International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.017

Backward Random Walk based Source Location Protection in Sensor Network

Nisha
Department of Computer Science
Banaras Hindu University
Varanasi, India
nisha.singh17@bhu.ac.in

S.Suresh
Department of Computer Science
Banaras Hindu University
Varanasi, India
suresh.selvam@bhu.ac.in

Abstract—Wireless sensor networks has expanded its view of applications from personal domains to as wide as asset monitoring domain. Homogeneous sensor nodes are deployed to gather information and inform the base station. However, attackers are on a continuous look out to backtrack and gain the source node location. Location privacy preservation of the assets against passive attackers is crucial. In this paper, we develop a source location preservation scheme based on the combination of backward and forward random walk, to provide security irrespective of the source location in the network. The performance of the scheme is measured in terms of safety period, randomness of the routing length and capture rate of adversaries. Simulation results prove that the proposed scheme provides significant improvement in privacy strength and other metrics as compared to existing approaches.

Keywords—source location privacy, security, adversaries, backward routing, random walk, forward random walk.

I. Introduction

In the fast changing, network oriented digital world wireless sensor networks (WSN) [1,2] play a key role in information processing. WSN is formed by a collection of sensor nodes deployed within an area to sense, process and transmit information by communicating among each other. The information transmitted in packets through multiple hops is directed towards the base station or sink. Sink can be termed as the final destination for all the packets sent by the sensor nodes, Due to the good feasibility and self-organizing structure of sensor nodes, WSN is used for monitoring applications like animal conservation, military, smart buildings and offices etc. [3-5]. In applications where the assets being monitored holds a very high value in terms of their importance to nation or nature, it is essential to preserve their location information from falling in wrong hands.

Location privacy preservation [6,7] is essential requirement in WSN. It is divided into sink location privacy preservation [8] and source location privacy (SLP) preservation [9,10]. As sink is the final destination of all the packet transmission taking place in the network, a successful attack on the sink would render the security measures useless. But it must also be noted that attack on sink is an extremely difficult task as sink is heavily protected to be resistant against all possible attacks. Whereas source location privacy preservation is aimed at securing the location of the sensor nodes that is transmitting information about the presence of the assets. Attackers in order to remain hidden might not interfere with the communication process but carry out passive attacks like eavesdropping, backtracking, network flow analysis, etc. to finally infer the source node location. This revelation can lead to capture of the assets or even loss of their life. Hence, SLP mechanisms must be devised to assure good levels of privacy against passive attacks by adversaries.

In this paper, we propose a routing mechanism named as Backward and Forward Random Walk (BaFRW) that is divided in 2 phases: first phase is where the event packet is randomly sent away from the source node towards the network boundary and second phase is where the packet is delivered to the base station using a previously developed mechanism termed as forward random walk. We discuss the mechanism in detail in Section 4. Major contributions of this work are:

- We develop a robust and randomized SLP mechanism BaFRW that guarantees a higher level of privacy strength against passive attacks.
- We perform an experimental analysis and simulation results depicted in Section 5 prove its efficiency.

The rest of the paper is structured as follows: Section 2 deals with the existing literature study and Section 3 gives an insight on the system models. The proposed scheme is explained in Section 4 while the experimental results are presented in Section 5. We conclude the paper and provide with possible future research studies in Section 6.

II. Related work

Ozturk et al. [11] in their work described about SLP problem through a Panda-hunter model. In this model, sensors are deployed in the network who pick up the presence of panda as soon as it appears within their transmitting radius. Then information regarding the location of panda is sent to the sink through multiple sensors in the path between the source node to sink. The authors suggested use of phantom flooding mechanism for SLP preservation. The packet containing information about the asset’s location is sent from source node to a phantom node for a specific Time to Live (TTL) counter after which it is flooded towards the sink. This mechanism used up a lot of energy while flooding thus degrading the network lifetime. Then came a mechanism termed as Phantom routing by Kamat et al. [12]. They suggested a change in the Phantom flooding method by replacing the probabilistic flooding with a single route to sink. This change of flooding phase by a single route contributed to saving on the energy loss and increasing network lifetime.

Chen et al. [13] proposed Forward random walk (FRW) in an attempt to provide SLP preservation. Forward random walk suggests using the close and equal neighbor nodes to transmit information. This mechanism chooses one node randomly from the list containing close and equal hop count neighbor nodes. This process is repeated till the packet reaches the sink.

Manjula et al. [14] proposed a SLP routing based on randomized routes (SLP-R) that consists of 3 phases. In the first phase, the event packet is routed to the outermost ring through shortest path followed by an equidistant routing where packets are routed in the same ring for a specific number of hops. Finally using the shortest path approach the packet is delivered to sink. This mechanism improved privacy levels by increasing the randomness measure of the transmission routes.

Many routing schemes have been proposed that includes circular routing, fake sources injection, phantom routes, geographic routing etc. for SLP preservation. Circular routing by Han et al. [15] proposed selection of number of interference rings to transmit the packet in a circular manner through cluster heads. Then a starting node selected through token system from amongst the cluster heads in the outermost ring carries a dummy packet to the sink through greedy path and as it comes through the event ring, the dummy contents get replaced with the real content. This dynamic routing scheme ensured higher security but led to greater energy loss as well. However, it must be noted that there is always a tradeoff between performance measuring parameters due to which there is always one or the other degradation that increased privacy brings along with it. We aim to develop a mechanism that balances all the parameters along with good privacy strength.

III. System Model

A. *Network model*

The network model that we consider in this paper is Panda-hunter model. As per the model illustrated in Fig.1, sensors nodes are deployed in the network region to monitor the movement of panda and these sensor nodes keep transmitting information regarding the location of panda to sink. There is an adversary who monitors the wireless transmission between sensor nodes and backtracks in an attempt to get the source location. The packets must follow transmission paths that is difficult for the adversary to backtrack within a specified time interval. We assume the network model to consist of the following characteristics:

- The deployment of sensor nodes in the network region is done with a specific density ‘ρ’. The sensors once set in a place are not allowed to change its location.
- There is only one sink located at the center of the network.
- The network is divided into rings and grids. Each grid consists of a cluster head chosen among the sensor nodes placed in the grid. The grid to grid transmission of packets take place through cluster head.

B. *Adversary model*

Adversary intend to monitor the transmission to infer the location of source node. He is assumed to have the following characteristics:

- There is a single adversary who monitors the network communication.
- He carries out passive attacks such as eavesdropping, backtracking, traffic analysis, time correlation etc.
- He has access to advanced equipments to monitor the transmission and memory and energy constraints are not a limiting factor for him.
- We consider the adversary to be a local adversary with restricted range of hearing. Global adversaries [16] are far more powerful and tend to have a view of the entire network region. However, our work involves securing the source location against local adversary having the above mentioned features.

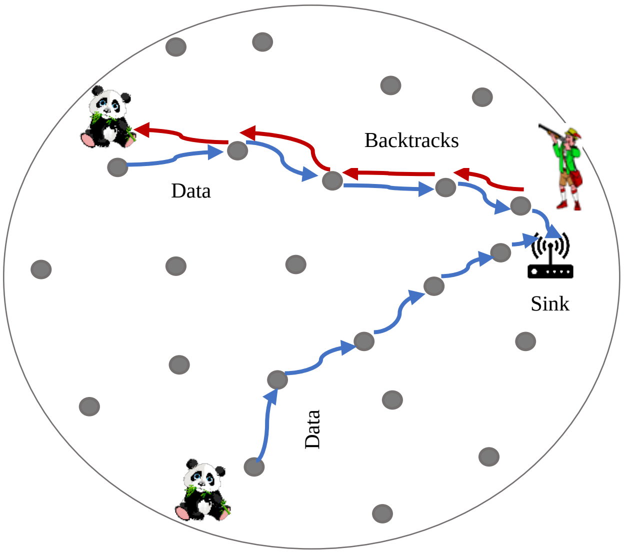

Fig. 1. Panda-hunter model

C. *Energy Consumption model*

The loss of energy for sensor nodes while packet transmission is computed by the following equations 1 and 2 [17] where equation 1 is for loss while transmitting the packet and equation 2 is the loss while receiving a packet.

$$E_{t=}l * E_{elec} + l * \varepsilon_{fs} * d^2, \qquad d \le d_0 \qquad 1(a)$$

$$E_{t=}l * E_{elec} + l * \varepsilon_{amp} * d^4, \quad d > d_0 \qquad 1(b)$$

$$E_{r=}l * E_{elec} \qquad 2$$

The description of the parameters is provided in Table 1.

TABLE 1. System Parameters

Parameters	Values
Distance threshold ($\mathbf{d_0}$)	87m
Distance between source and sink	d

$\mathbf{E_{elec}}$	50nJ/bit
$\boldsymbol{\varepsilon_{fs}}$	10pJ/bit/ m^2
$\boldsymbol{\varepsilon_{amp}}$	0.0013pJ/bit/ m^4
Packet length (l)	1028 s

IV. Description of BaFRW Mechanism

Before the transmission begins, the sink floods the network with an initial message which is meant for initialization and neighbor nodes discovery. The message contains information about the network range, system parameters, location of the sink and a counter to measure the hop count. The node that receives this message fills its routing table with the information, increments the counter variable and attaches its own id and location before passing it to adjacent neighbors. The neighbor node then updates its routing table with the information received from the packet and is able to identify its neighbors and their location. Then every node partitions its neighbors in 3 groups: close neighbors, far neighbors and equal hop neighbors relative to their distance from the sink with respect to itself. After this operation is performed by every node, the routing transmission begins. BaFRW consists of 2 phases that are described below.

D. *Backward Random walk*

This phase is dependent on the presence of neighbor with the same or more hop count. The source node carries out two functions before transmitting the event packet:

- Selects a random number from the range whose minimum value is the number of hops required to reach the outermost ring and maximum value is double the hop count for outermost ring. This value is attached to the packet.

$$h_{brw} = \text{rand}({}^{R}/_{2r} - h_{srcnode} \ \text{ to } \ {}^{R}/_{r})$$

- The source node forms a backward list consisting of nodes from equal and far neighbors group.

The source node selects a node randomly from the backward list and decrements the h_{brw} counter by one before sending the packet to the randomly chosen node. The node that receives the packet again chooses a node randomly from its backward list, decrements the counter and transmits the packet. This process is repeated till the packet reaches the outermost ring or h_{brw} becomes zero. The node at which this phase ends is termed as terminal node.

E. *Forward random walk*

The terminal node forms a forward list consisting of nodes from equal and close neighbor group and then randomly selects a node from it and transmits the packet. Every node that receives the packet follows the same till the packet is delivered to the sink. This phase is aimed at randomizing the route while the packet is delivered to the sink.

Fig.2 depicts the architecture and routing protocol of the BaFRW mechanism.

V. Experimental Analysis

A. *Settings*

We have simulated the algorithm in MATLAB 2018b to determine and compare the efficiency of our proposed scheme BaFRW with FRW and SLP-R. The network region is a circular region with sensors deployed randomly in each grid. The size of each grid is same as the communication radius. The parameters are specified in Table 2. The results are computed to be an average of 50 simulations.

TABLE 2. Network Parameters

Parameters	Values
Network length	800 m
Communication radius (r)	40 m
Initial energy	0.5 J
Network density	0.0015
Number of packets per simulation	100
Number of simulations	50

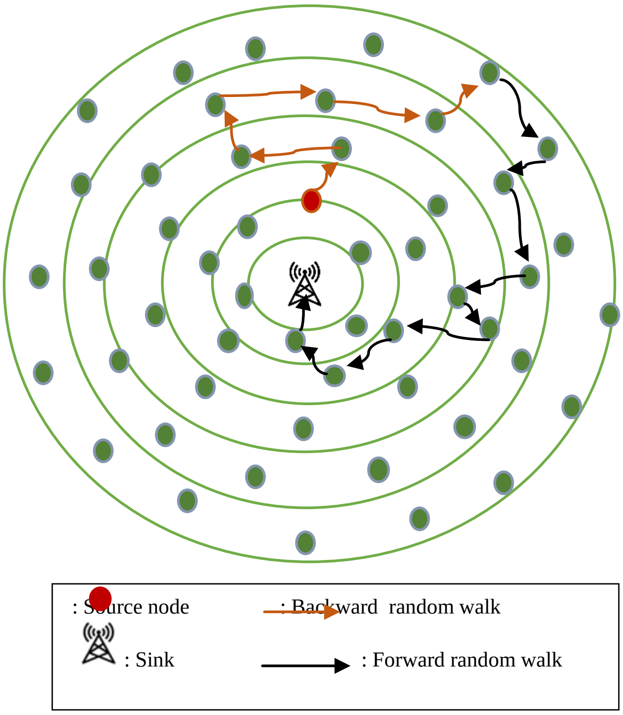

Fig. 2. Illustration of BaFRW scheme

B. *Results*

In this section, we discuss the experimental results of the three mchanisms i.e. SLP-R, FRW and BaFRW in terms of metrics like safety period, transmission delay, energy consumption, capture rate and entropy. Safety period is defined as the average number of packets that the sink receives before the adversary is able to locate the source node. Transmission delay is defined as the average number of hops taken by the event packet while being transmitted towards sink. Average energy consumption measures the loss accrued in the network while transmitting a single packet in each simulation. Total energy consumption is the amount of energy lost in the entire simulation and the loss is measured only while the sensor node transmits, receives and processes the packets. Energy loss is measured in terms of Joule. Capture rate depicts the adversarial success in locating the source node with respect to the total number of simulations. It is represented in terms of percentage. Entropy is a measure that depicts the randomness of the routes taken to deliver the packets to the sink.

a) Safety period: The measurement of privacy is done in terms of safety period that is computed on the basis of differing distances of source node from sink. The plot depicting the values for safety period is shown in Fig.3. FRW provides the lowest level of privacy to source node and the reason is the comparably shorter and frequently selected candidate nodes in the route. SLP-R performs better than FRW due to the packets being constantly sent to the outer most ring where further transmission takes place. This routes the packet away from source node and improves the randomness. The proposed scheme BaFRW provides higher safety period than the other mechanisms especially when the source node is located closer to the sink. This can be attributed to the fact that packets follow a more random route while routing the event packets away from source. However, we also observe that as the source node starts moving away from the sink and is located in the outer regions, SLP-R and BaFRW provides nearly the same safety period.

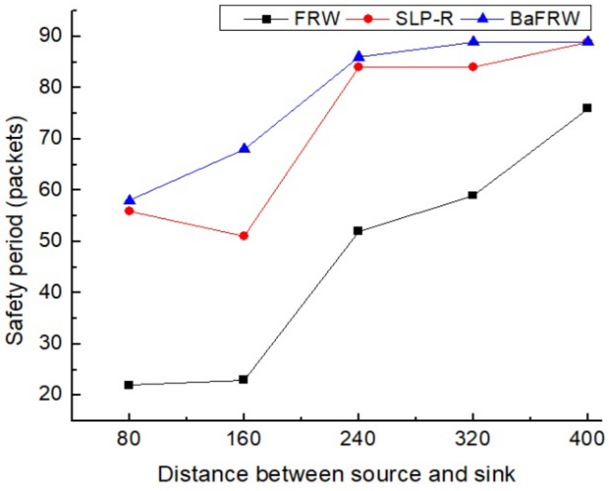

Fig 3. Safety period versus source location

b) Transmission delay: Fig. 4 shows the transmission delay for different location of source nodes in the network. It is the least for FRW as the packets are simply directed towards the base station by selecting the candidates with the same or lesser hop count, leading to a shorter route. We observe that the delay is the highest for our algorithm BaFRW as compared to other schemes. This happens because the hop counter attached with the event packet chooses a random number whose range is set high and moreover, it also combines forward random walk mechanism while routing the packet to sink in second phase. Both of these values yield a higher transmission delay for BaFRW while the source is located closer to sink.

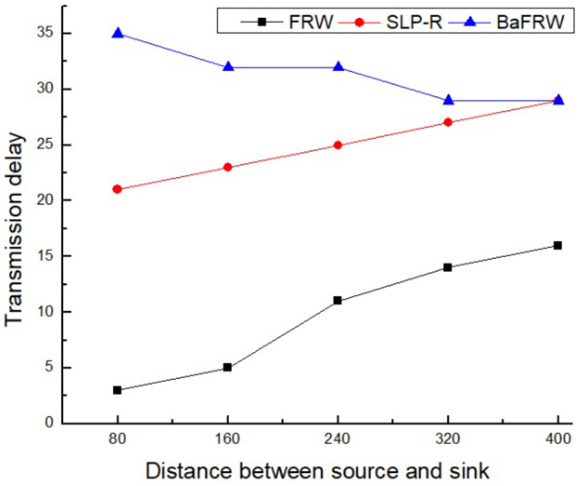

Fig 4. Transmission delay versus source location

c) Adversarial backtracks:The average number of hops backtracked by the adversary while attempting to locate the source node is expressed as adversarial backtracks. Gretaer the number of backtracking hops, higher is the security. Fig. 5 represents the adversarial hops for the three SLP mechanisms where it is clearly visible that BaFRW has the highest backtracks among the existing protocols. This shows that the adversary hasto travel a longer route and longer routes assist in improved security for the source node.

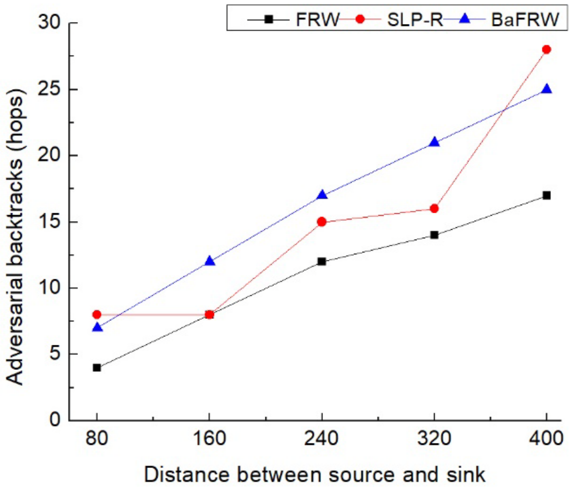

Fig. 5. Adversarial backtracks versus source location

d) Total energy consumption: The plot for representing the amount of energy loss in the simulation is provided in Fig. 6 and Fig.7. Fig 6 represents the average loss of energy per packet per simulation run whereas fig. 7 illustrates the total energy consumption occurred per simulation. We observe that the energy consumption is highest for BaFRW. It is due to the reason that safety period is high denoting a greater number of packets being forwarded and even the higher transmission delay that leads to a longer route. FRW consumes the least amount of energy in the entire simulation.

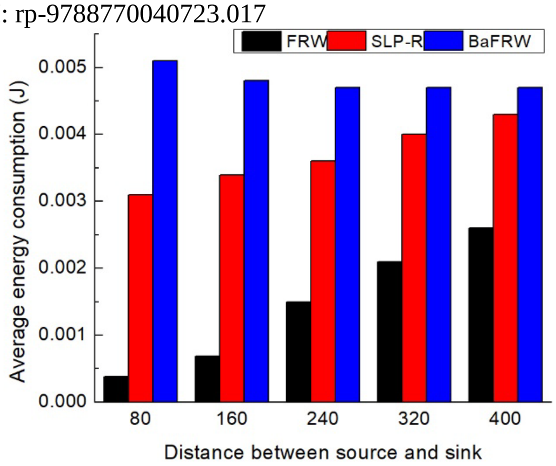

Fig 6. Average energy consumption for different source location

e) Capture rate: Capture rate denotes how well the algorithm secures the location by reducing the adversary's successful attempts at disclosing the source's location. A low capture rate means higher security. Fig.8 represents the capture rate with respect to source's location. The adversarial success rate is maximum for FRW. We observe that for source node locations closer to sink the capture rate is low for BaFRW as compared to SLP-R but for source located near the network boundary, the capture rate is similar.

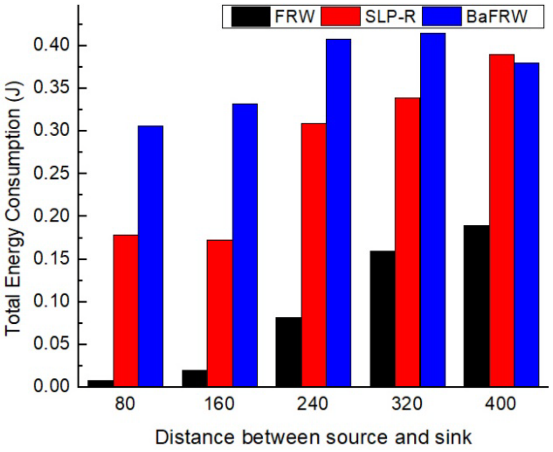

Fig. 7. Total energy consumption against varying source location

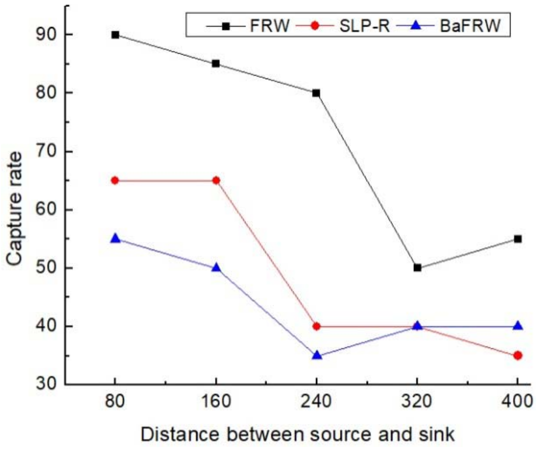

Fig. 8. Capture rate for varying source location

f) Entropy: The relationship between entropy and varying source location is shown in Fig. 9. The randomness measure is lowest for FRW and it represents that the transmission route usually follows through the same nodes to reach to sink. SLP-R has more random routes as compared to FRW. Gigher entropy level assures greater privacy. The entropy level is highest for BaFRW that denotes its efficiency in increasing the privacy.

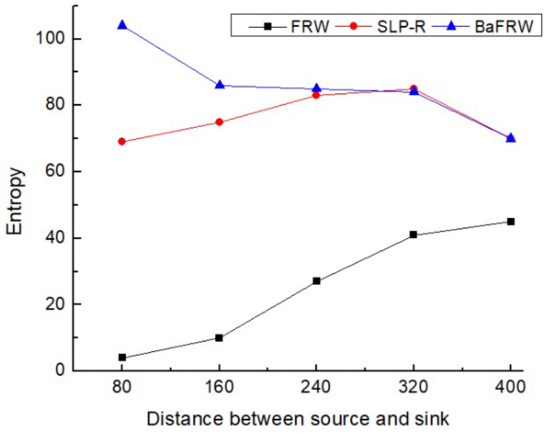

Fig 9. Entropy versus source location

VI. Conclusion

With the intent to secure the location information of source nodes in wireless sensor networks against passive attacks of adversaries, we developed a novel SLP mechanism named as BaFRW. In this, the transmission operation is divided in 2 phases: first phase is where each node forms a backward list and packet is randomly sent to one of nodes from backward list for a specific hop count towards the network boundary and after this phase ends, packet follows a forward random walk approach to route the packet to sink. Through simulated results, we observe that the proposed scheme improves the privacy, capture percentage and entropy for source located near the base station and almost same as SLP-R when the source node is located near the boundary of network. The major contribution is that the proposed protocol enhances the location privacy for assets moving near the sink that is considered a difficult task to achieve. Though the energy consumption is on higher range as compared to other SLP mechanism, it is also to be noted that BaFRW yields better security, lower capture rate and higher entropy. For future research directions, considering the improving strength of adversaries we plan on devising stronger routing mechanisms against global adversaries for securing the location of multiple assets on more practical approaches.

References

[1] GGulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., and Saravanan, G.,"A review paper on wireless sensor network techniques in Internet of Things (IoT)," Materials Today: Proceedings, vol. 51, pp. 161-165, 2022.

[2] M. S.BenSaleh, R.Saida, Y. H.Kacem,and M. Abid, "Wireless sensor network design methodologies: A survey," Journal of Sensors, 2020.

[3] D.Kandris, C.Nakas, D.Vomvas,and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," Applied System Innovation, vol. 3, no. 1, p. 14, 2020.

[4] H.Landaluce, L.Arjona, A.Perallos, F.Falcone, I.Angulo,and F. Muralter, “A review of IoT sensing applications and challenges using RFID and wireless sensor networks,” Sensors, vol. 20, no. 9, p. 2495, 2020.

[5] M. Aboubakar, M.Kellil,and P. Roux, “A review of IoT network management: Current status and perspectives,” Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 7, pp. 4163-4176, 2022.

[6] J. Jiang, G. Han, H. Wang, andM. Guizani, “A survey on location privacy protection in wireless sensor networks,” Journal of Network and Computer Applications, vol. 125, pp. 93-114, 2019.

[7] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, andA. Iyengar, “Location privacy-preserving mechanisms in location-based services: A comprehensive survey,” ACM Computing Surveys (CSUR), vol. 54, no, 1, pp. 1-36, 2021.

[8] P. Saxena, andK. Sharma, “Improved development of energy efficient routing algorithm for privacy preservation of sink in WSN”, Int Res J Eng Technol, vol. 3, pp. 21-27, 2016.

[9] H.Jiang, J.Li, P.Zhao, F.Zeng, Z.Xiao,and A. Iyengar, “Location privacy-preserving mechanisms in location-based services: A comprehensive survey,” ACM Computing Surveys (CSUR), vol. 54, no. 1, pp. 1-36, 2021.

[10] Moshika, A., Thirumaran, M., Natarajan, B., Andal, K., Sambasivam, G., & Manoharan, R. (2021). Vulnerability assessment in heterogeneous web environment using probabilistic arithmetic automata. IEEE Access, 9, 74659-

[11] C. Ozturk, Y. Zhang, andW. Trappe, W. “Source-location privacy in energy-constrained sensor network routing,” In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks, pp. 88-93, October, 2004.

[12] P.Kamat, Y.Zhang, W.Trappe,and C. Ozturk, “Enhancing source-location privacy in sensor network routing”, In 25th IEEE international conference on distributed computing systems (ICDCS'05), IEEE, pp. 599-608, June, 2005.

[13] H. Chen, andW. Lou, “On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks,” Pervasive and Mobile Computing, vol. 16, pp. 36-50, 2015.

[14] M. Raja, andR. Datta, “An enhanced source location privacy protection technique for wireless sensor networks using randomized routes,” IETE Journal of Research, vol. 64, no. 6, pp. 764-776, 2018.

[15] G.Han, L.Zhou, H.Wang, W.Zhang,and S. Chan, “A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things,” Future Generation Computer Systems, vol. 82, pp. 689-697, 2018.

[16] Rajesh, M., & Sitharthan, R. (2022). Image fusion and enhancement based on energy of the pixel using Deep Convolutional Neural Network. Multimedia Tools and Applications, 81(1), 873-885.

[17] J. Ren, Y. Zhang, andK. Liu, “An energy-efficient cyclic diversionary routing strategy against global eavesdroppers in wireless sensor networks”, International Journal of Distributed Sensor Networks, vol. 9, no. 4, p. 834245, 2013.