sensor networks.” 2003 1st international conference on Embedded networked sensor systems, pp. 193-204.

[16] Shannon, Claude E. “A mathematical theory of communication, Part I, Part II.” Bell Syst. Tech. J. 27 (1948): 623-656.

[17] Chan, Tung-Jung, Ching-Mu Chen, Yung-Fa Huang, Jen-Yung Lin, and Tair-Rong Chen. “Optimal cluster number selection in ad-hoc wireless sensor networks.” WSEAS Transactions on Communications 7, no. 8, pp. 837-846, 2008.

[18] Tunca, Can, Sinan Isik, M. Yunus Donmez, and Cem Ersoy. “Distributed mobile sink routing for wireless sensor networks: A survey.” IEEE communications surveys & tutorials 16, no. 2, pp. 877-897,2014.