A Review on Location Privacy Preserving Techniques in WSN

[1]Deepika H.T, [2]Vybhavi P, [3]Chinnaswamy C.N.

[1,2]PG Students, [3]Associate Professor
Department of ISE,
[1]The National Institute of Engineering, Mysuru, India

***Abstract*-Wireless Sensor Networks (WSN) is one of the main zone of research and it has been more well known in the real life difficulties by giving minimal effort arrangements. The system comprises of little sensor nodes capable for detecting, handling, computation and communication. The system comprises of various sorts of assault, the most harming assault is sinkhole assault. In this kind of assault, the sinkhole node tries to draw in information to itself by transmitting counterfeit data to neighbor nodes and henceforth it interferes with the usefulness of such systems. Thusly with a specific end goal to overcome from this sort of assault giving security is critical. In this paper we are proposing sink and also source area protection systems. With a specific end goal to give more protection these procedures like forward random walk (FRW) and BLAST (Base station location anonymity and security technique) is utilized. On account of forward random walk conspire requires every node to acquire its hop count to the sink, which can be accomplished by utilizing a sink-based flooding. Toward the starting, the sink will start a flooding, after which every node can get the both its neighbors hop count to the sink. On account of BLAST conspire the center thought is to change the transmission scope of an arrangement of some chose sensors around the base to befuddle the assailant. Through this procedure, we can make an arrangement of fake base stations which can't be recognized by a solid assailant.**

***Keywords*-Wireless Sensor Networks (WSN), Base station Location Anonymity and Security Technique (BLAST), Forward Random Walk (FRW), Edge Based Strain Smoothing Technique, 2-Phantom Angle Based Routing (2PAR).**

I. INTRODUCTION

Wireless Sensor network arrange comprises of minute sensor nodes, low-power, light weight, minimal effort. Because of the ease of these nodes, the situating can be in the request of result of thousands to million nodes. The sensor nodes perform desire estimations, process the information and send it to a base station, which is usually referred to as sink node. The base station gathers the information from every one of the nodes and assesses the information from every node. Source Location Privacy (SLP) in sensor arrange implies the status that the data about the locations of events identified by sensors nodes is appropriately secured from unauthorized users, for instance, the sink of the network, can acquire the data. Observing and identifying events is an ordinary utilization of sensor networks. Preserving source location in sensor networks is challenging primarily because of the accompanying reason, the restricted resources accessible in sensor networks requires exceptionally effective security protection components.

II. SECURITY REQUIREMENTS IN WSN

The most important security requirements in WSN are listed below.

- Confidentiality of data

For this situation the information or data are should be kept secret this is conceivable just when we encode it with a secret key, so no message in the network is comprehended by anybody aside from the proposed recipient.

- Data integrity

No message can be changed when it traverses from the sender to the planned recipient.

- Availability of data

Accessibility of information is concerned just when the capacity of a sensor node to utilize the resources and the sensor network is accessible for the communication of message. This prerequisite ought to be accessible dependably in presence of internal and external assaults.

- Data freshness

It shows that the information is new and affirms that no interloper can answer to the old messages. It is conceivable to check the freshness of information through nonce counter.

- Self-organization

A system which requires each node to be autonomous and sufficiently adaptable to act self-organization and self-healing to adapt up in various circumstances.

Types of attacks and security threats in Wireless Sensor Networks:

Table 1: Layer wise attacks in WSN

Attacks	Layer affected	Security threats
Jamming, Tampering	Physical	Availability, Integrity
Collisions, Exhaustion, Unfairness	Data Link layer	Confidentiality, Integrity
Spoofing, Selective Forwarding, Sybil, sinkhole, Wormhole, Node Replication	Network Layer	Availability, Authentication, Confidentiality
Availability, Authentication, Confidentiality	Transport Layer	Availability

III. LOCATION PRIVACY

Providing location privacy in sensor network is major challenging errands. By utilizing a few procedures if interloper decides the source and destination at that point there might be a shot that assailant can devastate the entire system. In location privacy there are two noteworthy undertakings which may encourages for the interloper to find their objectives, in particular by recognizing the movement of nodes and by the traffic pattern. There are a few ways that an interloper can follow the location one is packet headers which contain the whole data of source and destination, consequently ensuring this sort of data is critical in accomplishing location privacy. Consequently a few creators underlined a few techniques [1] to ensure the privacy protection against nearby spy.

Privacy assaults in WSN

The privacy assaults in for the most part arranged into two kinds: data oriented privacy, context oriented privacy appeared in **Figure 1**. On account of data oriented privacy principally focuses on giving privacy to the information, so interloper may discover troublesome in alteration of the information. Context oriented privacy concentrates on contextual data this incorporates location data that is source location and sink location or time of the event.

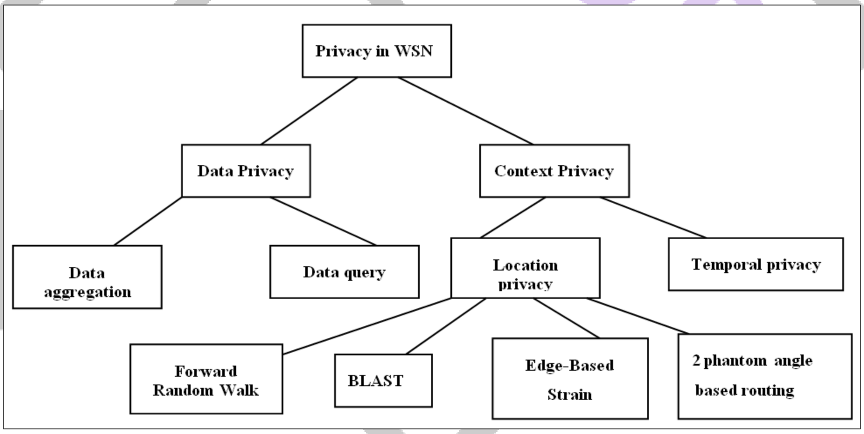


Figure 1: Classification of Privacy in WSN

Data oriented privacy is divided into data aggregation and data query. Data aggregation may be done by computing mean, standard deviation, variance etc., Context privacy is divided into location privacy and temporal privacy. Location privacy plays an important role in WSN such as, location of special sensor node, data source. In the case of temporal privacy it is important in the mobile target tracking application of WSN.

IV. LOCATION PRIVACY TECHNIQUES

- Forward random walk

In this scheme [2] each node transfers a received packet to a node haphazardly chosen from its forward neighbors whose hop-count to the sink is no bigger than its own. This procedure is rehashed at every node until the point that the packet comes at the sink. Consider a sample network, in the source sends packet periodically to the sink by multi-hop wireless communication Tr. In the event that the packets dependably venture out from the source to the sink along a fixed path, it will be simple for a foe to catch either the source or the sink through hop-by-hop tracing. The FRW [2] requires every one of the nodes acquire their hop count to the sink, which can be accomplished utilizing a sink-based flooding.

Toward the finish of the flooding, every node can get both of its own particular and its neighbors hop count to the sink. In the FRW scheme, each node isolates its neighbor into three lists, further list, equivalent list and closer list. Each neighbor in the further list contains bigger hop count than the sender, though neighbor in the closer list has a smaller hop count than itself.

Furthermore, the node in the equivalent list contains a smaller hop count with itself. The combination of the equivalent list and closer list forms the forward list.

Figure 2 indicates one of the message conveyance ways of the FRW scheme. When sending a packet, the node will arbitrarily choose a neighbor from its forward list as the next hop. Neighbors in the further list won't be considered as the contender for the next hop since they will naturally expand the latency.

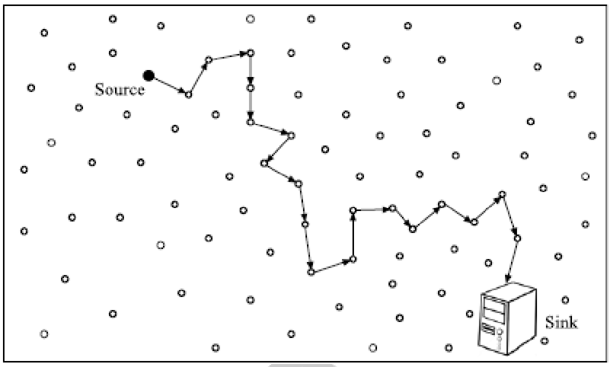


Figure 2: The scenario for the forward random walk scheme.

Algorithm 1 illustrates the procedure of FRW scheme

```
Algorithm1 FRW(node k)

1. Initiation: Next hop=null
2. Construct the forward list $FRL_{k.}$
3. While receive a message n do
4. Randomly choose a neighbour from $FRL_k$ as next hop.
5. Forward the received packet info to next hop.
6. End while.
```

- BLAST (Base Location Anonymity and Security Technique)

BLAST [3] expects to secure the base station from both packet tracing and traffic analysis assaults and give great protection against the global assailant. Network is separated into blast nodes and ordinary nodes. Collector is available some place nearby blast nodes. Source node sends packet to one of the blast nodes which is then retransmitted inside blast area. The enemy is uninformed of the communication between blast node and real beneficiary. Henceforth location privacy of the collector is kept up.

An example of blast routing can be seen in

Figure 3. The source A arbitrarily picks a blast node B from the ring. At that point, the packet is routed from A to B through the most limited path between them. The node B now blasts the packet with a transmission scope of K × tx which is the width of the security rings. This covers the entire ring and furthermore some additional nodes outside the ring. The real base station can be found anywhere inside the ring. To the foe, any node in the ring could be the base station. The significant preferred standpoint of this blast nodes strategy over the system depicted above is the energy consumption. Blast nodes procedure expends significantly less energy as just a single node in the path needs to transmit with more vitality for each packet and whatever remains of the path devours minimum conceivable energy.

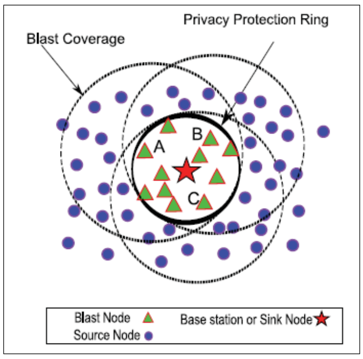


Figure 3: Working of blast node

- Edge based strain smoothing

Extended Finite Element Method (X-FEM) is a standard displacement based finite element approximation is enriched by additional functions using the framework of partition of unity and it is the standard tool to model arbitrary crack growth. An alternative method for arbitrary crack growth was proposed and successfully implemented by static setting and in dynamic setting. The main difference between alternative and original X-FEM is that the discontinuity jump is not obtained by introducing additional unknowns but by so-called Overlapping Paired Elements and when an underlying elements is cracked, the overlapping is introduced to handle the crack kinematics. Some of advantages are,

1. As no additional degrees of freedom are introduced, the implementation of the phantom node method in an existing finite element code is simpler.
2. No mixed terms occurs in improving conditioning.
3. Standard mass lumping schemes can be used due to the absence of enrichment. There are several contributions to develop diagonalized mass matrices in standard XFEM [5, 6], but they are based on certain assumptions.

In the ES-FEM [7], the domain Ω is partitioned into a set of non-overlapping no-gap smoothing domains constructed using element edges of the triangular elements. $\Omega^{(k)}$ satisfies the conditions $\Omega = \mathrm{U}^{Ne}{}_{k=1}\, \Omega^{(k)}$ and $\Omega^{(i)} \cap \Omega^{(j)} \neq \emptyset$ for all i≠j , in which Ne is the total number of edges of elements in the problem domain. In Figure 1, the smoothing domain, the smoothing domain corresponding to an inner edge k, and the smoothing domain for a boundary edge m are illustrated.

The displacement field within an element Ω_e is rewritten as

$$\forall x \in \Omega_e, u\,(x) = \Sigma_{I\in s1} u^1{}_I N_1(x) H(-f(x)) + \Sigma_{I\in S2}\ {}_U{}^2 N_I\,(x) H(f(x)) \qquad (1)$$

where $S_1$and S_2 are the nodes of superimposed elements 1 and 2, respectively. As illustrated in **Figure 4**, each element contains real nodes and phantom nodes marked by solid and empty circles, respectively; $NI$is the finite element shape function associated with node I, while $\mathbf{u}^1{}_I$and $\mathbf{u}^2{}_I$are nodal displacements of original nodes in superimposed element 1 and 2, respectively. $H$is the Heaviside function. Here, we choose the physical domain up to the crack line. The crack line will be the boundary in phantom node method. It is like the elements near the external boundary. So, we avoid singularity in phantom node method

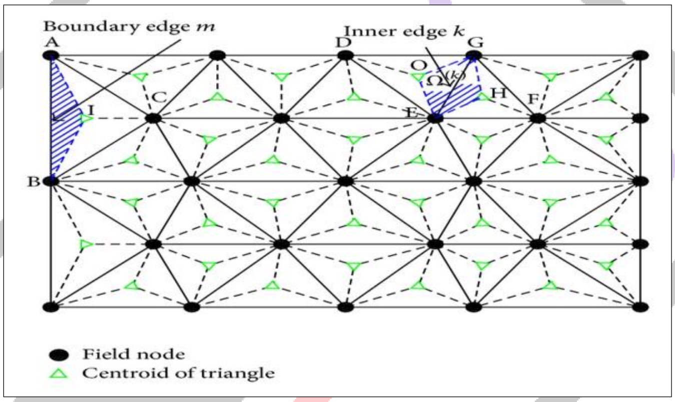


Figure 4: Construction of edge-based strain smoothing domains.

Numerical integration is implemented on chosen Gauss points as illustrated in **Figure 7** and **Figure 8** corresponding with split smoothing domain in **Figure 5** and tip smoothing domain in **Figure 6**, respectively.

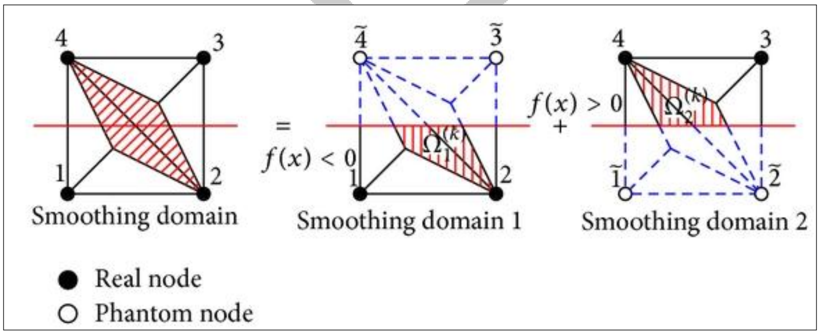


Figure 5: The decomposition of a completely cracked smoothing domain into two superimposed smoothing domains.

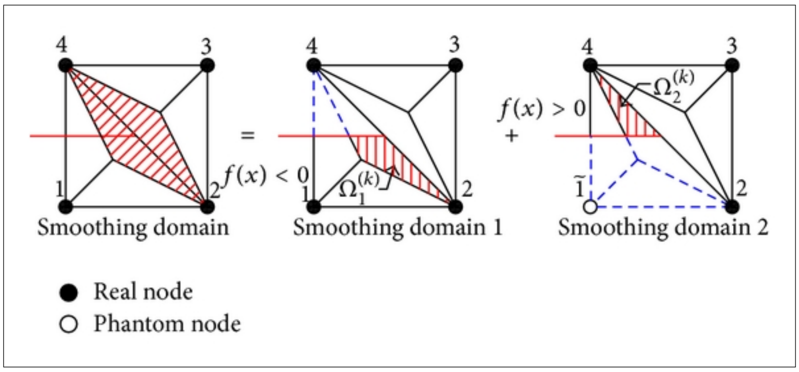


Figure 6: The decomposition of a cracked smoothing domain containing crack tip into two superimposed smoothing domains.

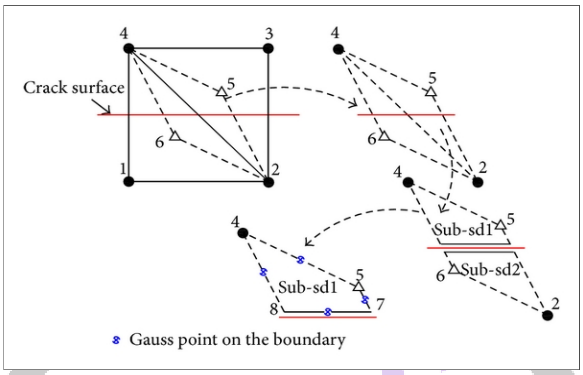


Figure 7: The decomposition of a completely cracked smoothing domain into two superimposed smoothing domains.

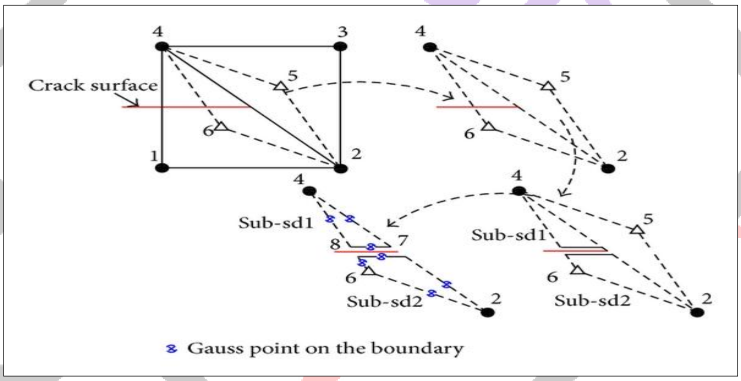


Figure 8: The decomposition of a cracked smoothing domain containing crack tip into two superimposed smoothing domains.

The jump in the displacement field across the crack is calculated by,

$$[\![u\ (x)]\!] = u1\ (x) - u2\ (x) \text{ on } \Gamma c; \qquad (2)$$

$I$is a phantom node in
{element 1 if ($\mathbf{x}I$) > 0, element 2 if $f(\mathbf{x}I) < 0$}.

Displacement and Strain Field

In the ES-FEM , the domain Ω is partitioned into a set of non-overlapping no gap smoothing domains constructed using element edges of the triangular elements. $\Omega(k)$ satisfies the conditions $\Omega = \bigcup^{N1}_{k=1}\Omega(k)$ and $\Omega(i) \cap \Omega(j) = 0$, for all $i \neq j$, in which Ne is the total number of edges of elements in the problem domain. In **Figure 4**, the smoothing domain, the smoothing domain corresponding to an inner edge k, and the smoothing domain for a boundary edge $m$are illustrated. Numerical integration is implemented on chosen Gauss points as illustrated in **Figure 8** and **Figure 9** corresponding with split smoothing domain in **Fig. 6** and tip smoothing domain in **Figure 7,** respectively.

- 2-PAR (2-Phantom Angle Based Routing)

2-Phantom Angle Based Routing is designed to improve the Source Location Privacy (SLP). This scheme uses the distance of each node from the Base Station (BS), its location information and the inclination angle between the nodes to form a triplet which is used to select the phantom nodes. The analysis shows that the safety period of the proposed algorithm is better than Phantom Single Path Routing Scheme (PSRS) and Multi-Phantom Routing Scheme (MPRS).

The first strategy based on a random walk to provide Source Location Privacy (SLP). It involves two phases: the random walk phase and the flooding phase. In random walk phase, when a source senses an event, the message is forwarded in a randomized manner up to h hops. The node at the end of the random walk is treated as a phantom source. After h hops, the packet is flooded towards the BS using baseline flooding. Another protocol named PSRS works similar to PRS. However in PSRS, instead of using baseline flooding, it forwards the message to the BS using shortest path algorithm.

The pure random walk is incompetent in keeping phantom source away from the real source as each node has an equal probability of being selected as an intermediate node [8]. This may led to message looping in a cycle near source node. In order to avoid the repetition of paths, directed random walk [9] was introduced which can be either sector-based or hop-based.

The adjacent nodes of a node is divided into two sets viz., north-west and south-east in sector-based directed random walk. In the situation of sensing an event by source, it arbitrarily selects one of the set and sends the message to an arbitrarily selected node of that set. Within the defined set of nodes, every midway node sends the message to arbitrarily opted adjacent node. In hop-based directed random walk, every node divides its adjacent nodes on the source of their distance from the BS to hop-count. This has two sets namely: larger hop-count neighbours and equal or smaller hop-count neighbours. This employs the same method for sending the message as in sector-based directed random walk.

An improvement of sector-based directed random walk is the Self-Adjusting Directed Random Walk (SADRW) [10]. The adjacent nodes of a node are separated into four sets: north, south, east, and west. On the occasion of a node sensing an event, it arbitrarily selects a set and sends the message to that chosen node of that set. Every midway node sends the message in the chosen direction. In case a node fails to send the message in the chosen direction, an arbitrary direction is chosen afresh from balance sets. When the packet is at the periphery of the network and had previously travelled I hops, h≥i, the random walk ends else the new direction is chosen from the balance sets. The Phantom Routing with Locational Angle (PRLA) [11] is an improvement to PSRS. Here, every node calculates the inclination angle between itself and adjacent nodes with BS as a vertex. Forward probability increases with greater inclination angle. Midway node is selected based on the forward probability of a node. The inclination angle is retained by the midway node to send the packet. After h hops, the end node which receives the packet is termed as phantom source. The shortest path algorithm is then used to forward the packet to the RRIN (Randomly selected intermediate node) which is an improvement of PRS [12, 13]. In this method, the arbitrarily chosen midway node receives the forwarded message from the source node and in the similar manner the message is forwarded to the BS. The safety period is improved by compromising with the cost of more delay and more energy consumption. The number of messages that are effectively received by the BS before the adversary arrives at the source location is termed as safety period. The Angle-based Dynamic Routing Scheme (ADRS) to improve the SLP. The inclination angle between the sender and receiver is determined in this routing. For sending the packets established on the inclination angle, this scheme generates a candidate set of nodes. For transmitting each message, the candidate set is converted which in turn generates numerous paths to the destination.

Also, the Energy-efficient Privacy Preserved Routing (EPR) is proposed. In this scheme, the author uses 2α-angle anonymity concept to generate the location of phantom sources [14]. A new protocol using two phantom nodes named MPRS [14]. This consists of two phases namely: Configuration phase and Working phase. In the configuration phase, BS is created by the group of three nodes. In the three node group the inclination angle between every two nodes should be at least 30 degree. In the case of sensing the event by the source in working phase, a node from three node groups is chosen (this works as phantom source) and the message is sent to the adjacent node with destination as phantom source. Using shortest path algorithm the phantom source forwards the message to the BS. Based on the arbitrarily generated numbers, the identification of phantom source is done.

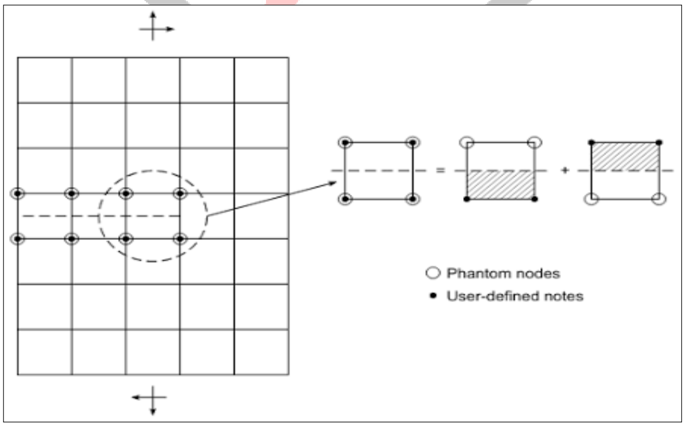
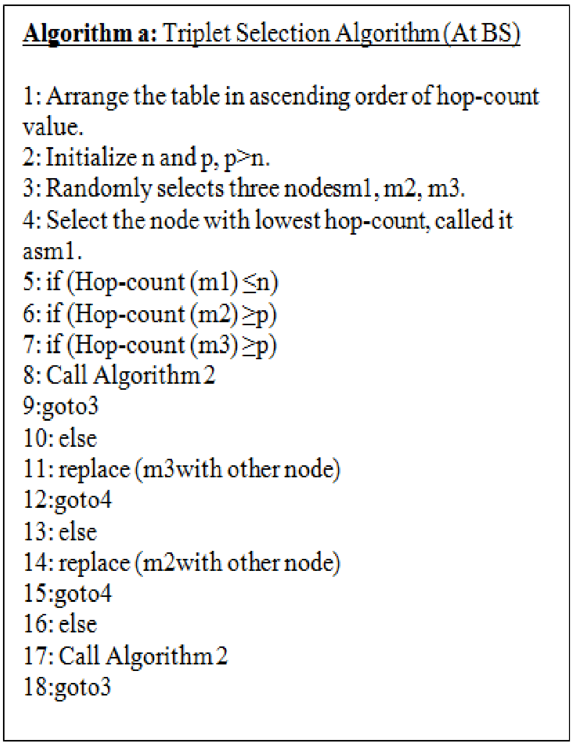


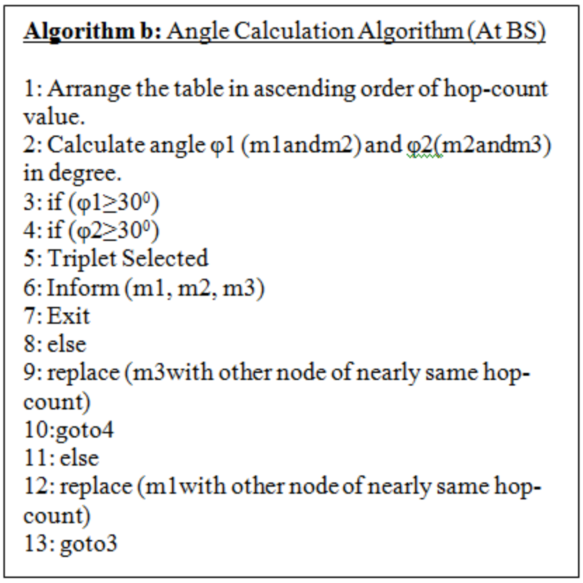
Figure 9: Phantom nodes and user defined nodes

Algorithm (a) and (b) illustrates the procedure of 2-PAR scheme



Algorithm a: Triplet Selection Algorithm (At BS)

```
1: Arrange the table in ascending order of hop-count value.
2: Initialize n and p, p>n.
3: Randomly selects three nodesm1, m2, m3.
4: Select the node with lowest hop-count, called it asm1.
5: if (Hop-count (m1) ≤n)
6: if (Hop-count (m2) ≥p)
7: if (Hop-count (m3) ≥p)
8: Call Algorithm 2
9:goto3
10: else
11: replace (m3with other node)
12:goto4
13: else
14: replace (m2with other node)
15:goto4
16: else
17: Call Algorithm 2
18:goto3
```



Algorithm b: Angle Calculation Algorithm (At BS)

```
1: Arrange the table in ascending order of hop-count value.
2: Calculate angle φ1 (m1andm2) and φ2(m2andm3) in degree.
3: if (φ1≥30⁰)
4: if (φ2≥30⁰)
5: Triplet Selected
6: Inform (m1, m2, m3)
7: Exit
8: else
9: replace (m3with other node of nearly same hop-count)
10:goto4
11: else
12: replace (m1with other node of nearly same hop-count)
13: goto3
```

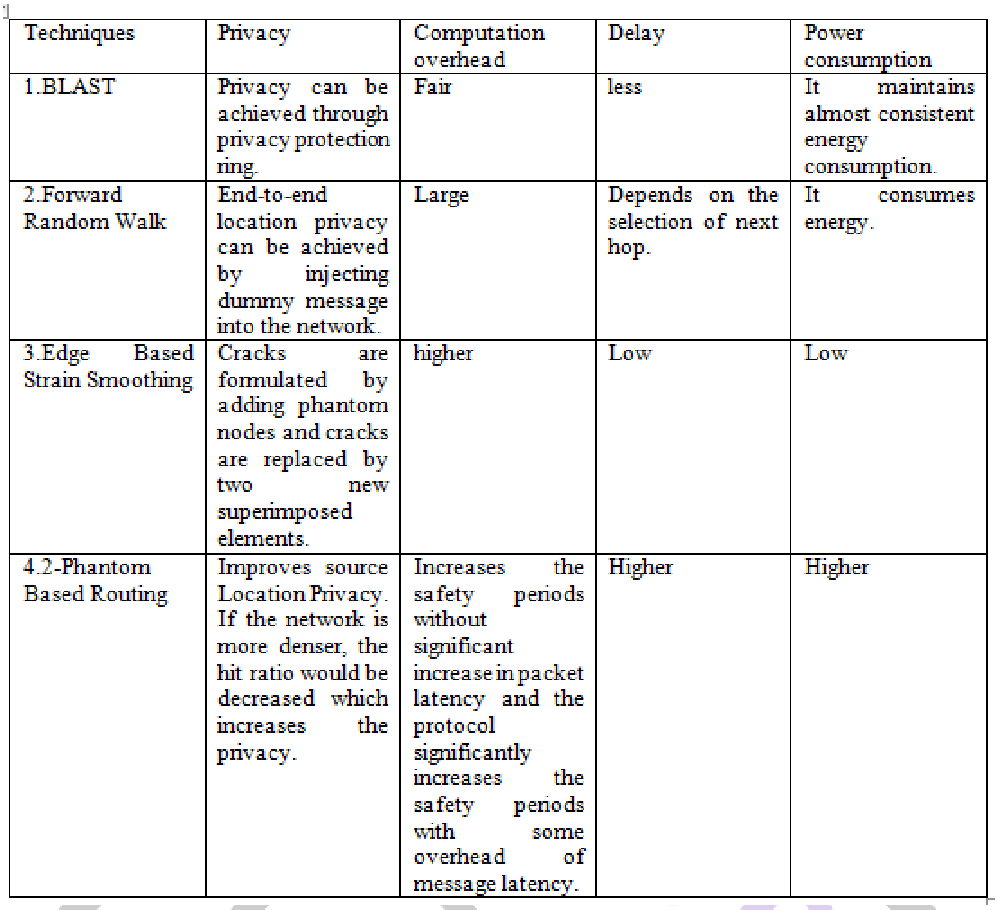
where,

- n and p: user defined values, where “n” is minimum hop distance of source node from the BS and “p” is the minimum hop distance of the phantom node from the BS.
- BS has locational information of all nodes deployed.
- BS selects the node having lowest hop-count among the selected nodes m1, m2 & m3 and treats it as a source node.

V. COMPARSION

From the above mentioned four techniques, forward random walk gives a solution to achieve end-to-end location privacy using randomized routing path whereas, in the blast technique this scheme will found more efficient then other existing location privacy techniques because it has strong location privacy of sink nodes, it reduces the energy consumption and it reduces the packet delay since shortest path algorithm is used. Edge Based Strain Smoothing technique is simple to implement and provides high accuracy compared to other methods whereas, in 2-Phantom Angle Based Routing technique provides better performance in terms of safety period as compared to single Phantom routing and increases the safety periods without any significant increase in the packet latency.

Table 2: Performance comparison of above four techniques.



Techniques	Privacy	Computation overhead	Delay	Power consumption
1.BLAST	Privacy can be achieved through privacy protection ring.	Fair	less	It maintains almost consistent energy consumption.
2.Forward Random Walk	End-to-end location privacy can be achieved by injecting dummy message into the network.	Large	Depends on the selection of next hop.	It consumes energy.
3.Edge Based Strain Smoothing	Cracks are formulated by adding phantom nodes and cracks are replaced by two new superimposed elements.	higher	Low	Low
4.2-Phantom Based Routing	Improves source Location Privacy. If the network is more denser, the hit ratio would be decreased which increases the privacy.	Increases the safety periods without significant increase in packet latency and the protocol significantly increases the safety periods with some overhead of message latency.	Higher	Higher

VI. CONCLUSION AND FUTURE ENHANCEMENT

Providing location privacy is an important issue in WSN. In this paper we propose four location privacy preservation techniques, forward random walk, BLAST, edge based strain smoothing, 2-phantom angle based routing which can protect the location privacy against local and global eavesdropper. In future better techniques can be implemented to secure safety period and also energy consumption. In Edge Based Strain Smoothing technique, a cracked element is replaced by two superimposed elements and a set of additional phantom nodes and performed to investigate convergence rate in terms of strain energy and stress intensity factors. The results have shown that the ES-Phantom node is able to produce super convergent solutions. Future applications of this method may deal with the interactions among a large number of cracks with the purpose of obtaining the higher accuracy and efficiency in solving complicated crack interaction. In 2-Phantom Angle Based Routing technique, the protocol significantly increases the safety period with some overhead of message latency. Future work may be done by increasing the number of phantom nodes and evaluating their cost benefits. The proposed protocol may be further enhanced by including other privacy preservation techniques.

REFERENCES

[1] Ying Jian, Liang Zhang, and Shigang Chen, "Protecting Receiver- Location Privacy in Wireless Sensor Networks," IEEE INFOCOM 2007 proceedings. pp. 1955-1963.

[2] H. Chen and W. Lou, "From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks," 2010 International Conference on IEEE.

[3] Venkata Praneeth Varma Gottumukkala; Vaibhav Pandit; Hailong Li; Dharma P. Agrawal, "Base station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks", 2012 IEEE International Conference on Communications (ICC) ,pp.6705 – 6709.

[4] T. Menouillard, J. Réthoré, A. Combescure, and H. Bung, "Efficient explicit time stepping for the eXtended Finite Element Method (X-FEM)," International Journal for Numerical Methods in Engineering, vol. 68, no. 9, pp. 911–939, 2006. View at Publisher · View at Google Scholar · View at Zentralblatt MATH · View at MathSciNet · View at Scopus.

[5] T. Menouillard, J. Réthoré, N. Moës, A. Combescure, and H. Bung, "Mass lumping strategies for X-FEM explicit dynamics: application to crack propagation," International Journal for Numerical Methods in Engineering, vol. 74, no. 3, pp. 447–

474, 2008. View at Publisher · View at Google Scholar · View at MathSciNet · View at Scopus.

[6] G. R. Liu, T. Nguyen-Thoi, and K. Y. Lam, “An edge-based smoothed finite element method (ES-FEM) for static, free and forced vibration analyses of solids,” Journal of Sound and Vibration, vol. 320, no. 4-5, pp. 1100–1130, 2009. View at Publisher · View at Google Scholar.

[7] Kamat, P., Zhang, Y., Trappe, W., Ozturk, C.: Enhancing source-location privacy in sensor network routing. In: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, ICDCS 2005, pp. 599–608. IEEE (2005).

[8] Yao, J., Wen, G.: Preserving source-location privacy in energy-constrained wireless sensor networks. In: 28th International Conference on Distributed Computing Systems Workshops, ICDCS 2008, pp. 412–416. IEEE (2008).

[9] Zhang, L.: A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing. In: Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, pp. 33–38. ACM (2006).

[10] Wei-Ping, W., Liang, C., Jian-Xin, W.: A source-location privacy protocol in wsn based on locationalangle.In: IEEE International Conference on Communications,ICC2008,pp.1630-34IEEE (2008).

[11] Li, Y., Lightfoot, L., Ren, J.: Routing-based source-location privacy protection in wireless sensor networks. In: IEEE International Conference on Electro/Information Technology, eit 2009, pp. 29–34. IEEE (2009).

[12] Li, Y., Ren, J.: Preserving source-location privacy in wireless sensor networks. In: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009, pp. 1–9. IEEE (2009)

[13] Spachos, P., Toumpakaris, D., Hatzinakos, D.: Angle-based dynamic routing scheme for source location privacy in wireless sensor networks. In: 2014 IEEE 79th Vehicular Technology Con- ference (VTC Spring), pp. 1–5. IEEE (2014).

[14] Kumar, P., Singh, J., Vishnoi, P., Singh, M.: Source location privacy using multiple-phantom nodes in wsn. In: TENCON 2015 - 2015 IEEE Region 10 Conference, pp. 1–6, November 2015.