International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 14101-14107

Novel Resource-Quality Aware Algorithm for Privacy- Preserving Location Monitoring in Wireless Sensor Networks

Soumyasri S M
Assistant Professor, Department of Computer Science,
Sri Dharmasthala Manjunatheshwara College (SDM College), Ujire,
Dakshina Kannada, Karnataka, India.
Orcid Id: 0000-0002-6597-4119

Dr. Rajkiran Ballal
Principal & Professor, Department of Electrical & Electronics Engineering,
Mangalore Marine College & Technology, Padil Padavu, Kuppepodavu Post,
Mangalore, Karanataka, India.
Orcid Id: 0000-0002-4209-0206

Abstract

The ultimate development in communication results in ever increasing application areas of the wireless sensor network. However, its need in the confidential area is still oscillating objective due to the security threats. The personal location identification is a major aspect in these aconfidential applications. The privacy threats by the untrusted server affect the individuals being monitored. To provide the solution for this problem this paper proposes a novel resource-quality aware algorithm. This technique is suitable for the system which is having threatened resources and requires high accuracy. The k-Nearest Neighbour methodology is included in the proposed technique for reducing the energy consumption of sensor nodes. Thus this method provides three pros such as object identification with reduced computational complexity, quality location estimation and power consumption reduction. The exemplification of proposed methodology has done in the result and discussion part with the parameters like communication cost, attack model error, cloaked area and computational cost.

Keywords: Privacy preserving location monitoring, wireless sensor network, k nearest neighbor, cloaked area, energy consumption and computational cost.

INTRODUCTION

The development of wireless sensor network (WSN) technologies makes its application to a broader range and in different areas. The major area of implementation services that is includes army and navy. Hence the application relies on the surveillance and vigilance [1]. The information of physical location is much more important in some of the applications of WSN [2]. Location monitoring is coming under the security issues in wireless sensor network. The privacy breach of location information affects the confidential data traffic in the network. Most probably the existing literature works have discussed the techniques for routing and data gathering is not considering security as an issue [3]. If the privacy attack may be by an intruder, then he targets the primary or intermediate nodes for extracting the information [4].

The attacks on the network are separated based on two kinds they are, local-eaves dropping model and the global eavesdropping model. In the first type the attacker can monitor communication among the sensor nodes, and in the latter, the traffic is monitored by the attacker [5]. The security attacks in the networks are in the form of modification, interruption and construction of unnecessary data with original information [3]. The application in WSN relies only on the reliable base stations (BS). Usually, the data transfer among the sensor nodes deployed in the network is based on short-range radio communication. For that, the BS is considered as a well-established one with necessary equipment [6].

The location identification of an object is reported to the server is carried out by the sensor nodes deployed in the sensor network. These are known as identity sensors, and unfortunately, it creates privacy threats. For mitigating this problem, aggregate location information is introduced. The accuracy of the location identification is getting importance in the current location-aware techniques [7]-[11]. In the location monitoring, the privacy preservation is depends upon an analysis of traffic. Sometimes the opponent or the adversary may destroy the location identity of critical nodes by network traffic analysis [12].

The opponent with better knowledge about the system can able to overcome the solution methodologies. It arranges its sensor nodes to sense the target network activities [13]. The hostile and confidential environments need the location preservation as a higher amount. The network traffic analysis is overcoming with by protection schemes as per today's security requirement.

In [14] the aggregation of user data is conducted in the presence of untrusted aggregator based on homomorphic encryption and information hiding is explained. The literature [15] discussed the sink node anonymity for the sensor networks. There exists ample scope for future expansion of existing research works [16]. Hence the below points explain the novelties of this work.

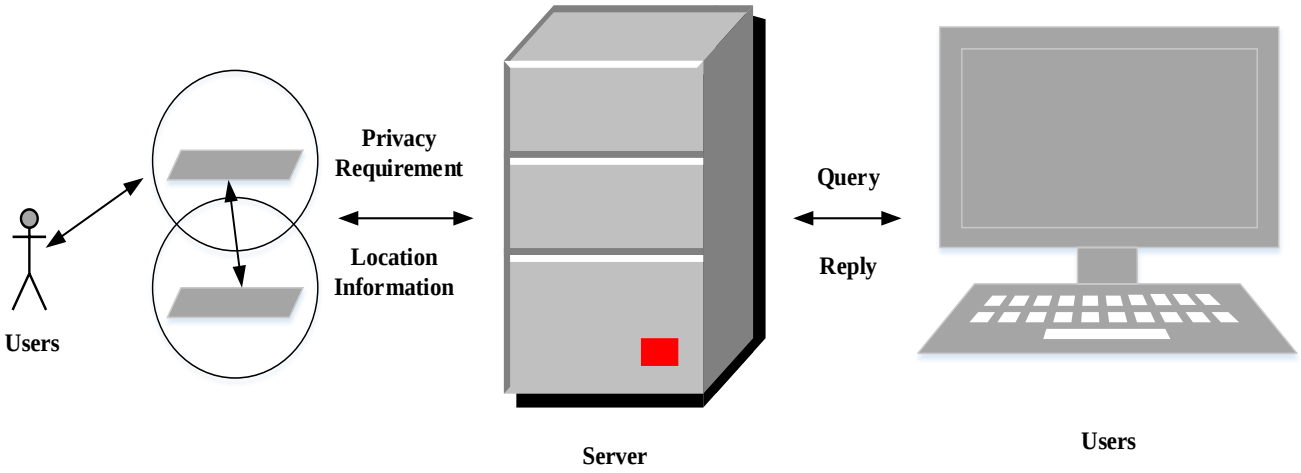

Fig 1: Architecture of network with users

1) The proposed resource-quality aware algorithm is suitable for the system with lower resources for communication and greatest need of accuracy.

2) Further, this work provides particular attention to the energy consumption reduction whereas the sensor nodes broadcasting the information.

SYSTEM MODEL

The major bodies of the considered network are a server, sensor node and users. The below figure is represents the planning of the proposed work with major bodies.

Problem Definition

Consider a set of sensor nodes with indication $S_1, S_2, \ldots\ldots, S_N$ having the sensing area $A_1, A_2, \ldots\ldots, A_N$. In the sensing area, it is considered $O_1, O_2, \ldots\ldots, O_M$ number of objects is presented. The sensor nodes are defined with anonymity level, k and the aggregate location of each sensor node is $A_i = (RA_i, Number_i)$. RA_i is defined as the rectangular area which contains the sensing area of the set of sensor nodes S_i and $Number_i$ is the number of objects present in the sensing area. The spatial histogram technique gives the query response. In general, the normal resource-aware and quality-aware algorithms are providing k anonymity privacy but which are suitable for the systems having rare computational sources and accuracy required applications.

In this work, the network topology is not assumed, but energy consumption between the sensor nodes whereas broadcasting the information is considered.

a. Major entities

Server

It provides a reply to the queries in the network based on the object distribution of each sensor node. This is identified by the spatial histogram, and provides the cumulative location of the sensor node and the number of objects presented in the sensing area of the sensor node.

Sensor nodes

The node deployed in the environment has the responsibility of finding a number of aggregate locations of objects presented in its sensing area and distorting the space into a cloaked area. This area is described with at least M number of objects.

Users

The valid users only can able to send range queries to the network through the server or via sensor nodes. The spatial histogram is used for answering the range queries to the server.

PROPOSED ALGORITHM FOR LOCATION IDENTIFICATION

This title broadly explains the in-network novel resource-quality aware algorithm for identifying the location of objects which presents in the sensing area of a sensor node and report to the server at every reporting period. This combined resource-quality algorithm considers the energy consumption while broadcasting the messages between the sensor nodes.

The steps included in the algorithm are,

1) Broadcast

2) Search space

3) Minimal cloaked area step

4) Validation

Algorithmic structure:

Resource-quality aware (Integer *k* , Sensor nodes M, List R)

Step 1: The broadcast step

Evaluate nearest neighbours

Send a message with identity of nodes

If Receive a message from a peer with identity

Then Add the message to Peer List

If The node has found an adequate number of objects

Then Send a notification message to neighbours

End if

If The adequate objects are not found

Then Forward the message to neighbours

End if

End if

Step 2: The search space step

Current minimum cloaked area as initial solution

Collect the information of the peers located in search space S

Step 3: The minimal cloaked area step

Add each peer located in S to X [1] as an item

Add M to each item set in X [1] as the first item

For i = 1; i ≤ M; i ++ do

For each item set Y = {s1,..., si+1} in X[i] do

If Area (MBR(Y)) < Area (current minimum cloaked area) then

If N(MBR(Y)) ≥ k then

Current min cloaked area ← {Y}

Remove S from X[i]

Perform firefly optimization

End if

End for

Area ← a minimum bounding rectangle of current minimum cloaked area

Step 4: The validation step

If No containment relationship with Area and server

Then

Send (Area, M) to the peers within Area and the server

Else if M's sensing area is contained by some R 2 R then

Randomly select an R'€ R such that R'. Area contains m's sensing area

Send R' to the peers within R'. Area and the server

Else

Send Area with a cloaked M to the peers within Area and the server

End if

a. Broadcast step

In this step, the number of objects in the sensing area of a sensor node is verified by the broadcasting messages. The broadcasting message consists of the identity of a sensor node, rectangular area and a number of objects. This message is sent to its all of the neighbours. The message transformation to all of its neighbours considerably reduces the energy of the particular sensor node. Therefore we are utilising k-Nearest neighbour algorithm for identifying the exact neighbours and then reduction of energy consumption.

The k-Nearest neighbour algorithm counts the distance between the sensor nodes S_a *and* S_b . The distance evaluation is based on the lifetime of the nodes. The lifetime is evaluated by using the equation (1).

$$L_{node} = \frac{E_0}{E_i} \tag{1}$$

In (1) E_i is the energy consumption rate of i_{th} node.

The distance between the nodes is evaluated by the below formula (2).

$$Dis\tan ce(S_a, S_b) = \sqrt{\sum_{i=1}^{N}(L_{nodea} - L_{nodeb})^2} \tag{2}$$

$$NR = k - Min(dis\tan ce(S_i, S_{t\arg et})) \tag{3}$$

Thus the sensor nodes only send the object information to its identified neighbours. Therefore it reduces the transmission energy to the non-nearest nodes.

B. Search space

The search space step typically finds the minimum cloaked area of the sensing area. Because the network deployed with a large number of sensor nodes increases the cost of the computation of the minimal cloaked area. By finding the number of nearest neighbours, the area is evaluated. By taking this field as an initial solution, the search space step is developed.

Below figure illustrates the search space for sensor node S_1 and is computed. Let rectangular area is the area for input which has been calculated form the output of the nearest neighbor algorithm.

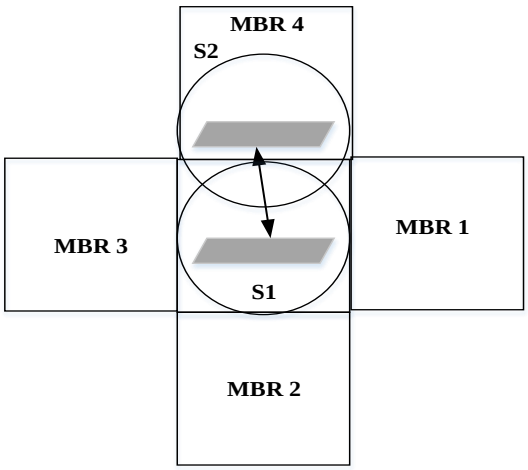

Figure 2: Search space evaluation

The two steps involved in the search space calculation are,

1) Identify the minimum bounding rectangle of the sensing area S_1. The major point in the calculation is the area should be in an irregular shape.
2) Evaluate minimum bound rectangle area by extending the edges of initial minimum bound rectangle.

*C. **Minimal cloaked area***

The minimal cloaked area evaluation relies on a set of peers located in the search space of a sensor node. This area compresses the whole network into it; therefore, the calculation is simple high. So the computational cost of this step is reduced based on metaheuristic optimization algorithm. In the existing literature, this part is explained with two optimization algorithms. However, which considers the minimum bounded rectangle of four sensor nodes is equalised with two nodes. To avoid this flaw we insist optimization algorithm here to reduce the computational cost. The Firefly optimization is used here for evaluating the reduced computational cost.

Firefly Algorithm

Three major rules are used in the Firefly optimization based on the flashing characteristics of the fireflies. The three characteristics are,

- All fireflies are assumed as same gender, and then only the less bright fireflies are moving towards more fascinating and brighter fireflies regardless of their gender.
- The brightness is proportional to light intensity and is proportional to attractiveness.
- The brightness of a firefly is estimated by the objective function of the given problem. If the objective function is a minimization problem, then the light intensity is inversely proportional to the objective function.

The objective function is estimated based on the equation (4).

$$objective = \min(computational\cos t) \qquad (4)$$

(i)Attractiveness (Brightness)

The attractiveness varies with the distance or space between the fireflies can be defined as,

$$\theta = \theta_0 e^{-\gamma r^2} \qquad (5)$$

Where θ_0 is the attractiveness or brightness at r = 0.

(ii)Distance

The distance between the two fireflies (sensor nodes) is calculated from the below relation. It is generally known as Cartesian distance.

$$r_{ij} = \left\| x_i - x_j \right\| \qquad (6)$$

Where i and j are the two fireflies and r_{ij} is the distance between the two.

(iii)Movement

The firefly with less brightness is a move towards the firefly with greater brightness than the movement of the firefly is described as,

$$x_i{}^t = x_i{}^{t-1} + \theta_0 e^{-\gamma r_{ij}{}^2}\left(x^t{}_j - x^t{}_i\right) + \alpha\varepsilon_i \qquad (7)$$

In (3) α *and* ε are constants. The three terms in the above relation denote some points. The first is the current term position of the firefly; the second term denotes the attractiveness of a firefly based on brightness, and the random movement of the firefly defined by the third term.

*D. **Validation step***

In this step, it is ensured that with the proposed algorithm the attacker not able to obtain the aggregate location of the objects in the sensing area of the sensor node.

SPATIAL HISTOGRAM FOR ESTIMATING THE LOCATION OF OBJECTS

The distribution of objects is evaluated by identifying the exact location of the sensor nodes which is done by the spatial histogram. It helps the server to provide the reply for the query of the users outside of the sensing area. The sensing area has defined by the sensor nodes using the aggregate location of neighbours estimated by k nearest neighbour algorithm.

Steps in the spatial histogram are defined as follow:

Step 1: Initialize the process by using the value of a number of

moving objects is distributed in a uniform manner in the network.

Step 2:The aggregate location of the object is grouped into a particular partition set.

Step 3:Update the aggregate location of objects for every partition created.

Step 4:Evaluate the estimation error for the partition.

Step 5:Evaluate the sum of estimation error.

Step 6:Update the histogram estimator by represented in [17].

ATTACKER MODEL

For the evaluation of proposed method, the system assumes an attacker model. It specifies the intrusion into the network for knowing the location details of the objects. It is assumed that the attacker has enough knowledge about the network [17].

RESULT AND DISCUSSION

The location monitoring with privacy preservation is a valuable and most required task in the today's wireless sensor network. This paper proposes and validates a novel resource-quality aware algorithm with k-nearest neighbour technique and firefly algorithm for preserving the privacy. Table 1 gives the parameter setting for the evaluation of the proposed method.

Table 1: Initial parameters

Description	Default Value
Number of nodes	Max: 100
Frequency range	0.5 Hz to 3 kHz
Histogram size	200 ×200
Query region size ratio	0.001 to 0.064
Neighboring technique	K-nearest neighbor
Object mobility speed	10m/s
K-anonymity level	20
Number of moving objects	5000

For evaluating the performance of the proposed algorithm, some of the metrics are considered. These are explained with graphical representation below.

a. Attack model error

This metric evaluates the flexibility of the system. It is processed through the estimation of relative error between the measured numbers of objects in the sensing area to the actual number of objects.

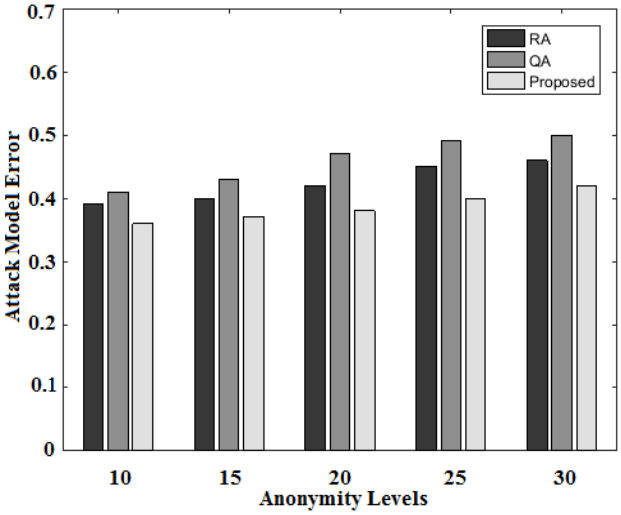

Figure 3: Attack model error

The proposed algorithm has compared with resource aware and quality aware algorithms for the evaluation and on anonymity levels. For the above graph, it is reported that the proposed method creates a larger cloaked area for strict anonymity levels. The number of objects gets greater, and therefore it reduces the error.

b. Communication cost

From this metric, the power consumption is also evaluated in the sensor nodes. This can find out by,

$$Communication\ \cos t = \frac{number\ of\ bytes\ sent}{reporting\ time} \qquad (8)$$

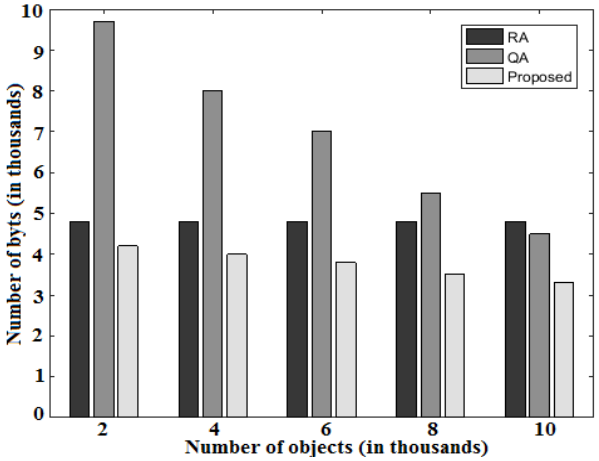

Figure 4: Communication cost

Here special attention is taken for power consumption reduction by avoiding the non-nearest nodes to the sender node. The graph indicates the reduction of communication cost and power consumption. In the existing algorithms, the quality-aware algorithm reduces the communication cost. The proposed

method outperforms significantly for reducing the cost of communication.

C. Cloaked area size

The aggregate locations of the objects are measured by the sensor nodes and further need to be reported to the server. This quality evaluated with cloaked area size. For the satisfaction of the privacy requirement, the algorithm generates smaller cloaked area for a large number of sensor nodes.

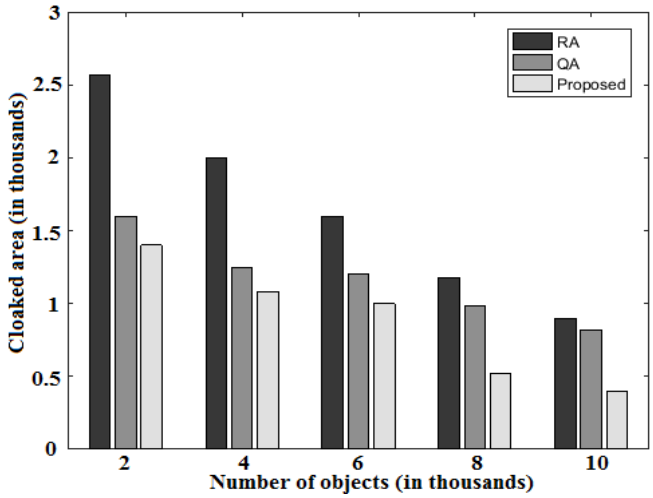

Figure 5: Cloaked area size

D.Query region size

The performance of the proposed method is validated by another measure query region size which is varied from 0.001 to 0.064. The query answer error has reduced whereas the query region size is increased. From this point, it concludes that the planned algorithm provides better location privacy for increased size of query region.

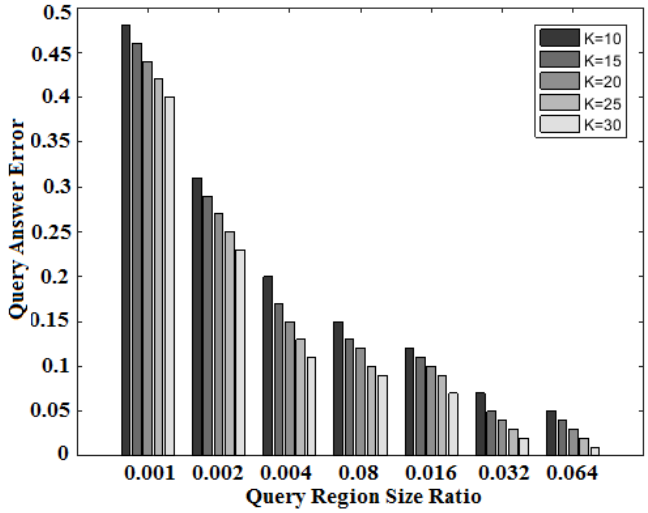

Figure 6: Query region size

E. Computational cost

The cost for computation has also reduced because this paper proposes a novel algorithm with reduced number of steps for computation. Thus it significantly reduces the computational cost.

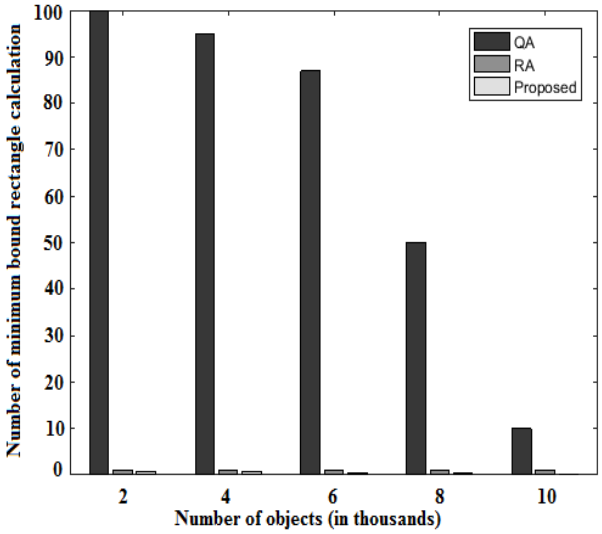

Figure 7: Computational cost

F. Accuracy

The location accuracy of the proposed method has compared with existing resource aware and quality aware algorithm. The proposed resource-quality algorithm is better regarding accuracy and provides 95%.

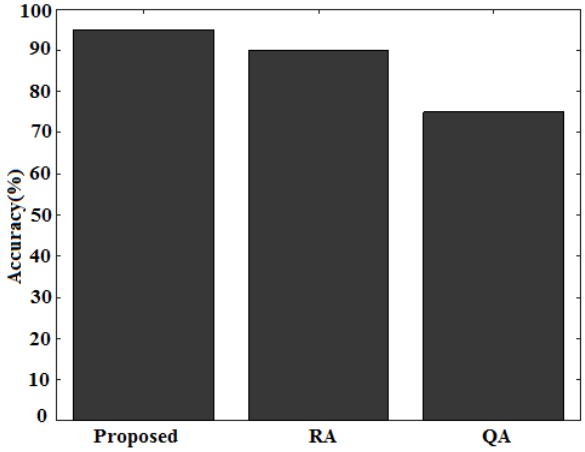

Fig 8: Accuracy

CONCLUSION

In this paper, a privacy-preserving location monitoring system for wireless sensor networks has proposed. For location preservation a novel resource-quality aware k-anonymity algorithm is proposed. The additional benefit added to this paper by considering the energy consumption fact of the sensor nodes.

The energy consumption has been reduced by evaluating the necessary nodes for broadcasting the identity messages. By the diminution of non-nearest nodes in the sensing area, the minimal cloaked area has also reduced. The resource-quality aware algorithm provides an accuracy of 95%. It is 5% more than that of the quality-aware algorithm in the existing literature and 20% more than that of existing resource aware algorithm. This algorithm simplifies its computational complexity by adding firefly algorithm for evaluating the minimal cloaked area.

REFERENCES

[1] Na Li, Nan Zhang , Saja l K . Das, and Bhavani Thuraisingham, " Privacy preservation in wireless sensor networks: A State -of- the- art survey ", Ad Hoc Networks, vol. 7, pp. 8, pp.1501-1514, April 2009.

[2] Yong Xi, Loren Schwiebert, and Weisong Shi, “Preserving Source location privacy in Monitoring - based wireless sensor Networks ”, In the proceedings of Parallel and Distributed Processing, no. 1, pp. 8, April 2006.

[3] Kirankumar B. Balavalad, Ajayakumar C K Atageri, Prithviraj S. Patil, and Basavaraj M. Angadi, "A Privacy- Preserving Location Monitoring System for WSNs with Blocking Misbehaving Users in Anonymity Networks", Journal of Advances in Computer Networks, vol. 2, no. 4, December 2014.

[4] Priti C. Shahare, and Nekita A. Chavhan, “ An Approach to Secure Sink node's Location Privacy in Wireless Sensor Networks”, In the proceedings of Communication Systems and Network Technologies, no. 1, pp. 748-751, April 2014.

[5] Mayank Raj, Na Li, Donggang Liu, Matthew Wright, and Sajal K Das, “ Using data mules to preserve source location privacy in Wireless Sensor Networks”, Pervasive and Mobile Computing, vol. 11, no. 1, pp. 244-260, 2014.

[6] C. Y. Chow, M. F .Mokbel, and T. He, “ A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks ”, IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp. 94-107, 2011.

[7] D.K.Lee, T .H. Kim, S.Y. Jeong, and S.J.Kang, “ A T Three - Tier Middleware Architecture Supporting Bidirectional Location Tracking of Numerous Mobile Nodes under Legacy WSN Environment”, Journal of Systems Architecture, vol. 57, no. 8, pp. 735- 748, 2011.

[8] J.Yick, B.Mukherjee, and D.Ghosal, “Wireless Sensor Network Survey”, Computer Networks, vol. 52, no. 12, pp. 2292-2330, 2008.

[9] H. Liu, H. Darabi, P.B anerjee, and J.Liu, “S urvey of Wireless Indoor Positioning Techniques and Systems”, IEEE Transactions on Systems, Man , and Cybernetics, Part C (Applications and Reviews), vol. 37, no. 6, pp. 1067-1080, 2007.

[10] L.Hu, and D. Evans, “ Localization for Mobile Sensor Networks”, In Proceedings of the Mobile Computing and Networking, no. 1, pp. 45-57, 2004.

[11] Y.Gu, A.Lo, and I.Niemegeers, “ A Survey of Indoor Positioning Systems for Wireless Personal Networks”, IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 13-32, 2009.

[12] B.Di Ying, D.Makrakis, and H.T.Mouftah, “Anti-Traffic Analysis Attack for Location Privacy in WSNs”, EURASIP Journal on Wireless Communications and Networking, no. 1, pp. 131, 2014.

[13] K.Mehta , D.Liu M, and M.Wright, “Location Privacy in Sensor Networks against a Global Eavesdropper”, IEEE International Conference on Sensor Networks, no. 1, pp. 314-323, 2007.

[14] L.Zhang, X. Wang, J.Lu, P.Li, and Z. Cai, “ An Efficient Privacy Preserving Data Aggregation Approach for Mobile Sensing ”, Security and Communication Networks, vol. 9, no. 16, pp. 3844-3853, 2016.

[15] E.C.H.Ngai, “ On Providing Sink Anonymity for Wireless Sensor Nettworks ”, Security and Communication Networks, vol. 9, no. 2, pp. 77-86, 2016.

[16] K. Bicakci, H. Gultekin, B. Tavli, and I.E. Bagci, “Maximizing Lifetime of Event- Unobservable Wireless Sensor Networks”, Computer Standards & Interfaces, vol. 3, no. 4, pp. 401-410, 2011.

[17] Chi - Yin Chow, Mohamed F. Mokbel, and Tian He, "A Privacy - preserving location monitoring system for wireless sensor networks ", IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp.94-107, 2011.