Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(CBCDR)CLUSTER BASED CYCLIC DIVERSIONARY ROUTING: ENERGY EFFICIENT ROUTING STRATEGY FOR LOCATION PRIVACY

C. NAVANEETHAN, M. BABAJAN, G. VINOD KUMAR, P. SARATH REDDY

Vellore Institute of Technology University, Vellore, India

E-mail: navaneethan.c@vit.ac.in, mogal.babajan2013@vit.ac.in, gubba.vinodkumar2013@vit.ac.in, pottim.sarath2013@vit.ac.in

ABSTRACT

A Wireless Sensor Networks (WSNs) is a network of sensors which sense the surroundings and communicates the information gathered from the monitored field through the virtual medium. The system designed for communication should utilize less energy. Sensors in the field are very small and can utilize the energy for constraints like receiving, transferring, and data processing. Based on the contextual information during data transmission, the location of monitored objects and sinks has been disclosed to an adversary. So that protecting the location from strong adversary is an important task.In general providing location privacy from a strong adversary will consumes high energy and also reduction in network lifetime. This paper aims at reducing energy consumptions by using the clustering technique. For this, we use hotspots generating routing paths in areas away from sink which balances energy consumption in overall network. The analysis and simulation upshot that the cluster based Cyclic Diversionary Routing (CDR) can significantly increase the security for location by reducing the energy consumption without effecting the network lifetime.

Keywords: *WSNs, CBCDR, Source-Location privacy, Energy, Network Lifetime.*

1. INTRODUCTION

A WSN is a network with a distribution of sensor nodes where the data can be sensed, processed and conveyed to its interested nodes. Now-a-days Sensor Networks plays a vital role in many applications such as military surveillance, environment monitoring and security. Sensor networks are used in data transmission and gathering from source to sink in efficient way. However these networks are encountered by many threats such as lacking of security, direction disrupting, target tracking and data modification. These threats are of two types i.e., first one is, Active attacks [14], where the data can be modified by injecting additional data or duplicate messages can sent to the sinks resulting the data received is malfunctioned. To reduce these attacks we are having many encryption and decryption techniques and Second one is Passive attacks, where the message stream can be observed by the eavesdropper but cannot be modified, resulting tracking the path of data. These passive attacks can be overcome by using location privacy techniques.

In general the data over any network consist of content as well as contextual information, where the content of the data is moving over the network after performing encryption, which can reach the sink efficiently and accurately with the help of proper keys. Whereas the contextual data does not having any security. By using the contextual information a trespasser can explore either the source location or sink by tracing the path of the contextual information. For example consider a network consisting of n nodes, the data is transmitted between sources and sink via these node. While the data is transferring among nodes in the network, the adversary can collect the information related to the path and can identify the locations of source and sink that depends on the capacity of the adversary.

Recently we have many techniques such as fake packet generation, proxy nodes to protect the location against strong adversary, but these methods leads to degradation of the network lifetime. So along with the location privacy, network lifetime is also to be considered as important criteria.

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In this discussion our focus is on location privacy and network lifetime which gives balanced energy consumption of a network with the help of diversionary routings [6]. In this diversionary routings we are confusing the adversary to protect the location and increasing network lifetime. The following are the techniques used in this paper:

1. Forming of clusters, selecting the cluster head and cyclic based diversionary routing
2. We conduct extensive simulation, Analysis and simulation results shows the improvement in security towards location privacy and also gives better network life time with balanced energy consumptions

The residual of the paper is as follows - Related work, System model, proposed work, Results and algorithms, Conclusion and References.

2. RELATED WORK

In recent years data transfer over networks is increasing rapidly moreover the threats for the data also increasing in the same order. One of the main threats is location privacy. Here the attackers will locate the source or sinks location based on the contextual information. There are two types of attackers i.e. Local eavesdroppers and Global eavesdroppers. Local eavesdroppers are the one who can perform their attacks in small areas as their coverage is limited to some area where they initiates the task from sink and comes towards the source hop-by-hop by gathering the previous nodes information. The strong adversaries are the one who are effective when compared to local adversaries. The methods used in location privacy against local eavesdropper cannot affect the schemes of global eavesdroppers.

To provide the privacy for the location there are many techniques some of them are discussed here:

k-anonymity [1] and private information for Location-based services and fake packet generation [2] which uses dummy packets to confuse the adversary.

Phantom single path routing [2], in which the packets travels through different random paths before reaching to the destination.

Li and Ren [3] proposed a three two phase dynamic routing, here they send the packets to the far away node which is away from source and then to destination by using a single path routing technique.

Deng et al. [4] introduced a technique for location privacy by means of *multi parent routing scheme, controlled random walk scheme, hot spot scheme, and fake packet scheme* [15] which protect the receiver's location where they assumed that adversary as a local.

Mehta et al. [5] presented two techniques for source location privacy – periodic collection, in which nodes send packets to destination that it has actual data to send or not and source simulation, in which we create multiple paths to divert the adversary. Similarly they proposed two techniques for sink location privacy – sink simulation, in which they hide the traffic of original sink and objects by creating the multiple traces in the directions of dummy sinks and back bone flooding, in which they send the packets to the selected portion.

Yang et al. [7] proposed a technique proxy filtering, it include the proxy sensors which can filter the fake packets while arriving to sink, placing the proxies optimally leads to NP-Hard problem which shows the impact on the network lifetime.

The above mentioned techniques will provide location privacy against the strong adversaries but the consumption of energy is high which leads to degradation of network lifetime. Considering energy as a main constraint of the network, our CBCDR scheme will form the clusters which can provide the cyclic diversionary routing paths, where the cluster heads (CH) are selected and these CH will acts as a dummy to refine the fake packets which are delivered by dummy sources.

3. SYSTEM MODEL

The following are the assumptions in sensor network:

(1) The WSNs consisting of sensor nodes that are dispersed in a 2-dimensional space and unable to get the energy resources after deployment.
(2) We assume nodes to be defined with GPS connection so that they can know about the location whenever they need.
(3) We assume that adversary cannot attack the nodes which are in one hop range of distance away from the sink and we need not maintain uniform energy absorption in between the nodes.

The following are the constraints needed to neglect:

(1) Size and density of the network.
(2) Spreading of energy between nodes and node probability of cluster head.

Providing a security to the content of data is out of scope.

Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Energy Consumption Model

A network comprises of many nodes in which every node perform transmitting, receiving and processing, main constraint consider for this process is energy consumption. In our work we are going to consider energy which is being used for transmission and receiving of data. As per the radio model [8] energy consumption for transmission is given as follows

$$E_t^{l,d} = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & ;if\ d < d_0, \\ lE_{elec} + l\varepsilon_{amp}d^4 & ;if\ d > d_0, \end{cases} \quad (1)$$

where E_{elec} is circuit loss during transmission. Free space (d^2) and multi path fading (d^4) are taken as channel models. ε_{fs} and ε_{amp} are the energy parameters of power. The usage of energy for receiving l bit packets is

$$E_r^{\ l} = lE_{elec}. \quad (2)$$

4. THE CLUSTER BASED CYCLIC DIVERSIONARY ROUTING SCHEME (CBCDR)

Here, we discuss about CBCDR scheme for providing location privacy and optimizing the lifetime of the network. The principles to be followed for this CBCDR are: (1) All the diversionary routing tracks [6] and original data routing tracks must be homogenous such that there may be no chance to distinguish the nodes by their sizes and shapes. By this, in at any time during gathering period the security for a network get improved. (2) We know that the energy life time of whole network depends on the energy at hotspots, our scheme don't lay the over burden on the hotspots. (3) The area far away from sink will consume less energy; it must be reduced by making the use of large amounts of energy. These principles will provide us a maximum life to a network along with security.

4.1. Overview of the CBCDR scheme

To perform the fake packet traffic without affecting lifetime of the network, here lifetime means the duration of last hotspot node to run out of the power [9]. Also we know that the fake packet traffic directly effects the whole network lifetime directly. In order to maintain the security at peaks the fake packet traffic must be high which shows impact on network lifetime. In CBCDR scheme, the cluster heads are used to dribble fake packets. In this case, considering the intercluster data flow and neglecting the data generated for interference in the network will always maintain the system at moderate level [6]. By using this scheme, even after diversionary routing energy levels of the system are balanced.

We split the entire region into rings depending on the hop count that is from source (sensor) to sink and establish the CBCDR at various levels (with variable probability). The main theme of the work is as follows: (i) select certain area as hotspot around the sink and divide the remaining area in rings into clusters apart from the hotspot and select the cluster heads. One of the cluster heads in outer most rings can be labeled as *Forwarder*. (ii) Whenever the object appears in a ring it will form an interference route while the nodes in hotspot will act as a relay that can pass the real data to sink. The remaining rings are suppose to form the CBCD route that have the probability p_i , at the same time the sensors will send the dummy packets to the cluster heads with probability q. (iii) At last data transmission will start to sink with one fake packet. When the data packet arrives, it will establish a CBCDR and travel around to gather information from all cluster heads in a ring. Then the data will get transferred to cluster head of next ring in it next hop. If not, it route the data to inner ring immediately.

***Advantages of CBCDR*:** Increased network lifetime, more secured.

4.2. Description of CBCDR scheme

We proposed a cluster based CDR for location reclusiveness and increasing the network lifespan. Here this scheme is divided into 3 sections, (1) generation of clusters and selecting cluster head, (2) intra cluster data aggregation, (3) establishment of route.

As we described in the overview of CBCDR scheme, here we consider an area which is divided into several rings with certain count of nodes in each ring. But here we considered rings as hotspot ring, outermost ring and other rings between them, to represent the total area as shown in figure:1.

4.2.1. Generation of Clusters and Selection of Cluster Head

Every network with sensor nodes has bounded energy, increasing the network's life and scalability is a main task which will improve the performance of the whole network. Here we use Distributed Weight Based Energy Efficient Hierarchical clustering protocol (DWEHC) [12- 14].In this algorithm, each and every node finds it neighboring nodes and selects one among the neighbors as cluster head. The procedure for selecting the cluster head is: first we calculate the weights of neighbor

Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes based on its residual energy and how much far the node is, second is the largest weighted cluster node is selected as cluster head. The remaining nodes other than cluster node in a cluster will join the hierarchy. The cluster process described in the algorithm below takes O(1) process which does not depend on network size and structure. The structure of cluster is as follows:

In clustering, let R be the radius of a cluster where radius means the distance of farthest node from the clusterhead throughout the network. Selection of the clusterhead mainly depends on *weight* of nodes. The calculation of weights depends on the distance *d* between the source and neighboring nodes *N* and also depends on the remaining constraints, initial energies of source node E_{res} and E_{ini} respectively, the formula to calculate the weight of node is:

$$Weight = \left(\sum_N \left(\frac{R-d}{6R}\right)\right) \frac{E_{res}}{E_{ini}} \quad (3)$$

Clusterhead will collect the data from its child nodes and transfer it to neighbor cluster, which consumes more energy. The residual energy plays a key role in selecting the clusterhead. And also the energy rely upon number of nodes in a single cluster; hence one must maintain a cluster with limited number of nodes in it. In each cluster, the distance between each child node must be located in the range of clusterhead. The *range* of clusterhead is given as

$$\text{range} = \sqrt{(CH\_x - x)^2 + (CH\_y - y)^2} \quad (4)$$

dist is the distance of minimal energy towards clusterhead

dist = neighbours dist + (distance towards neighbour)^2 (5)

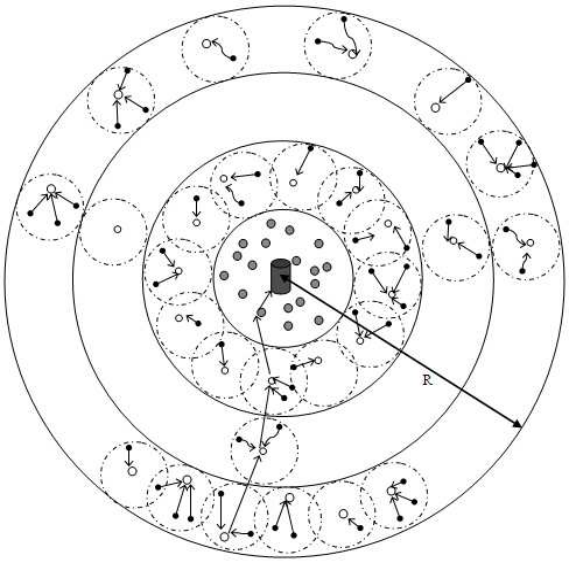

Fig.1. Sketch Of CBCDR

Features of clustered network:

- In a cluster, every node is either a CH or a child for CH.
- The clusterheads are distributed all over the network.
- Cluster is designed with a topology having minimum energy with limited number of child nodes.

After clustering, the clusterhead is labeled as "*Forwarder*". By using token ring protocol [10, 11],

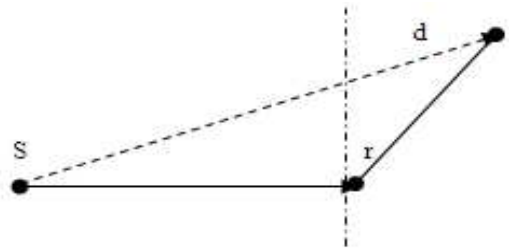

Fig.2. Relay through node r

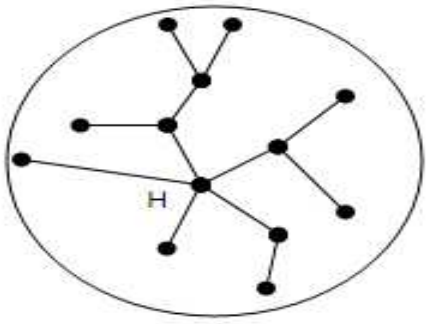

Fig.3. Levels in DWEHC

Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Notations

id, (x, y) – represents id, (x, y) x and y axis of node.
level, weight, range – node's level and weight, range is the distance to the CH
dist – distance with min energy towards the CH
tmp_CH – a node will be temporary head tmp_CH = 1;
CH_num – assigns temporary CH id for the neighbor nodes
per – proportion of node becoming temporary CH
tmp_CH_id – temporary cluster head id
CH_x, CH_y – coordinates for the cluster head
direct_parent – id of the direct parent node
maxlt : maximum limit for the neighbors

Algorithm:

1- Plot the two dimensional coordinates;
2- Gather the cluster nodes;
3- Find the neighbors in a cluster:
4- Find the weights and distribute them;

Generation of clusters

5- For(i=0; i<maxlt; i++){
5.1. If level = -1 {
5.1. a. If weight is highest compared to neighbors then
{
tmp_CH = 1;
CH_num = id;
}
Else
{
tmp_CH = 0;}
CH_num = tmp_CH_id;
}
5.1. b. distribute CH_num;
5.1. c. If ((per ≥ maxlt-i/maxlt & tmp_CH = 1) | (zero neighbours) | (neirgbour's level > -1))
{
level = dist = 0; CH_x = x; CH_y = y;
//for original CH
distribute level, dist, CH_x, CH_y;
} //end 5.1.c.
}//end 5.1
5.2 If (level <> 0)
{
Receive data from neighbor;

$$\text{range} = \sqrt{(CH\_x - x)^2 + (CH\_y - y)^2};$$

dist_new = neighbors dist + (distance towards neighbour)^2
If((dist_new<dist & level > 0)|(range <= range of cluster & level = -1))
{
level = level of neighbor + 1; dist = dist_new;
direct_parent = id of neighbour;
CH_x and CH_y = neighbour's CH_x & CH_y;
distribute level, dist, CH_x, CH_y;
}
}//end5.2
}//end 5
6- Do the above process for one more time;

the Forwarder in outermost ring can be selected which can passes the token hold by it to the clusterheads in the course of clustering.

At the beginning of all periods, first ring and all other rings except the ring at which the object appears will perform the CBCDR with probability *p*. depending on this the sink will get an idea about the routing information and distribute the data over the network.

4.2.2. Intra cluster Data Aggregation:

Based on the information at the beginning, the clusterhead which is in the rings with interference begin to collect the information from the cluster nodes. Here the cluster members rather than the real data will convert to fake packet generators with a probability of *p* that can forward fake messages to their respective clusterheads. Here the nodes which are participating in intracluster communication will confuse the adversary. However fake packet generations will consume high energy, so to maintain a trade-off between consumption of energy and security. It can be reached by interference routing where the dummy packets generated by randomly selected nodes will send the message to cluster head, cluster head will dump the fake packets and holds only the real messages where the data can be sent safely.

4.2.3. Establishment of route

After completion of data aggregation which is intracluster, the data forwarding is started by the Forwarder in outermost ring. Initially the network will decide to generate the interference based on the information during initial stage. If a network decided to schedule the interference in the ring then the Forwarder will start data transmission to its next hop and the hop that receive the data will forward it to the next hop which is continued for all iterations. While forwarding to next hop, clusterhead will check for the data whether it is correct or not, if the received data is real then it will release the dummy packet and transfer the original data that it received else the received data will directly transferred to next hop. The CBCDR is said to be completed when the data received to the Forwarder again. The promoter in the present ring will try to forward the

Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

data to a ring which is nearest to the sink and that is ring must be an adjacent one. The clusterhead that received the data from its upper ring will also make a decision as the clusterhead in upper ring performed. During this if no interference route is existed then the data will be forwarded to the inner ring which is nearest to the sink. By following this pattern of routing, the data will reach the sink safely.

However in the first iteration the interference routing is done, but in next iteration there is a chance for an adversary to depict the location based on the strong properties such as correlation of time and rate of monitoring, by which the ring that generates the real object can be detected. To avoid this, a distribution scheme is included in CBCDR, where the interference routing can be generated even if the object is in the corresponding ring. The whole algorithm is as below:

CBCDR routing

Stage-1:

1.1- Let L_n be the ring with objects Inter $f_{L_n} \leftarrow 0$, and Inter $f_{L_n} \leftarrow 1$;

1.2- Perform the following: for all levels except L_0 and L_n

1.3- Decide the probability p_i for Inter f_{L_i};

1.4- End for;

1.5- From outer most ring select a node N_j randomly for holding the Forwarder's token i.e. $pt = N_j$;

1.6- Distribute Inter f and pt among all the sensor nodes;

Stage-2:

2.1- Clustering starts with the help of DWEHC Algorithm;

2.2- After performing clustering, the Forwarder node delivers the token to cluster head;

2.3- For (all cluster nodes in each cluster)
{
Fake message is transmitted to cluster head having a probability q;
}

Stage-3:

3.1- For each sensor s which stays in ring r do

3.2- transmit = 0;

3.3- If(s = cluster head) then

3.4- If (Inter f_{L_r} == 1)
then
s transfer the data to its neighbour CH which is right side of s
Else
s will transfer the data to the CH in the lower ring which is nearest to sink;// End if

3.5- transmit = 1;

3.6- else If
(s receives data from its upper ring)
then
If(Inter f_{L_r} == 1)
Then
If s receives original data then it leaves the dummy packets and sends the original packets which is received to next hop,
If not
the fake data is transferred.
Else
If(s receive real packets)
then
it leaves the dummy packets and sends the real data which is received to lower ring,
If not fake data is transferred to lower ring.//End if;

3.7- transmit = 1;

3.8- else If (s receives data from same ring)
then
If (transmit ==1)
then
S transfer the data to lower ring
Else
If (s has real packets)
then
releases the received dummy and send the original packets to next hop of same ring,
If not
send dummy to next hop;//End if;

3.9- transmit = 1;

3.10- End if

3.11- End if

3.12- End for

5. ANALYSIS

5.1. Analysis for energy

By using CBCDR we can easily confuse the adversary from tracking the location. For this the ring will generate the routing of interference with a probability p_i and the cluster must send the fake packets in ring with a probability q. In CBCDR we have three sections: clustering, data aggregation and route establishment. The energy consumption in a network is discussed as follows:

Let the energy consumption for the nodes in a cluster be $E_{cluster}$, for nodes in i^{th} ring the average energy consumed by the nodes is given by,

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

If i = 1 then,

$$E_{i(avg)} = \frac{E_t^{\sigma\frac{r}{2}} + E_r^{\sigma}}{\pi r^2 \rho};$$

else

$$E_{i(avg)} = E_c + \left(P_i q\left(N_i - N_i^c\right)\left(E_t^{\sigma\frac{r}{2}} + E_r^{\sigma}\right) + P_i N_i^c\left(E_t^{\sigma r} + E_r^{\sigma}\right) + E_t^{\sigma r} + E_r^{\sigma}\right)/N_i$$

Where, $N_i = A_i\rho = \pi\rho(2i-1)r^2$

$N_i^c = \frac{A_i}{A_c} = \pi(2i-1)r^2/\pi(r/2)^2$

A_i = Area of the i[th] ring with diameter r,

A_s= Area of each cluster,

N_i = Number of clusters in each ring,

The cluster and clusterhead will consume some amount of energy which is given by,

$$e_t^{cluster} = qE_t^{\sigma\frac{r}{2}}$$

$$e_r^{clusterhead} = E_r^{\sigma}$$

For routing the average energy consumption in i[th] ring is

$$e_i^{cdr} = N_i^c\left(E_t^{\sigma r} + E_r^{\sigma}\right)/N_i$$

When the probability P_i is taken into consideration then the energy consumption of CBCDR of the i[th] ring is

$$E_i^{cdr} = e_i^{cdr} P_i$$

Energy consumption for the routing the data to inner ring is

$$E_i^{sink} = \left(E_t^{\sigma r} + E_r^{\sigma}\right)/N_i$$

By adding all the equations given above we will obtain the total energy equation.

For improving the location privacy without disturbing network lifespan [9] energy consumption should meet the following criteria:

$$E_i^{avg} = E_{i+1}^{avg} \qquad i \in 2 \text{ to } m-1$$

$$E_i^{avg} \leq E_1^{avg} \qquad i \in 2 \text{ to } m$$

Although several routes are present, we observe that lifetime of the network is same as shortest path routing.

6. RESULTS

In this section, we first form a network with the help of a simulator where the network looks like a circular area, this area is partitioned into circles, and these circles are taken as ring. The nodes are distributed over the network that covers whole region which are homogenous in nature. The properties of nodes are considered to be unique. Establishing the sink in the middle of the network by which it can receives the data from whole network. The density of nodes in the network must be in the way, that high densities near the sink and less dense in the area far away from sink. The first ring will acts as hot spot due to its dense distribution of nodes. The nodes apart from the hot spot area must be distributed in such a way that each and every ring must contain a count of nodes. Then clustering will come into action where the area in the every ring is divided as clusters except the area which is in hotspot such that the outer most rings is communicated with the inner rings and sink. The parameters required for the network are radius of the ring (R), cluster range (r), density (ρ), no. of bits (σ) and we define the radius of cluster as half of its transmission. The total circular network is taken in a square region with an area of 4 times the range of the ring. According to location privacy scheme [5, 16] the network is divided into number of cells using two level trees. By considering energy as criteria general packet generators are selected and remaining are fake packet generators which is in the ratio of 4:1. The buffering time for a proxy node is taken as 5 times of delay in transmission.

In clustering according to laws of wireless transmission attenuation power is proportional to square of range covered. If the range of cluster is less the attenuation factor is in a linear manner and cluster head selection will also forms an energy criteria based on energy remained. By using DWEHC algorithm we can perform clustering where inter and intra cluster transformation takes place which is explained in algorithm above. The ranges of energy utilization for inter and intra cluster transformation is plotted in the graphs given below with respect to HEED which creates overhead between cluster heads and sink while transmission. Due to the overhead between cluster head and sink the interference routing is decreased which results in higher energy utilization. By using DWEHC in clustering process the network will remains for higher period which shows network is energy efficient.

Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

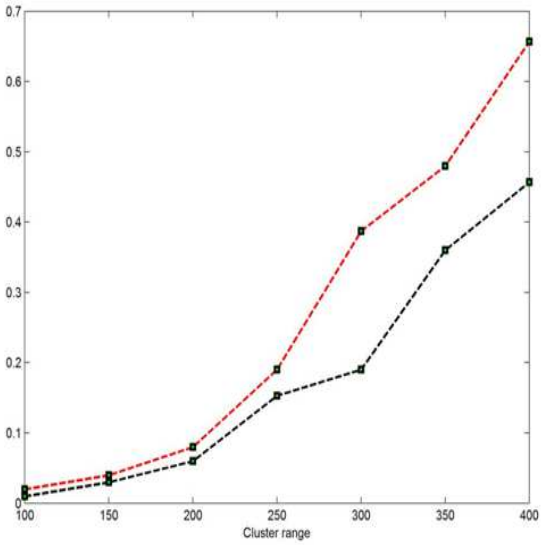

Fig.4. Average Energy For Intracluster

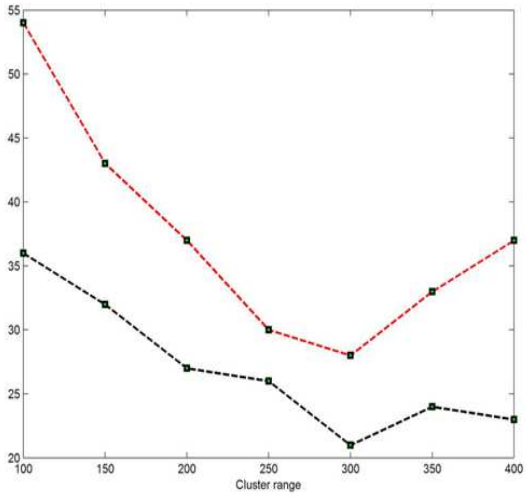

Fig.5. Average Energy For Intercluster

For diversionary routing, fake generators are created to improve security in network. Even, for improving security the energy is highly utilized which can be analyzed by verifying relations of probabilities P_i and q during data aggregation. There will be a correlation which is not positive leads to higher energy utilization. We are also considering hotspot's energy utilization since they are located in initial rings i.e. one hop region from the sink. If we maintain less energy utilization in the first hop region network lifetime is maintained. Apart from hotspot the outer ring also maintained to consume less energy.

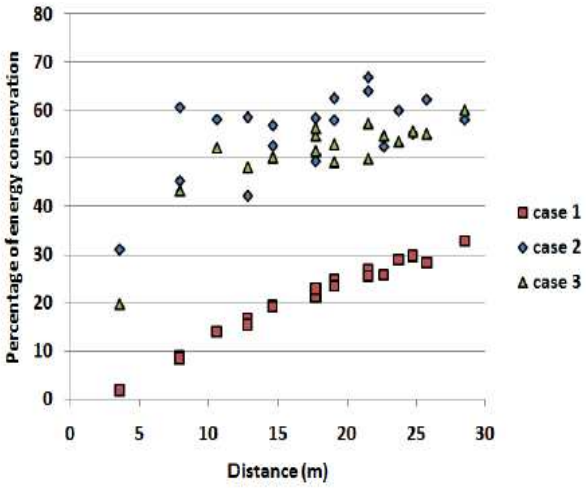

Fig.6. Energy Consumption Along The Distance Of Rings

Regarding the security, due to fake packet generation during data aggregation the transmission delay is high in one period. Due to this delay and fake packet generators the adversary gets confused by which the security is achieved. If we increase the range R then the security is decreased. So, we want to maintain the range in limited value.

7. CONCLUSION

In this paper, we proposed cluster based cyclic diversionary routing scheme (CBCDR) which depends on clustering and diversionary routing against strong adversaries in WSN which provide location privacy. This scheme utilizes the energy which is remained in areas far from sink by which many cyclic routes are created that confuses the adversaries and provide the privacy with balance energy utilization and also we increase network lifetime with the help of last hotspot running out of power.

Above works specifies that network is very strong against strong adversary. The directions that we have a chance to focus are: the delay of the routing is not taken into consideration that is optimization of network latency and location privacy for moving nodes.

8. REFERENCES

[1] B. Bamba, L. Liu, P.Pesti, and T.Wang, "Supporting Anonymous Location Queries In Mobile Environments with Privacy Grid," Proc.Int'l Conf. World Wide Web(www '08), 2008.

[2] P.Kamat, Y.Zhang, W.Trappe and C.Ozturk, "Enhancing Source-Location Privacy In Sensor Network Routing," Proc .Int'l Conf.

© 2005 - 2014 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Distributed Computing Systems(ICDCS '05), June 2005.

[3] Y.Li and J.Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in Proceedings of the IEEE CONFERENCE on Computer Communications (INFOCOM '10), San Diego, Calif, USA, March 2010.

[4] J.Deng, R.Han and S.Mishra, "Decorrelating Wireless Sensor Networks Traffic to Inhibit Traffic Analysis Attacks," Pervasive and Mobile Computing J.,Special Issue on Security in Wireless Mobile Computing Systems, VOL. 2, pp.159-186, Apr.2006.

[5] K.Mehta, D.Liu, and M.Wright, "Location privacy in sensor networks against a global eavesdropper," in Proceedings of the 15th IEEE International Conference on Network Protocols (ICNP/07), pp.314-323, Beijing, China, October 2007.

[6] Ju Ren, Yaoxue Zhang, and Kang Liu, "An Energy-Effiecient Cyclic Diversionary Routing Strategy Against Global Eavesdroppers in Wireless Sensor Networks," in the Proceedings of Hindawi publishing Corporation, IJDSN, Vol.2013.

[7] Y. Yang, M. Shao, S. Zhu, V. Urgaonkar, and G. Cao, "Towards Event Source Unobserbillity With Minimum Network Traffic In Sensor Networks," Proc.

[8] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks," IEEE Transactions on Parallel and Distributed Systems, 2013

[9] Kewei Shah and Weisong Shi, "Modelling The Life time of Wireless Sensor Networks," in the Proceddings of Sensor Letters, VOL.3, 1-10, April 2005.

[10] F. Wei, X. Zhang, H. Xiao, and A. Men, "A modified wireless token ring protocol for wireless sensor network," in Proceedings of the second IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet '12), pp.795-799, 2012

[11] A. Ray and D. De, "Energy efficient cluster head selection in wireless sensor networks," in Proceedings of the IEEE 1st International Conference on Recent Advances in Information Technology (RAIT '12) pp.306-311, 2012

[12] P. Ding, J. Holiday, Aslihan Celik, "Distributed Energy-Efficient Hierarchical Clustering for Wireless Sensor Networks"

[13] G. Sikandar, M. H. Zafar, A. Raza, M. Inayatullah Babar, S. A. Mahmud, and G. M. Khan, "A Survey of Cluster-based Routing Schemes for Wireless Sensor Networks"

[14] C. kaufman, R. Perlman, M. Speciner "Network Security: Private Communication in a Public World," 2nd Edition

[15] A. Jhumka, M. Leeke, and S. Shrestha, "On The Use of Fake Source Location Privacy: trade-offs between Energy and Privacy," Computer Journal, VOL. 54, no. 6, pp. 860-874, 2011.