Energy Efficient Technique for Concealing Sink Location in WSN

Sumeshwar Singh, Palak Aggrawal, Shiv Ashish Dhondiyal, Santosh Kumar, Deepak Singh Rana

Abstract: In a wireless sensor network, concealing the location of the sink is critical. Location of the sink can be revealed (or at least guessed with a high probability of success) through traffic analysis. In this paper, we proposed an energy efficient technique for concealing sink location named EESLP (Energy Efficient Sink Location Privacy) scheme. Here we proposed an approach, in which we are concealing the sink location in such a way so that node energy utilization while securing sink in network can be minimum, to defending sink's location privacy and identity when the network is subjected to multiple traffic analysis attack. EESLP designs the network area of coverage with multiple spots generating fake message traffic for fake sink location creation that resembles the traffic behavior that is expected to be observed in the area where the sink is located. To achieve this we select some sensors away from the actual sink location which act as fake sinks by generating dummy or fake packet. The simulation results prove that EESLP can improve network life time and QOS (congestion, throughput, packet delivery rate) of sensor network while protecting sinks Location privacy.

Keywords: Fake sink, dummy or Fake packet, E-LEACH, M-LEACH, Clustering

I. INTRODUCTION

Wireless sensor networks are applicable in the fields of environmental monitoring , surveillance , military war and distraous region [1,2] the WSN are deployed in a region , the sensor node inside the region communicate with each other and collect the information , send this information to a particular node called sink .WSN is vulnerable to many active and passive attacks among all these threat , in case of passive attack , the knowledge of location of sink make possibility for cyber/physical attack , some schemes [3,4,5] are provided to secure the location of source node for getting the information ,if the sink node comes under the threat the WSN become unable to provide the useful information to its user , so here it is a crucial job for us to secure the location of the sink in WSN such as way that while securing sink location the nodes energy utilization can be minimum as much as possible so that our sensor network can work for long duration. This is really a very tedious and challengeable task as we know that our sensor always have scarcity of electrical power or energy resources in WSN. Though there are lot of work is done in securing the sink location, which we will be brief ahead but not enough work done to make this hiding sink location energy efficient, so very few literature are available on this topic, despite some security methods [6, 7, 8] are applied to conceal the location of sink by using the encryption techniques. However, a passive attacker is able to get the location information of the sink by only traffic analysis. To get the location of sink traffic analysis is a good method, to avoid the detection through traffic analysis, a method in [9] [21] are given in which some dummy or fake sink packet injection [21] scheme are used to confuse the attacker by creating multiple fake sink locations but the drawback of this existing approach is that while generating a fake packets by each node spot for securing sink location increases computation and energy overhead. Which consequently reduce the sensor network life time and degrade the values of Qos. Therefore it is challenge for us to secure the sink location without impacting network life time and QOS parameters simultaneously i.e. WSN energy consumption of each node must be minimum, so that the sensor network can work for a long duration. Therefore to achieve this objective we adopt energy efficient routing protocol for hiding sink location.

A. E-Leach Protocol

E-LEACH is modified version of LEACH protocol to balance the distribution of energy consumption among sensor nodes. The E-LEACH have the same round mechanism with of LEACH but selection of cluster head is totally based upon residual energy. In leach we know that cluster head selected on the basis of random order sequence, but the drawback is that some time, those node who have very least amount of residual energy for communication can become cluster head and in the end due to low residual energy during communication they would die soon, and those node who have judicial amount of energy they would miss the chance to become cluster head , therefore this protocol of cluster head selection some time put the question mark on its credibility. In this hierarchical routing protocols, the no of cluster head selection is also very sensitive matter, if the no cluster head will be minimum then each cluster has to cover a wide region to communicate with other node, as consequence of it , the node which are very far from cluster head they have to utilized more energy to communicate with cluster head therefore they will die very soon ,

Revised Manuscript Received on August 10, 2019.

Sumeshwar Singh, Department of Computing, Graphic Era Hill University, Dehradun, Uttarakhand, India. E-mail: singhsumeshwar@gmail.com

Palak Aggrawal, Department of Computer Science Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India.

Shiv Ashish Dhondiyal, Department of Computer Science Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India.

Dr. Santosh Kumar, Department of Computer Science Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India.

Deepak Singh Rana, Department of Computing Graphic Era Hill University, Dehradun, Uttarakhand, India.

on the other side if we will take excessive no of cluster head selection in sensor network then much amount of energy utilized by sensor networks which lead to reduce the network life time , therefore it must be ensure that there should be optimal no cluster head selection in WSN so that we can reduce the energy consumption in sensor networks, Therefore in the E-LEACH [17,18,19] we select the cluster head which has largest residual energy . That's why we can say that Energy-LEACH protocol improves the choice method of the cluster head.

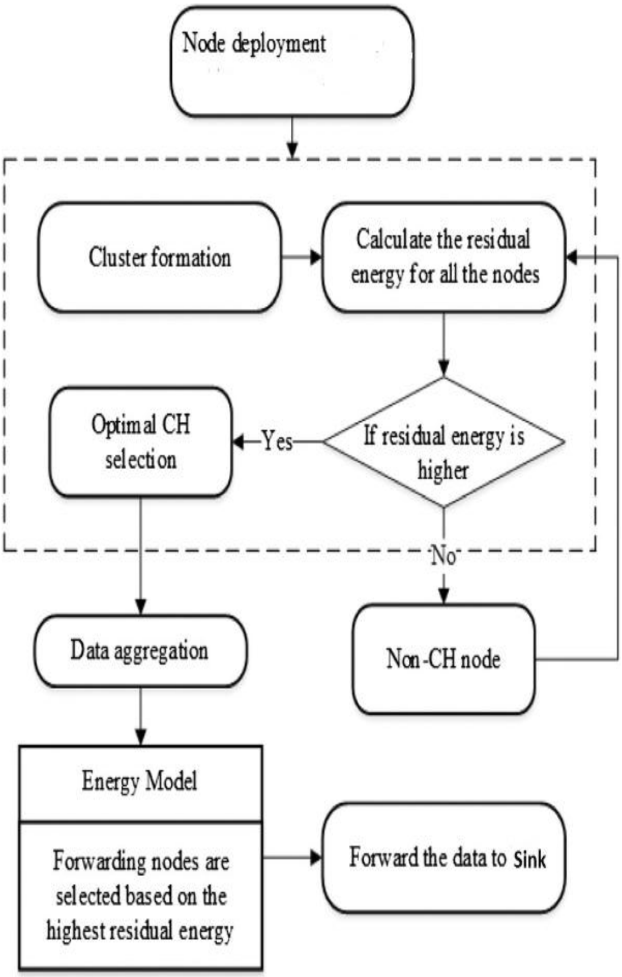
Node deployment
Cluster formation
Calculate the residual energy for all the nodes
If residual energy is higher
Yes
Optimal CH selection
No
Data aggregation
Non-CH node
Energy Model
Forwarding nodes are selected based on the highest residual energy
Forward the data to Sink

Fig.1. Flow chart of E-leach

B. M-Leach Protocol

Multi hop Leach [15, 17] is an extension of original leach protocol that saves the energy consumption of each node in WSN. This protocol is different from Leach in manner it takes multi hop path to send data to the sink [15, 17]. Leach is not suitable for large are network because it uses only single hop communication between CH and SINK; therefore, for more distance it will consume more energy. Multi hop leach proposed by F. Xiangning [15], overcomes this problem by adopting multi hop communication between CHs and sink. Therefore we used these protocol with E-leach , here the purpose of using this approach only to minimizes the energy utilization during packet routing towards sink location, in case of cluster head node which are very away from sink location.

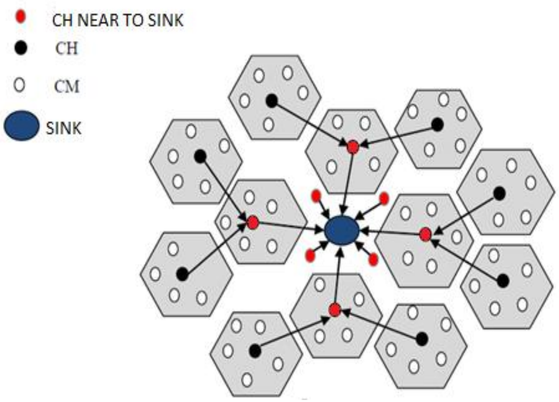

Fig.2. Network architecture of M-leach

II. LITERATURE SURVEY

A non-secure environment can arise inside the WSN due to the leakage of content and contextual privacy [5]. Content privacy can be obtained by the use of different cryptographic techniques however, even after the application of strong cryptographic techniques we are not able to secure the WSN for contextual information about the traffic inside the wireless sensor network [10, 11].

WS Deng et. Al. [12] suggested two types of traffic analysis attack inside the WSN as: rate monitoring analysis attack and time correlation attack. In rate monitoring attack, an attacker measure the rate of pack transmission for a node. The node with high packet rate is more susceptible for getting moreinformation so the attacker moves toward the node which have high packet rate for the time correlation attack. The defender node can use the buffer to store the packet to be forwarding of packets for the sake of network life. For the traffic analysis attack, some method have been proposed inside the network and bound the resource to send the packet periodically, forming the looping path for sending the packet [3, 5], Y. Jian et al. proposes a routing protocol to secure the location of receiver inside the network by injecting some fake packets inside the network. So that an attacker cannot identify the location of receiver by tracking the direction of the packet [4]. Nezhad et al. in [13] suggested an algorithm for topology discovery, in this algorithm all the nodes are able to broad cast the message for route discovery. The packets are labeled according to the incoming or outgoing packet. But in a whole process of securing the sink location in previous approach we found some weakness in fake packet generation as Y.jian et al. proposed, and routing method. Fake packets generation and routing mechanism among nodes both consume extra amount of node energy as result it reduce the network life time and impact the QOS parameter. So here we proposed a scheme which also using fake packet generation phenomenon and packet routing method but that is much energy efficient in comparative to previous scheme i.e. LEACH based hiding sink location. Here in our proposed scheme that is EESLP having special node called CH node or intersection node which are supposed to generate fake packets for fake sink location creation.

So that attacker which surround the sink location area can be diverted randomly towards the fake sink location. This is being proposed by[21] Malviya, Abhishek R., and Balaso N. Jag dale.

Along with it there is another draw back in the previous scheme that is cluster head selection in LEACH based hiding sink location done randomly. Therefore some time node having minimum energy become cluster head which later cannot be able to delivered packet to sink succefully because they already having low energy level so they die in very short period of time.

There is another reason for short network lifetime that is in LEACH based previous scheme. The packet routing executed in single hop fashion therefore node required utilize large power for packet transmission, if selected cluster head is deployed at very large distance from sink location. So instead of it we prefer multihop communications routing protocol in our proposed scheme.

Above mentioned are the main cause in previous leach based hiding sink location scheme which degrade our network operation and its life time. Therefore to resolve this energy limitation issue among node. We have decided to integrate our security technique with energy efficient protocol such as E-LEACH [17, 18, 19] and M- LEACH [15,17,18, 19]. Both protocol are improved version of LEACH [17,18,19], which enable the sensor network utilize low electrical energy while operating, that leads to make our sensor network can work for a long time. In this paper our prime aim not only to secure our sink location but also emphasis to explore the energy efficient mechanism to hide the sink location. Our new approach for hiding sink location scheme is called EESLP (energy efficient Sink location privacy), scheme.

In previous LEACH based hiding sink location scheme there are many drawbacks we found in context of shortest network life time, degrade values of Qos and causes are below:

a) Basic leach operation with hiding sink location leads to reduce the durability of network. As we know that in LEACH cluster head selection in each round not on the basis of maximum residual energy, therefore some time the node with least energy selected as cluster head instead of node having more residual energy as consequence of it node cannot delivered packet to destination successfully
b) Basic Leach operation having some cluster head node which are located at farthest distance from sink. Therefore they require more energy to establish connection with sink for packet delivery. By virtue of it the sensor energy decaying very instantly and reduced the network life time.
c) Fake packet generation used by each node spot to confuse the attacker. This mechanism cause the extra node energy utilization on each node, which degrade or reduced the network life time drastically. Therefore here we proposed an approach in which we have to restrict the fake packet injection among node. Instead there are special node only they are designated for fake packet injection. These node are called intersection node or cluster head node. Along with it we have adopt the order of cluster head selection on the basis of max residual energy[17,18,19] and packet routing in muti hop[15,17,18,19] order. These above are the changed methodology we implemented which minimize node energy utilization level to increase the sensor operation durability while concealing the sink location.

On the basis of literature survey we have discussed and found many weakness in previous hiding sink location scheme in context of network life time and Qos. Therefore we proposed a new energy efficient scheme EESLP and Network model in next section.

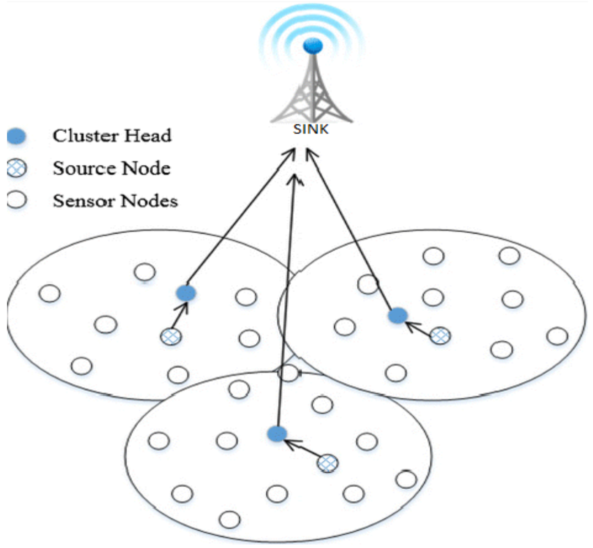

Fig.3. Basic LEACH Network architecture with single hop communication

III. PROPOSED METHOD

A. Proposed Network Model and Approach

According to Fig.4, Fig.5 and Fig. 6, we have elaborate the proposed energy efficient technique to secure the sink location . As far we know that in previous LEACH based hiding sink location scheme we used fake packet injection among nodes to confuse the attacker by masking the identity of receiver and sender during real packet transmission. But that scheme is energy consuming and reducing network lifetime . Therefore here in mention Fig 4, Fig 5 and Fig 6. we proposed a scheme that is much energy efficient and exhibiting longer sensor network life time while hiding the sink location. Here what we do first in proposed model we use fake or dummy packet injection scheme for creating a multiple fake sink location(orange nodes)unlike previous hiding sink location.

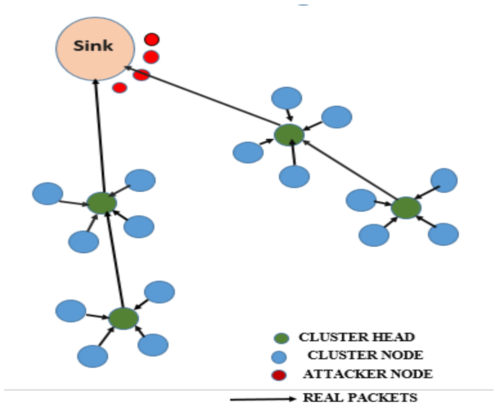

Fig.4. Showing the initial state of network when our sink location are surrounded by multiple attackers and therefore it is not safe for cluster head and sink location to exchange any messages.

Therefore, attackers which surround the sink location can be diverted randomly to fake sink location and meanwhile, sink can get more safe and privacy time for send and receive a packet from different cluster zone and vice versa. Here real packets are confused with fake packets so that attackers can be diverted towards randomly created multiple fake sink location. Because of this temptation or greediness an adversary will spend more time in tracing the wrong directions towards fake sink location. Therefore cluster head and sink node get the enough time to transmit or receive real packets safely. This process we can named as cluster based sink location privacy routing protocol. But here we must keep in mind that fake packet is generated only by cluster head nodes called intersection nodes. So that energy utilization among nodes can be reduced. Secondly we adopt energy efficient routing protocol for packet delivery from source to destination location while securing the sink location. In our proposed scheme whole cluster based network model must follow energy efficient routing protocol E-LEACH & M-LEACH. So that our deployed nodes while concealing sink location utilize less energy and sensor network can operate for long duration of time. Here in mention Fig. 4, Fig. 5 and Fig. 6 whole of the network divided into no of clusters each cluster have its cluster member nodes or source nodes (blue) and the cluster heads (green).

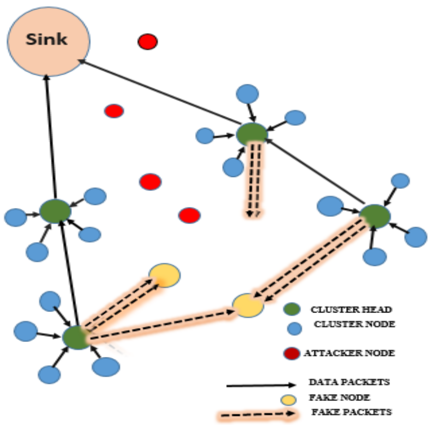

Fig.5. Cluster head start creating fake sink location by injecting dummy or fake packet towards random destination.

Cluster nodes responsible to record the physical event and send to their respective cluster head, the Selection of cluster head is executed on the basis of maximum residual energy. At a regular interval of time the designation and responsibility of cluster head changes. Here above we discussed about green node which are also called CH(cluster head) or intersection node responsible receive the packet from source node(blue). CH also responsible for fake packet generation to divert the attacker towards random fake destination. These nodes possess high energy because they have to aggregate the collected packet simultaneously with fake packet generation and it changes role dynamically. Along with it there is one pink node called sink node which is responsible to receive a packet from all cluster head or intersection node and in the last there are orange nodes called fake sink location to attract or give temptation to attacker.

B. Energy Model

This study also considers first order radio energy model [16] for computing the energy dissipated in communication. The transmitter consumes energy to run the radio electronics and power amplifier whereas the receiver consumes energy to run the radio electronics. We consider both free space model (d2 power loss) and multi- path fading model (d4 power loss) depending on the distance between transmitter and receiver.

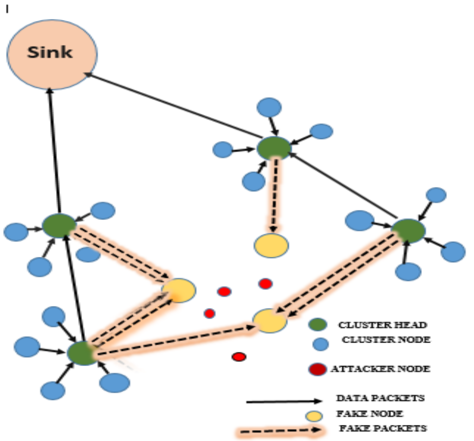

Fig.6. Showing, after injection of fake packet the attackers start migrating towards fake sink location, as a result the cluster head and sink get time to safely exchange the messages

Energy consumption of transmitting k-bits at distance d is taken as:

$$E_{TX}(k,d) = \begin{cases} (E_{elec} \times k) + (\varepsilon_{mp} \times k \times d^4), & d \geq d_0 \\ (E_{elec} \times k) + (\varepsilon_{fs} \times k \times d^2), & d < d_0 \end{cases} \quad (1)$$

Energy consumption of receiving data is taken as:

$$E_{RX}(k,d) = E_{elec} \times k \quad (2)$$

Where d_0 is threshold distance and defined as

d_0= (E_{fs} / E_{mp}) ^ 0.5

Algorithm
Notations Used
P: Desire of a sensing element node to becomes cluster head.
Em: Remaining energy of sensing element node.
En: most energy a sensing element node will have.
CH: Cluster head
BS: Base station
CM: Cluster member
The algorithmic rule is divided into two phases:
1. Setup part
2. Steady state part

1. SETUP STATE
Step 1: Every sensing element node 'S' generates a variable quantity Tmin (0<Tmin<1).
Step 2: Calculate minimum threshold T(s).
T(S)=Max(q/{(1-q)*mod1/q)}*[En/Em] if S belongs to G
T(s) = 0 otherwise
Step 3: **if** (Tmin< T((s))
Then sensing element node S becomes cluster head(CH) for this current round 'r'.
Else Sensing element node 'S' becomes cluster member(CM).
Step 4: All cluster heads(CHs) advertise message to non-cluster head sensing element node to hitch them.
Step 5: Every sensing element node be a part of the CH that is at minimum distance from it and kind the cluster.
Step 6: For every next round (r+1)
if (tmin< T(S))
Then sensing element node S is still stay cluster head.
else
Go to step 2 to pick out new cluster head.
Step 7:Finish of setup part.

2. STEADY STATE
Step 1: cluster head (CH) allocate TDMA time slot to cluster members (CMs).
Step 2: Each CMs sends the data to CH.
Step 3: Each CH aggregate the data and send first packet to base station(BS).
Step 4:if (send _packet< threshold)
then send _flag(CH,CM) = 0;
elsesend_flag(CH,CM) = 1;
Step 5:if (flag =1)
then continue the round and send remaining data to BS.
else Put the entire cluster into sleeping mode for this round.
step 6 : End of data transmission phase.
step 7: **End of algorithm**.

IV. SIMULATION RESULTS AND DISCUSSION

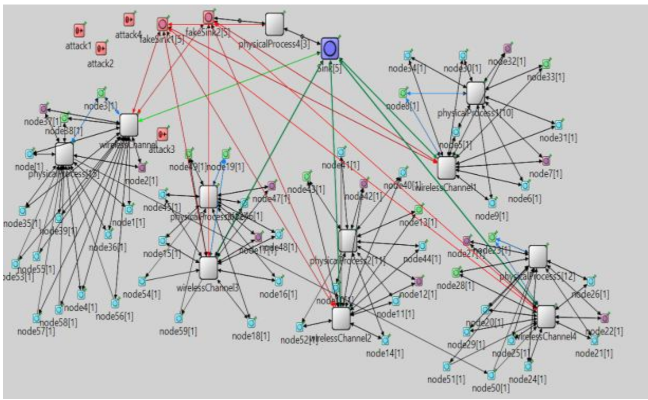

Fig.7. Simulation model

Here we have simulation model Fig.7 having with standard parametric value listed in table1 we have video sensor application for enemy surveillance propose. In above given simulation model we have sensor network of 60 nodes blue in color. Whole of the network is divide into 5 cluster each having its cluster head(violet)for collecting recorded data (black line) from blue node. There is also supporting neighbor (green) cluster head nodes for multi hop communication. Here is one sink node navy blue in color responsible to collect data packet (green line) from each cluster head or supporting cluster head. Simulation Fig.7 also show attacker node square shaped red in color diverted to fake sink location by fake packet injection (Red line).

In our simulation work our main objective to observe and evaluate the performance differences in context of network life time and Qos parameters. When we compare LEACH based hiding sink location previous scheme with EESLP basedhiding sink location proposed schemeWe performed comparative analysis of both approaches in context of Qos (packet delivery rate, congestion, and throughput and network lifetime).

Table 1. Simulation parameters

Parameters	**Values**
Size of Sensing Area	200x200 m^2
Location of sink	(100,10)
Number of nodes deployed in network	60
Initial energy of normal sensor node(E0)	1 KJ
Packet size	2000 bits
Number of static clusters	5
Type of distribution	Static
Energy level of node to be alive	0.009 J
Energy consumed in the electronics circuit to transmit or receive the signal, E_{elec}	50nJ/bit
Energy consumed by the amplifier to transmit at a short distance, E_{fs}	10pJ/bit/m2
Energy consumed by the amplifier to transmit at a longer distance, E_{mp}	.0013 pJ/bit/m4

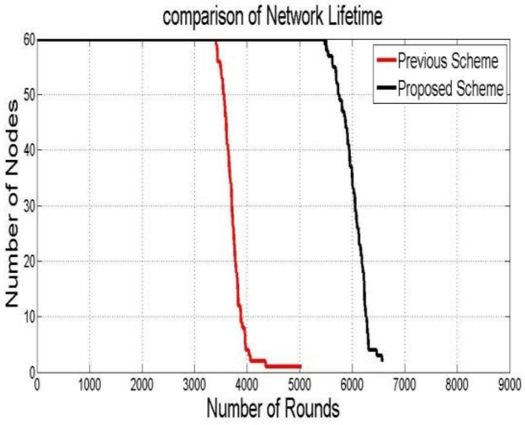

Fig.8. No of Nodes vs. No of rounds

Fig.8 shows a relation between No of Nodes vs. No of rounds. It is being observed that initially 60 nodes are alive in both scheme but later nodes start dying with increase of no. of rounds. Here in comparative analysis of both scheme we find in previous scheme that all of the sensor nodes dies till 5000 round. whereas in proposed scheme as graph show all nodes are alive still 5000 round and it dies all at 6800 round therefore it signifies that our proposed scheme based sensor have more durability to work in comparison to previous scheme.

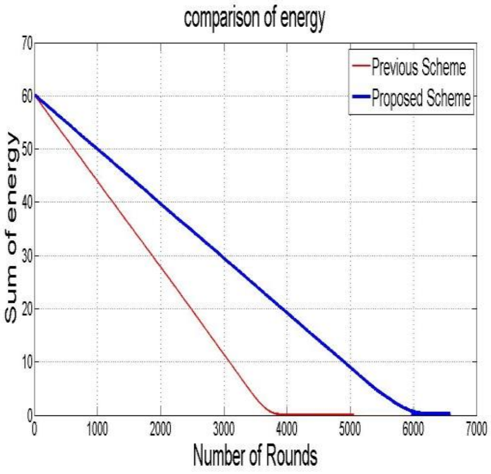

Fig.9. Sum of Energy vs. No of rounds

Here we have another Fig.9. Showing relation between sums of energy vs. No of rounds. It has been observed from graph that initially we have 1KJ energy per node i.e. aggregate sensor network energy is 60 KJ. We can analysis from the graph that in previous scheme nodes aggregating energy dissipated completely at 5100 round which cause to sensor network dies soon. Whereas on the other side in our proposed scheme nodes still have aggregating energy 10 KJ and still operating, it dies at near about 7000 round. So we can conclude on the basis of graph reading that previous scheme based node network alive for short duration in comparison to previous scheme as node exhausted very soon. Causes behind the sensor energy frequently dissipation are as follows:

a) Extra computation load arises on node due to fake packet injection
b) Single hop communication for packet delivery
c) Random order for cluster head selection

Fig.10 shows a relation between packet delivery rate vs. Simulation time. Here after the graphical analysis we found that our previous scheme exhibiting low packet deliver rate in comparison to proposed scheme as in proposed scheme we have 80%, 85% of packet delivery rate then previous scheme shows range of 62-67% rate.

Here Fig.11 and Fig.12 showing throughput and congestion level of both scheme. We know that through put rate is directly impacted by the congestion level in network. Therefore after having a graphical analysis of both scheme, we find that previous scheme showing high packet drop and minimum through put due to rising of congestion level.

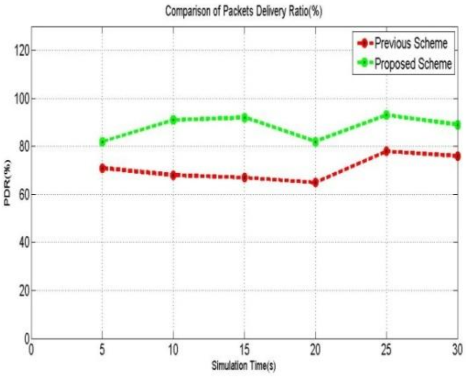

Fig.10. Packet delivery rate vs. Simulation time.

The reason behind is that previous scheme is not energy efficient. Therefore due the non-availability of sufficient energy required by nodes. Each cluster head node cannot successfully deliver packet to destination successfully, therefore packet start dropping at sensor local buffer level and network level which cause high traffic queue inside the network.

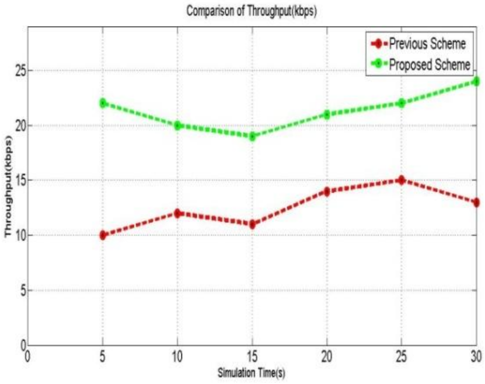

Fig.11. Throughput vs. Simulation time

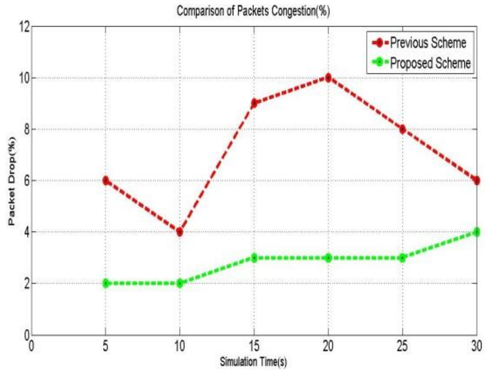

Fig.12. Packet drop vs. Simulation time

V. CONCLUSIONS AND FUTURE SCOPE

We have proposed the energy efficient sink location privacy scheme (EESLP) for hiding the sink location. This is an approach which not only conceal sink location but also improves the energy issue in WSN. Limitation of energy is a prime factor which severely impact the sensor network life time and Qos (packet delivery rate, congestion, and throughput) in WSN. We have observed and done comparative analysis of both scheme through graphical representation and find that how the availability of minimum or maximum node energy in both scheme impact sensor network life as well as QoS values. These are the following optimizations we performed by adopting EESLP approach

- Reduce energy consumption among node which increase in network life time while concealing the sink location
- Increase sensor operation durability.
- Resolve the Tradeoff between energy and security.
- Reduce the congestion level so that throughput and packet delivery can be increased.

We have observed the high network traffic load at sink node while packet routing from cluster heads to sink. Which cause high inter-cluster traffic interference that leads to data collision and congestion at sink location. So there is a scope to further work on it, along with it some enhancements can be done in context to increase the sensor network lifetime by use of solar technology.

VI. ACKNOWLEDGMENT

The authors of this paper wish to acknowledge department of Computer Science and Engineering, Graphic Era University, Dehradun, India for all the facilities provided for this research work.

REFERENCES

1. Hart, J. K., & K. Martinez, “Environmental Sensor Networks: A revolution in the earth system science”, Earth-Science Reviews, pp. 177-191, 2006.
2. Bokareva, Tatiana, Wen Hu, Salil Kanhere, BrankoRistic, Neil Gordon, Travis Bessell, Mark Rutten, and Sanjay Jha, “Wireless sensor networks for battlefield surveillance”, In Proceedings of the land warfare conference, pp. 1-8, October 2006.
3. Ozturk, Celal, Yanyong Zhang, and Wade Trappe,“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.
4. Jian, Ying, Shigang Chen, Zhan Zhang, and Liang Zhang. "Protecting receiver-location privacy in wireless sensor networks", In IEEE INFOCOM2007-26th IEEE International Conference on Computer Communications, pp. 1955-1963. IEEE, 2007.
5. Kamat, Pandurang, Yanyong Zhang, Wade Trappe, and CelalOzturk,“Enhancing source-location privacy in sensor network routing”, In 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05) pp. 599-608, IEEE, June 2005.
6. Deng, Jing, Richard Han, and Shivakant Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks", Dependable Systems and Networks, International Conference on. IEEE, 2004.
7. Shakshuki, Elhadi M., Tarek R. Sheltami, Nan Kang, and Xinyu Xing ,“Tracking anonymous sinks in wireless sensor networks”, In International Conference on Advanced Information Networking and Applications, pp. 510-516, IEEE, May 2009.
8. Reed, Michael G., Paul F. Syverson, and David M.,Goldschlag ,“Anonymous connections and onion routing”, IEEE Journal on Selected areas in Communications, pp.482-494, 1998.
9. Wu, Xiaoxin, Jun Liu, Xiaoyan Hong, and Elisa Bertino. "Achieving anonymity in mobile ad hoc networks using fuzzy position information", In International Conference on Mobile Ad-Hoc and Sensor Networks, pp. 461-472. Springer Berlin Heidelberg, 2006.
10. Perrig, Adrian, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E. Culler, “SPINS: Security protocols for sensor networks”, Wireless networks, Vol. 8, No. 5, pp.521-534, 2002.
11. Eschenauer, Laurent, and Virgil D. Gligor, "A key-management scheme for distributed sensor networks", Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47, ACM, 2002.
12. Deng, Jing, Richard Han, and Shivakant Mishra ,“Countermeasures against traffic analysis attacks in wireless sensor networks”, In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), pp. 113-126, IEEE, September 2005.
13. Nezhad, Alireza A., Dimitris Makrakis, and Ali Miri, “Anonymous topology discovery for multihop wireless sensor networks”, In Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, pp. 78-85, ACM, October 2007.
14. Younis, Mohamed, Moustafa Youssef, and Khaled Arisha, “Energy-aware management for cluster-based sensor networks. Computer networks”, Vol. 43, No. 5, pp.649-668, 2003.
15. Prabha, Divya, and Vishal Kumar Arora, “Enhancement of Network Lifetime Using Multihop Clustering Routing in WSN”, International Journal of Advanced Research in Science and Engineering,Vol. No. 4,September 2015.
16. W. Heinzelman, A. Chandrakasan and H. Balakrishnan, “An application specific protocol architecture for wireless micro sensor networks”, IEEE Transaction on Wireless Communications, vol. 1, pp. 660-670, 2002.
17. J. Gnanambigai1, Dr. N. Rengarajan2, K. Anbukkarasi3, “Leach and Its Descendant Protocols: A Survey”, International Journal of Communication and Computer Technologies, Vol. 01, No. 3, 02 September 2012.
18. Amit Bhattacharjee, BalagopalBhallamudi and Zahid Maqbool, “Energy- Efficient Hierarchical Cluster Based Routing Algoritham in WSN: A Survey, “In International journal of Engineering Research & Technology (IJERT), Vol.2, Issue 5, pp.302-311, May 2013.
19. M. Aslam, M. B. Rasheed, T. Shah, A. Rahim, Z. A. Khan, U. Qasim, M. W. Qasim, A. Hassan, A. Khan, N. Javaid, “Energy optimization and Performance Analysis of Cluster Based Routing Protocols Extended from LEACH for WSNs”, September 2013.
20. Rajesh Patel, Sunil Pariyani and Vijay Ukani, “Energy and Throughput Analysis of Hierarchical Routing Protocol (LEACH) for Wireless Sensor Network”, International Journal of Computer Applications, April 2011.
21. Malviya, Abhishek R., and Balaso N. Jagdale, "Sink Location Privacy Protection in Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, Issue 2, February 2015.