Source Location Privacy Using multiple Phantom Nodes in WSN

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

[1]PG Student, [2]Associate Professor, [3]Professor
[1,2]Department of ISE, [3]Department of CSE
[1,2]The National Institute of Engineering, Mysuru, India
[3]Vidyavardhaka College of Engineering, Mysuru, India

Abstract: **Wireless Sensor Network (WSN), are spatially distributed autonomous sensors to monitor physical and environmental conditions, such as temperature, sound, pressure, etc and to co-operatively pass their data through the network to other locations. The application of WSN includes health, military, environment, home & other commercial areas and tracking & monitoring sectors. Monitoring often needs protection. Source Location Privacy (SLP) in sensors network means the locations of events detected by sensors nodes is properly protected such that only authorized entities, for example, the sink of the network, can obtain the information. Source location privacy is one of an important security issue and have many factors that influence the effectiveness of a solution. Preserving source location in sensor network is challenging mainly due to the limited resources available in sensor network which requires highly efficient privacy preservation mechanism. In this project, we are proposing two phantom techniques i.e., Edge Based Strain Smoothing and 2-Phantom Angle Based Routing (2-PAR) is being studied for monitoring Source Location Privacy in WSN. In standard phantom nodes method, the cracks are created and it is formulated by adding phantom nodes and cracked elements are replaced by two new superimposed elements. This technique is simple to implement into existing Explicit Standard Finite Elements (ES-FEM) which leads to certain simplification with existing nodes. Taking the advantage of phantom node & ES-FEM, we introduce an Edge Based Strain Smoothing technique for the phantom method. The studies have established that this technique provides high accuracy compared to other methods. Another technique is 2-PAR. 2-PAR is designed to improve source location privacy. This scheme considers a triplet for selecting the phantom nodes. A triplet is a group of three nodes formed on the basis of their distance from sink, their location information & the inclination angle between them. For every packet transmission, selection of phantom is performed thereby creating alternative paths is done. As the path changes dynamically, the safety period increases without significant increase in packet latency. As a result, this technique provides better performance in terms of safety period compared to single phantom routing. Simulation results will be demonstrated is carried out using NS3 simulator.**

Keywords: **Wireless Sensor Networks (WSN), Source Location Privacy(SLP),Edge Based Strain Smoothing,2-Phantom Angle Based Routing(2-PAR), Explicit Standard Finite Elements(ES-FEM).**

I. INTRODUCTION

Wireless Sensor Network (WSN) is a cluster of spatially discrete and devoted sensors for monitoring and recording the conditions of the environment and organizing the collected data at the central location. Admissions to the different network that uses dissimilar protocols is included in WSN gateway and the routing paths is provided for transmission of data, representation is as shown in fig-1.

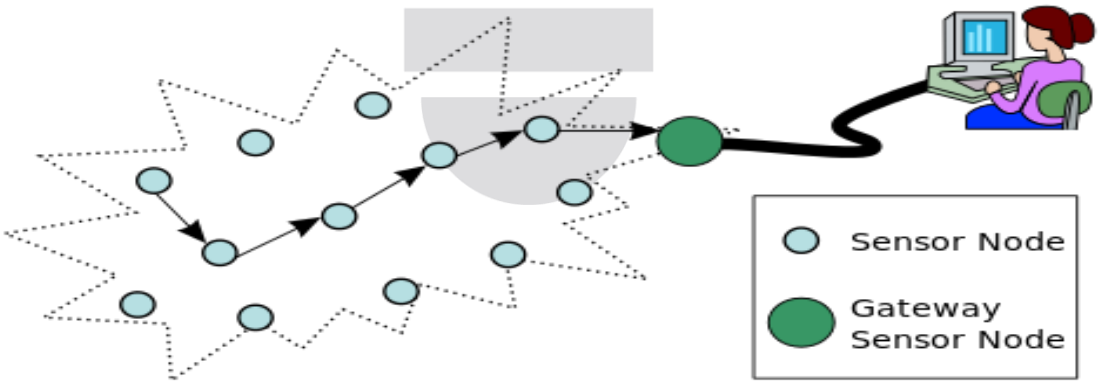

Fig. 1:Gateway Sensor and Sensor Nodes

Sensor nodes is a node in the sensor network that is capable of collecting sensory information, process the captured information and communicate with inter-connected nodes in the network. Monitoring of physical and environmental situations viz., pressure, temperature and sound etc., and transmit the data to the other locations in the network is due to the spatially dispersed autonomous

sensors in Wireless Sensor Network (WSN). WSN consists of nodes which may vary from fewer to larger (thousands) and each node is at least connected to one sensor. WSN has varied applications. Due to technical advancements in computing, communications and power efficient embedded computing instruments, now WSN has become a standardized services adopted in industrial and commercial sector. WSN's sensor node is multi-purposeful and low energy consuming wireless instruments. WSN may consists of various types of sensors like low sampling rate, seismic etc. The application of WSN includes health, military, environment, home & other commercial areas. This application includes tracking and monitoring, in which monitoring needs the protection. Source Location Privacy (SLP) means the status that the information about the locations of events detected by sensors nodes is properly protected such that only authorized entities, example, the sink of the network, can obtain the information. Monitoring and detecting events is a typical application of sensor networks. In sensor network, it is exigent in maintaining source position because of the following reason, the limited resources available in sensor network requires highly efficient privacy preservation mechanisms.

Types of attacks in WSN:

Table 1: Layer wise attacks in WSN

Layers	Attacks
Physical	Jamming, Tampering
Link	Collision, Exhausting
Network	Helloflood, Sybil, sinkhole
Transport	Flooding
Application	Denial-of-Service, cloning

II. RELATED WORK

Giving area security in sensor organize is major testing errands. By using a couple of strategies if intruder chooses the source and goal by then there may be a shot that aggressor can annihilate the whole framework. In area security there are two essential endeavors which may urges for the intruder to discover their destinations, specifically by perceiving the development of hubs and by the movement design. There are a couple of ways that a gatecrasher can take after the area one is bundle headers which contain the entire information of source and goal, therefore guaranteeing this kind of information is basic in achieving area protection. Thus a couple of makers underlined a couple of methods to guarantee the security assurance against close-by spy.

III. TECHNIQUES

- **Edge based strain smoothing** Extended Finite Element Method (X-FEM)[1] 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 [2] and successfully implemented by [3] 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 an enrichment. There are several contributions to develop diagonalized mass matrices in standard XFEM [4, 5], but they are based on certain assumptions.

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 $\Omega = \cup^{Ne}_{k=1} \Omega^{(k)}$ and $\Omega^{(i)} \cap \Omega^{(j)} \neq \infty$ for all $i \neq j$, in which Ne is the total number of edges of elements in the problem domain. In Figure 2, 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

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

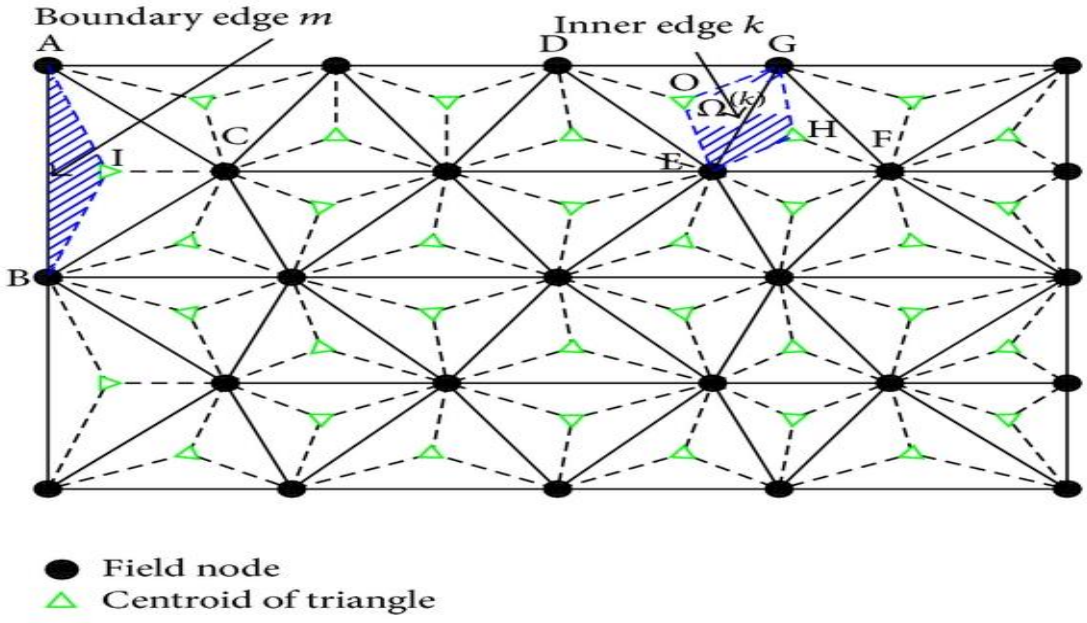

Fig. 2: Construction of edge-based strain smoothing domains.

- **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 [6]. This may led to message looping in a cycle near source node. In order to avoid the repetition of paths, directed random walk [7] 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. 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 [8]. A new protocol using two phantom nodes named MPRS. 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.

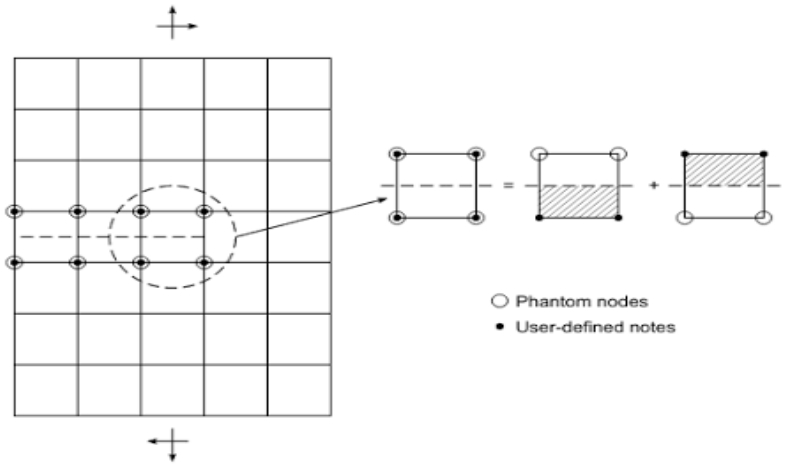

Fig. 3: Phantom nodes and user defined nodes

IV. EXPERIMENTAL RESULTS

In this section, we plan implementation framework of proposed algorithm using latest version 3.23 of NS3.

- **Edge Technique**

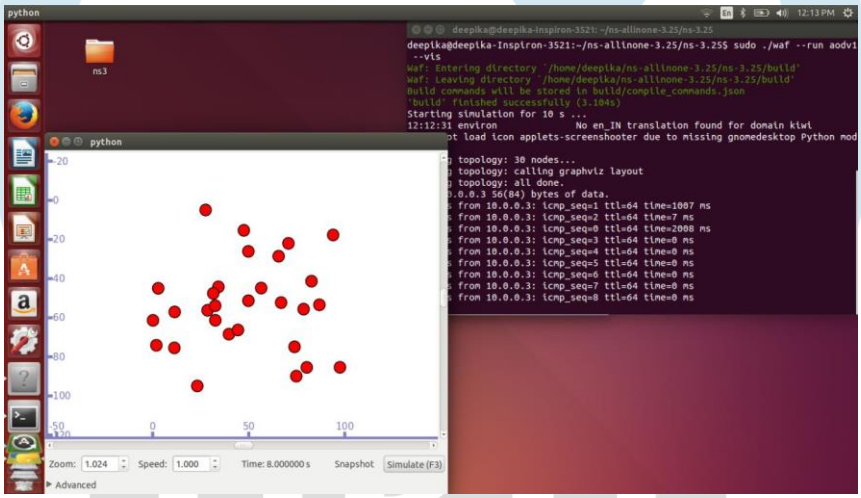

Fig. 4: Initial Network configuration in Edge technique

Fig 4 shows that, Source node will broadcast the packet which is sensed in the environment by the WSN network, the packet will be received by all nodes in the network even by the sink.

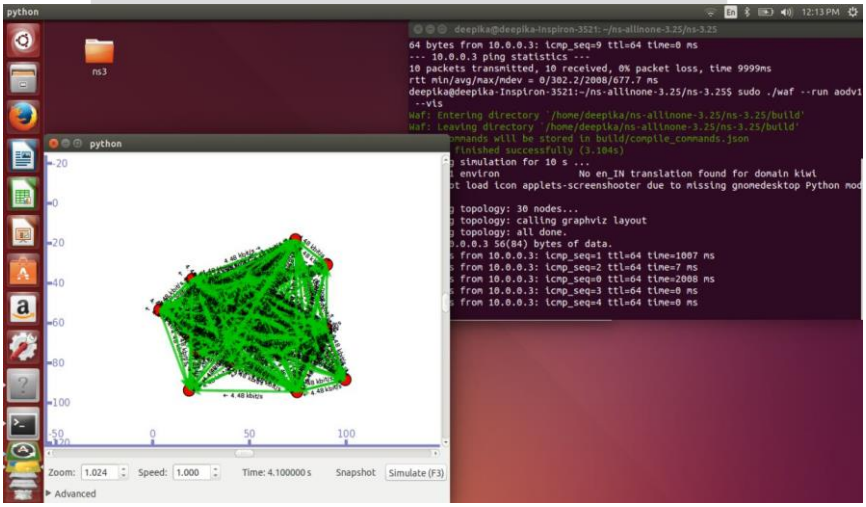

Fig. 5: Sending unicast packet from source to master node

Fig 5, shows that Source will send unicast packet to master node, then master node will broadcast the phantom node, finally sink will receive it, so attacker won't get the location of destination because traffic is same in all nodes.

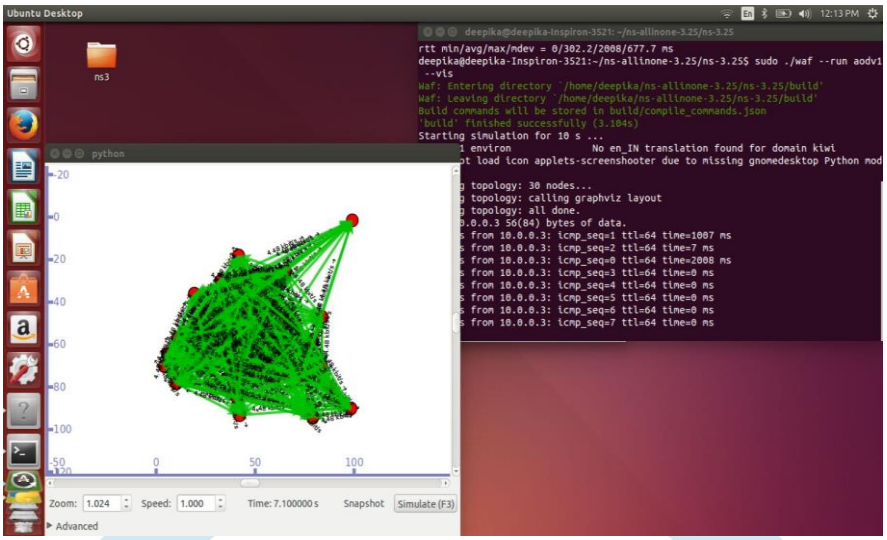

Fig. 6: Changing of the path

Fig 6, shows Source will change the path when ever breakage takes place in the network, so that attacker unable to get the location of sink because traffic is same in all nodes in the nodes.

- **2-Phantom Angle Routing Technique**

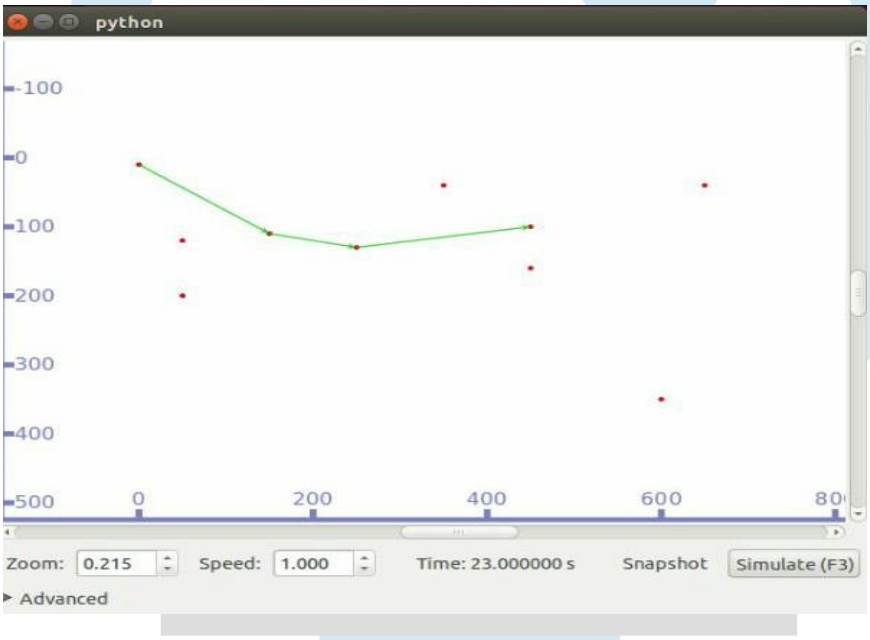

Fig. 7: Initial Network configuration in Phantom technique

Fig 7, shows that Source node will broadcast the packet which is sensed in the environment by the WSN network, the packet will be received by all nodes in the network even by the sink.

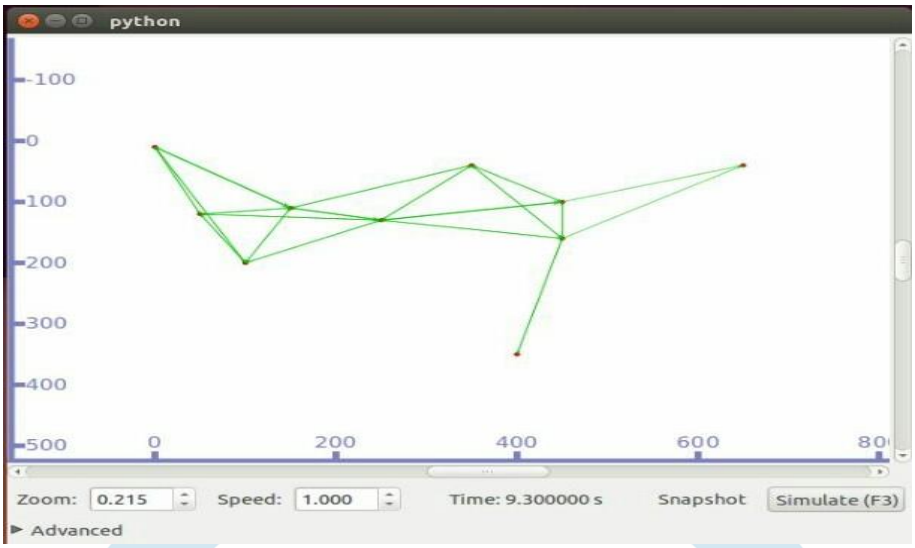

Fig. 8: Sending unicast packet from source to master node

Fig 8, shows that Source will send unicast packet to master node, then master node will broadcast the phantom node, finally sink will receive it, so attacker won't get the location of destination because traffic is same in all nodes.

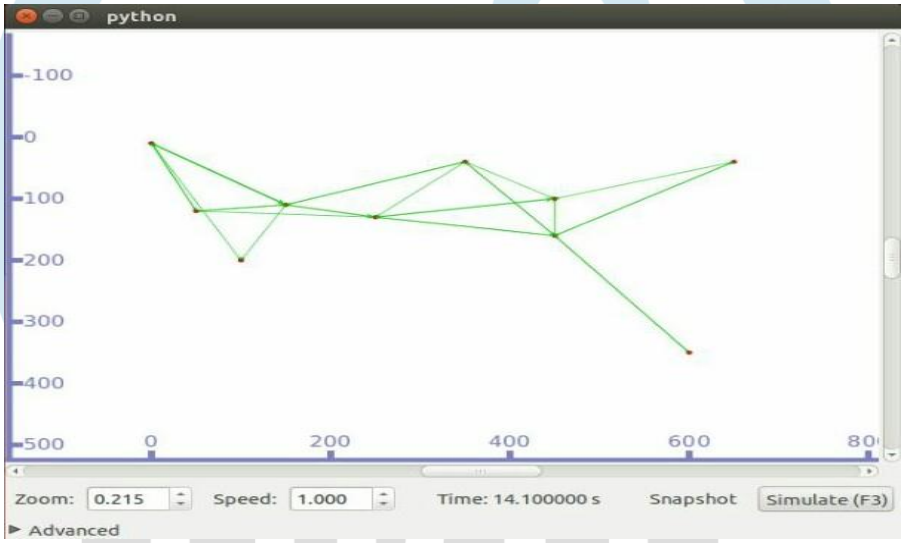

Fig. 9: Changing of path

Fig 9, shows Source will change the path when ever breakage takes place in the network, so that attacker unable to get the location of sink because traffic is same in all nodes in the nodes.

- **Throughput**

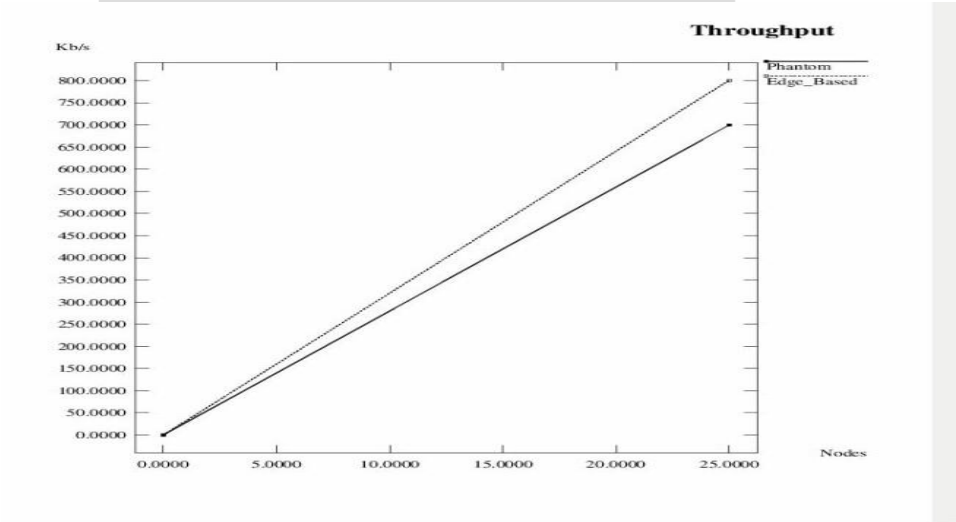

Fig. 10: Throughout in Edge Smoothing and Phantom technique

Throughout in Edge Smoothing and Phantom technique is shown in fig 10. The thin line shows the phantom technique and thick line shows the edge smoothing. As the time increases throughout of both the techniques will increases.

- **Packet Delivery Ratio**

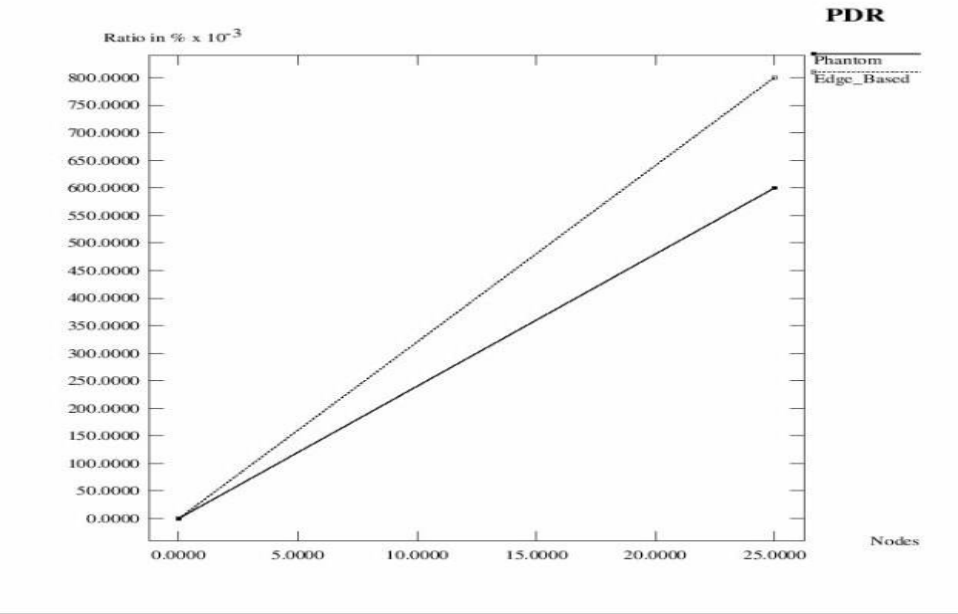

Fig. 11: PDR in Edge Smoothing and Phantom Technique

PDE (Packet Delivery Ratio) in Edge Smoothing and Phantom technique is shown in figure 11. The thin line shows the phantom technique and thick line shows the edge smoothing. The packets will be delivered successfully to the destination from the source.

V. CONCLUSION AND FUTURE ENHANCEMENT

Providing location privacy is an important issue in WSN. In Edge Based Strain Smoothing technique, the broken elements are restored by two superimposed elements and a set of extra phantom nodes and executed to enquire convergence rate in terms of strain energy and stress intensity factors. As a result, the ES-Phantom node will create super convergent to solve problems. Future applications of this method may deal with the interactions among a huge number of breaks with purpose of obtaining the higher accuracy and efficiency in solving difficulty in breaks interaction. And in 2-Phantom Angle Based Routing technique, some overhead of message latency with the safety periods will be increased by protocol significantly. Increasing the number of phantom nodes and evaluating their advantages of the cost will be existed in the future. By taking additional privacy preservation techniques the proposed protocol will be enhanced further.

REFERENCE

[1] T. Belytschko and T. Black, "Elastic crack growth in finite elements with minimal remeshing," International Journal for Numerical Methods in Engineering, vol. 45, no. 5, pp. 601–620, 1999. View at Google Scholar · View at Scopus

[2] A. Hansbo and P. Hansbo, "A finite element method for the simulation of strong and weak discontinuities in solid mechanics," Computer Methods in Applied Mechanics and Engineering, vol. 193, no. 33–35, pp. 3523–3540, 2004. View at Publisher · View at Google Scholar · View at Zentralblatt MATH · View at MathSciNet · View at Scopus

[3] J. Mergheim, E. Kuhl, and P. Steinmann, "A finite element method for the computational modelling of cohesive cracks," International Journal for Numerical Methods in Engineering, vol. 63, no. 2, pp. 276–289, 2005. View at Publisher · View at Google Scholar · View at Scopus

[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] 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)

[7] 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)

[8] Manjula, R., Datta, R.: An energy-efficient routing technique for privacy preservation of assets monitored with wsn. In: 2014 IEEE Students' Technology Symposium (TechSym), pp. 325–330. IEEE (2014)