ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 6, August 2012

Zone based routing protocol in WSNs for varying zone size

Poonam Rautela, Vinod Kumar Mishra, Pankaj kumar
Department of Computer Science and Engineering
Bipin Tripathi Kumaon Institute of Technology, Almora (Uttarakhand)

Abstract-In this paper, we propose a zone based routing protocols for varying zone size. We will increase a size of a zone if the routing path is shorter and decrease zone size if the routing path is larger. If the zone size is smaller it requires larger number of cluster heads and longer path during routing so we vary the zone size according to requirement by increasing or decreasing the radius. Simulation results show the effect of increasing zone radius on received packet and on error rate. We are calculating the number of received packet and error rate for different zone radius. It shows that with increase in the zone radius the number of received packet increases and the error ratio are decreases. If zone size is small and network size is larger it needs more number of zones with the increase in zone number then more zone head are required. So the nodes more communicate with each other to make a zone head for every zone, which result into high battery consumption.

Keywords-Wireless sensor network, zone size, LEACH, zone head, varying zone size, routing protocol.

I. INTRODUCTION

Wireless sensor network contain larger number of sensing nodes such as hundreds or thousands and these sensing nodes communicate with each other or to an external base station. If there is a larger number of sensing nodes it senses a larger number of areas with greater accuracy. Each sensor node has an ability of sensing, processing, transmitting and position finding. These sensors nodes are tightly constrained in terms of processing, energy and storage capacities. Sensors lifetime depends upon the battery lifetime. Sensed phenomenon can be static or dynamic it depends on an application such as it will be static for forest monitoring for fire detection and it will dynamic for target tracking where movement of the sensors are required. As sensor are attaching to a patient or doctor to track and monitor the position of a patient and doctor inside a hospital.

Wireless sensor network are used in a place where human interaction is less feasible [1]. It is used to solve the real world problems as to count temperature, humidity, soil moisture, for monitoring forest fire detection, flood detection, remote health monitoring, It can also be used in military application and in police. WSN is derived from the wireless adhoc network, the adhoc routing protocols have been proposed as routing protocols in WSN. Routing protocols are of proactive, reactive and hybrid [2]. The proactive routing protocol are table driven it pre computes the routes. Each node maintains a routing table for its routing zone, with the help of routinng table it can find a route to any node in the routing zone from this table. Proactive routing protocol have an advantage that it have no delay in the route determination but it has traffic overhead due to the periodic route update. Reactive routing protocol compute route on demend so it has an advantage that it has less traffic overhead than proactive routing protocol. Hybrid routing protocol is the combination of both the proactive and reactive routing protocol [3]. It combines the advantage of proactive and reactive routing protocol. It reduces the proactive control traffic as well as reactive route discovery delay. Zone based routing protocol are example of hybrid routing protocol.

In zone based wireless sensor networks we divide the network into small zones or clusters. It defines zones for every node. Inside a zone, a proactive routing protocol will be used and outside

Manuscript received Aug, 2012.

Poonam Rautela, *Computer Science and Engg., UTU/ Bipin Tripathi Kumaon Institute of Technology. Almora, India*

Vinod Kumar Mishra, *Computer Science and Engg. UTU/ Bipin Tripathi Kumaon Institute of Technology/, Almora, India,*

Pankaj Kumar, *Computer Science and Engg., UTU/ Bipin Tripathi Kumaon Institute of Technology/, Almora,*

each zone, reactive routing protocol will be used [4]. The routing in ZRP is divided into two parts intrazone routing and interzone routing .In intrazone routing the packet is sent within the routing zone of the source node to reach the peripheral nodes and in the interzone routing the packet is sent from the peripheral nodes towards the destination node.

If we used Enhanced Zone Routing Protocol (EZRP) then in this protocol we check the reliability of the route. If the routes are reliable then packets are sending through this route directly without route searching and if the routes are not reliable then we again search for a new route [5]. If we used new zone routing protocol then it reduces the control packet. In conventional routing packets are sent periodically. In this routing protocol the packets are sent only when node moves [6]. If location based protocol are used, in this protocol greedy routing are used which depend upon cost function. And these cost functions are depending upon the shortest path from the source to the destination [7]. If we used Elegant routing protocol then it uses hybrid routing framework. This locally uses proactive routing and globally uses reactive routing protocol [8]. If we used position based routing then in this protocol we integrate the function of mobility and routing [9].

II. RELETED WORK

LEACH: It perform local computation in each cluster so that it can reduce the amount of data that are transmitting to the base station [10]. LEACH is divided into two phase set up phase and steady phase [3], [11], [10]. In the setup phase each node decide for a current round whether or not it will a cluster head or not and it depend upon the threshold. In the steady state cluster head collect data from the sensor nodes then aggregate these data then send it to the base station.

LEACH Centralized: In setup phase the base station receives all information about each node regarding their energy status and location. The base station run local algorithm for the formation of cluster and cluster head and then broadcast the message that contains the cluster head ID for each node [3]. In steady state phase cluster head collect data from the sensor nodes then aggregate these data then send it to the base station.

LEACH Fixed Cluster: The base station receives all information about each node regarding their energy status and location then LEACH-F uses fixed cluster that are formed once in the first setup phase by the base station. Cluster head position rotate and every node become cluster head of its cluster.

TEEN: TEEN is designed to respond to the change in the sensed attribute such as temperature. The cluster head broadcast two threshold to the sensed attribute these are soft threshold and hard threshold [3], [10]. Hard threshold allow the node to transmit data only when it is in the range of interest. It is used to reduce the transmission. The soft thresholds further reduce the number of transmissions if there is a little or no changes in the value of sensed attribute.

APTEEN: APTEEN periodically collect the data. If a node sensed data beyond the hard threshold then it send value only when its value become less than or equal to the value of the soft threshold.

PEGASIS: In PEGASIS it forms chain from sensor nodes rather than forming multiple clusters so that each node transmits and receives from a neighbor and only one node is selected from that chain as leader node to transmit to the base station. PEGASIS allow only local only local coordination between nodes that are close together so that the bandwidth consumed in communication is reduced. PEGASIS decrease the number of transmission and reception by using data aggregation although the clustering overhead is avoided [3][12]. It eliminates the overhead caused by the dynamic cluster formation.

III. ZONE ROUTING PROTOCOL

Zone routing protocol consists of inter zone routing and intra-zone routing. If the packets are send within a routing zone it is called intra-zone routing and if data are send outside the routing zone then it is called inter-zone routing [13][12]. The packets are first send from source node to the peripheral node then from peripheral node to the destination node. The nodes which come under a zone are called in-zone and those who come outside the zone are called out-zone.

In Fig.1, S is the source node, in this node A,B,C,D,E,F,G,H,I and S are inside the routing zone and node J and k are outside the routing zone. In this Fig. node G, H, I and F are peripheral nodes. Peripheral nodes are those nodes which are exactly at a distance as the radius is. In the given figure radius=2 and nodes G, H, I and F are at a distance of 2 hops. Nodes J and K are at a distance of 3 nodes from the centre node S so these node are outside the routing zone of S.

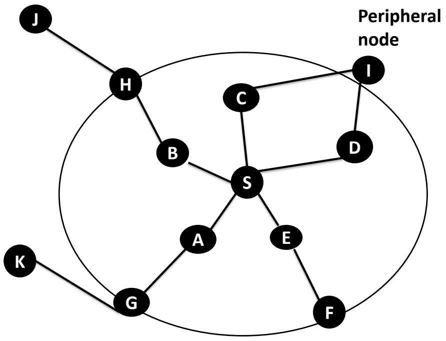


Fig.1 (In-zone and Out-zone of radius=2)

If the data are send within the routing zone then it is called intra-zone routing and if data are send outside the routing zone then it is called inter-zone routing. Fig.2 shows that, if data are send from the source node S to reach the peripheral nodes a, b, c, d, or e then intra zone routing are done and if data are send from the source node to the destination node D then these are done through inter-zone routing. Data are sending inside a routing zone through proactively and outside the routing zone through reactively. That means inside a routing zone a proactive routing protocol will be used and outside a routing zone a reactive routing protocols are used [10].

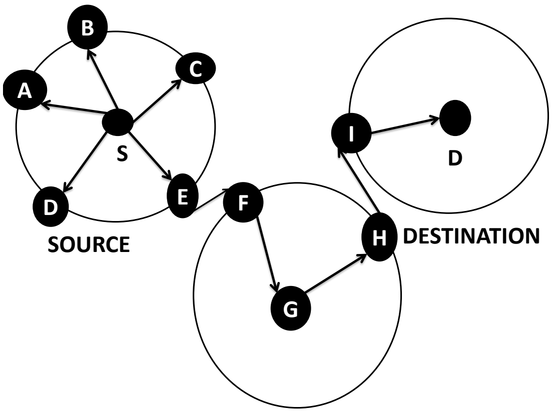


Fig.2 (Intra and Inter-zone routing)

IV. APPLICATIONS OF WSNs

Wireless sensors network have many application. It is used in many places where human interaction is less feasible such as to count temperature, humidity inside the territory, environmental monitoring, flood detection, forest fire etc.

1.) Healthcare applications: - In the healthcare application sensors are used in monitoring and tracking of doctors and patients inside the hospitals [14]. It is used to detect heartbeat and blood pressure of the patient [15].

2.) Environmental applications: - In environmental application sensors are used in tracking and monitoring environmental conditions that affect livestock and crops and the movement of small animals. Wireless sensor networks collect readings over time across an area large enough to exhibit significant internal variation.

3.) Military applications: - In this sensors are used to detect as much information as possible about the enemy [14]. Sensors are used to detect enemy movements, nuclear and biological attack detection, explosions etc. Sensors help to locate the source of incoming fire so that counter attacks can be launched against them quickly.

4.) Traffic Signal: - Sensors are used to detect vehicles and control the traffic lights. It is costly, thus traffic monitoring is usually only available at a few critical points in a city.

5.) Industrial Sensing: - Sensor nodes are used to monitor the health of machines. Sensor nodes can be deeply embedded into machines to ensure safe operation. Rohrback Cosasco System (RCS) apply WSNs in their corrosion monitoring. WSN are also used in food industry to prevent the incidents contaminating the food supply chain.

6.) Home applications: - Sensors can be used in home as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled.

V. ATTACKS ON WSNs AND ITS PREVENTION

1.) **Denial of service: -** It prevents legitimate network users from accessing services or resources to which they are entitled [15], [14], [16]. This attack may have target a particular user or entire network. If the target is particular user an entity may suppress all messages directed to a particular destination and in another case is disruption of an entire network either by overloading the network with messages or by disabling the performance to degrade performance.

DOS can be prevented by strong authentication, identification of traffic and pushback. In this the data are divided into several small data and every data contain the hash of the next message so that the attacker are not able to hijack the ongoing transmission because it is not easy to construct a message that matches the hash contained in the previous message.

2.) Sybil attack: - In a Sybil attack a single node appears as a set of nodes so that the node actual position can't be determine in the network. It shows nodes that do not exist. Detection of Sybil nodes in a network is not so easy. The Sybil attack occur when sensors in a wireless sensor network work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information [15], [14].

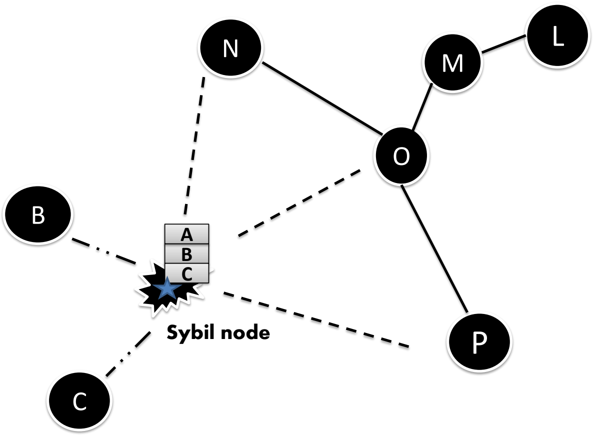


Fig.3 (Sybil attack)

To prevent from **Sybil attack** unique identity are given to every node in a network [15].

3.) Selective Forwarding attack: - In the selective forwarding attack the sensor node doesn't forward many of the data or packet which they received [14]. In this the nodes forwards only the selected data and ignore the rest of the data which cause the loss of lots of data.

To prevent form **selective forwarding attack** multipath routing are used. In the multipath routing the data or packet are send through the path whose nodes are prevented from selective forwarding attack.

4.) Sinkhole attack: - In this the attacker are able to insert itself between the communication nodes. And the attacker can do anything to a packet passing through them. In this the malicious node attract all the traffic it replies to the entire node that it has a shortest path to the destination [15].

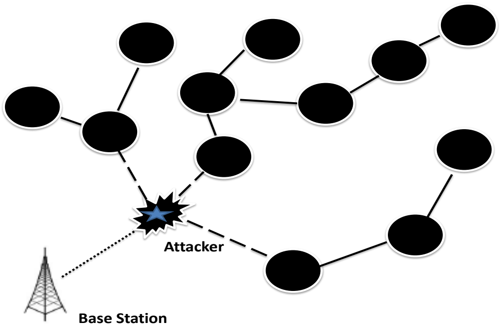


Fig.4 (Sinkhole attack)

To prevent from the **Sinkhole attack** is to use geographical routing protocol.

5.) Wormhole attack: - In the wormhole attack the sender send a route request, attacker node received this request and it to its neighbour nodes [15], [14]. Now the neighbour node of the attacker node think that they are only at one hop distance of a sender node and reply the sender nodes but they are actually at multihop distance of the sender node.

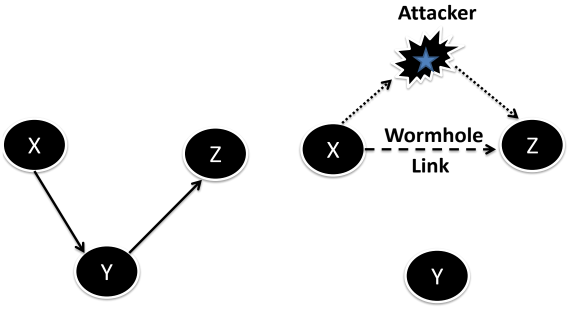


Fig.5 (Wormhole attack)

To prevent from **wormhole attack** a hierarchical tree are made in which the base station are consider as root and the sensor node are internal and leaf nodes.

6.) Hello flood attack: -In this an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN so that a large number of nodes even far away in the network choose it as the parent[15][14].

The **Hello flood attacks are** prevented by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop [15].

VI. NETWORK SETUP

We take a network with a varying zone size so that we can increase or decrease a zone size according to our requirement. Zone size can be increases when the routing path is shorter so that it can cover large distance in less time without path breakage and zone size can be decreases when routing path is larger. Zone size is increase if routing path is larger it may cause path break.

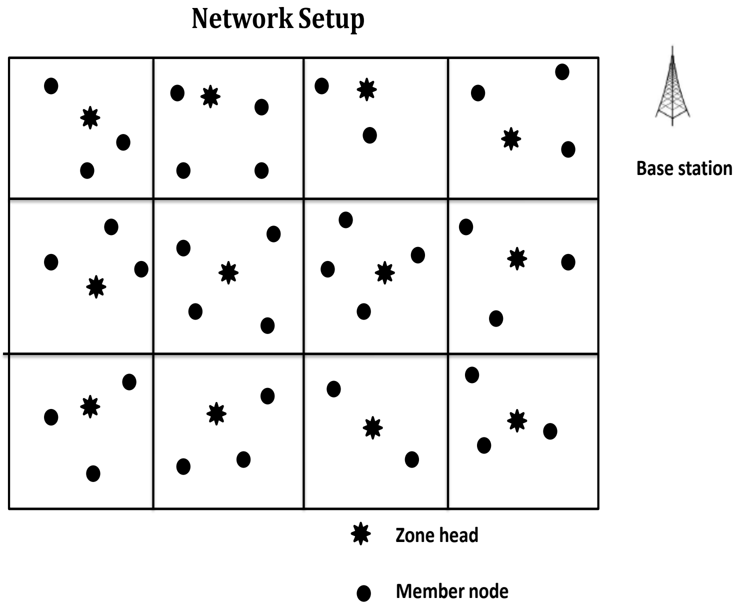


Fig.6. (Network)

We consider a network then divide it into zones. Each zone has a zone head which is used for routing. Zone head are used for routing data to the destination i.e. to the base station [3][12]. Data are transmitted with the help of zone head. Other member nodes are not used for routing. They only transmit data to their zone head within the zone. Within a zone data are sending through intra-zone routing and outside the zone data are sending through inter-zone routing [12].

Dividing network into different zones: When the network is created next step is dividing it into different zones. We are considering varying size of zone. Its size can be increases or decreases as per requirement as when the routing path is larger zone size is increased and when routing path is smaller zone size is decrease. When zone size is small there will be more number of zones in a network and it will take more time to reach data to the destination(Base station) ,which may also cause path breakage. We increase zone size when routing path is larger so that data reach to the destination without causing any path break.

1.) **Creating zone head: -** Every zone has a zone head which is used for routing data to the destination. One node is considered as zone head and all other is simple node. These nodes sends data to their zone head and then zone head send the data to the base station [3], [1]. For to creating zone head we are considering mobility factor. Every node sends its mobility factor to another node within the zone and node which have highest mobility factor are zone head of the zone.

Mobility= Location change/Zone change [3]

Mobility of a node have certain disadvantages as when a zone head of a zone move to different place and another zone head of other zone take its position it may cause error. When a zone head move to different place it may also cause path break. So mobility of a node is note consider adequate but in certain place mobile node are required such as for path tracking. As if we want to track the position of doctor or patient in hospital sensors are attached to them. But in certain place as detection of forest fire mobile nodes are not required. So mobility of a node may be static or dynamic according to the application.

2.) **Routing in the network: -**After creating the zone head routing take place. Data are sending from source to the destination. All nodes within the zone send its data to its zone head. After receiving the data from the different nodes zone head communicate with base station directly or via other zone head by choosing the best path to the destination.

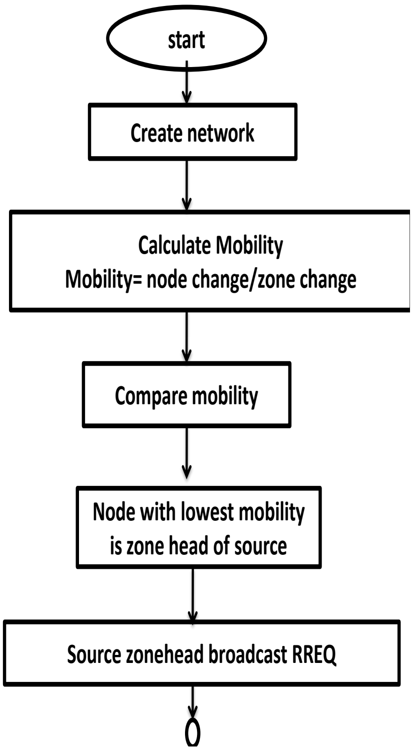
A.)Request for root: - Request for root is generated if there is no root for the base station. In this network the originator ID are the node ID of the originator zone head. Sequence numbers of the originator are zone head sequence number. Destination ID is the ID of the base station. And destination sequence number is the last known sequence number of the base station. In this first route request ID are last route request incremented by 1 and hop count field are set to zero. Then route request are broadcasted until it reaches to the base station. The symbolic form of this procedure is as follows:

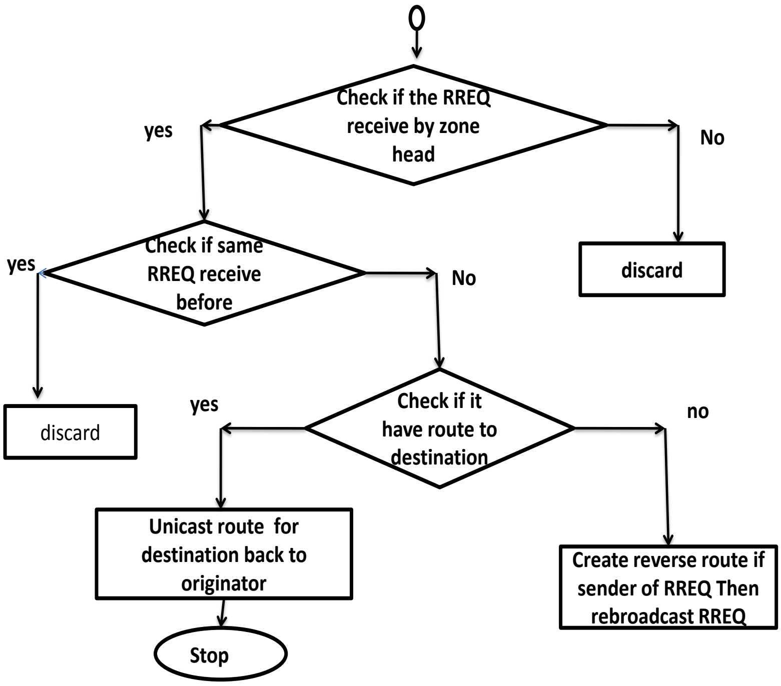
Originator ID→ Node ID of Originator ZH
Originator SeqNum→ Zone head SeqNum
Originator ZoneID→ Zone in which originator of RREQ exists
Destination ID→ID of BS
DestSeqNum→ Last known SeqNum of BS
RREQ ID→ LastRREQ ID+1
Hop Count Field→ 0
RREQ broadcast

B.)Route reply: - When route request are send it is discarded if the node are not a zone head. If route requests are received by the zone head then it first check that the same route requests are received before or not. If the same route requests are received before then it is discarded. And if it is not received before then it send route to the destination if it have. If it doesn't have route to the destination then it create reverse route to sender and rebroadcast it. If no intermediate node has route to destination route request reaches to the base station. Base stations create a reverse route with the sender and then generate a route reply and unicast it toward sender. Intermediate nodes cache the sender in the forward path. Then the data are sending to the base station through these paths.

C.)Route maintenance: - The data are sends through the shortest path to the base station with the help of the zone head.We increase the zone size so that less number of node should be communicate with the zone head which cause less battery consumption means less energy are wasted so the sensors remains alive for larger time i.e with the increase in the zone size the lifespan of the zone are increases. Also with the increase in the zone size the battery consumption is decreases. If the zone size are small then the more nodes communicate with the zone head which results more battery consumption and less time span. But we increase the zone size when the routing path is shorter because for large routing path increase in zone size may cause path break. So for better result we increase the zone size when the routing path is small and decrease the zone size when the routing path is larger. We increase or decrease the zone size by with the change in the radius of the zone. With the increase in the radius of the zone the zone size also increases and with the decrease in the radius of the zone the zone size decreases. The error rate are also low with increase in the zone size .

Flow Chart


start
Create network
Calculate Mobility
Mobility= node change/zone change
Compare mobility
Node with lowest mobility
is zone head of source
Source zonehead broadcast RREQ
0


0
Check if the RREQ receive by zone head
yes
No
discard
Check if same RREQ receive before
yes
No
discard
Check if it have route to destination
yes
no
Unicast route for destination back to originator
Create reverse route if sender of RREQ Then rebroadcast RREQ
Stop

In this paper we are taking the network size 1500*1500m, maximum transmission range are set to 150m and We varied the network size from 400, 500, 600 nodes .From Fig-7 and Fig-8, we conclude that for larger zone radius the error rate is less and for the small zone radius the error rate is high. The error decreases when we increase the zone size and the number of zones and when we are increasing the radius from 10 to 30 the error rate is decreases. We are also increasing the

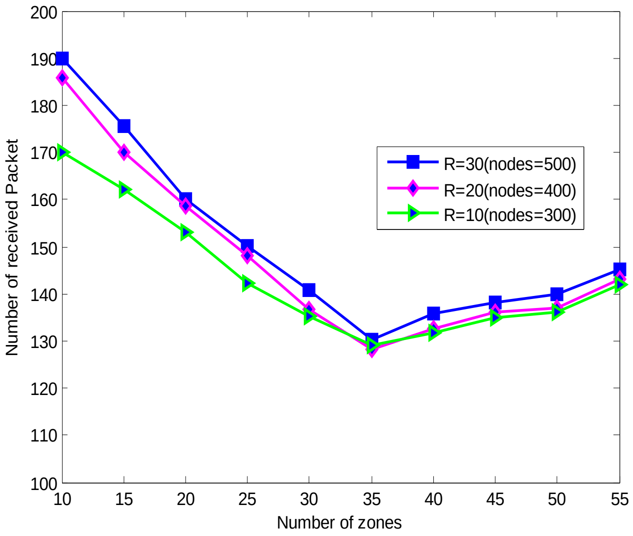


Fig.7 (Number of received packet)

number of nodes with the zone radius. When we increase the radius of the zones the number of received packet are also increases.

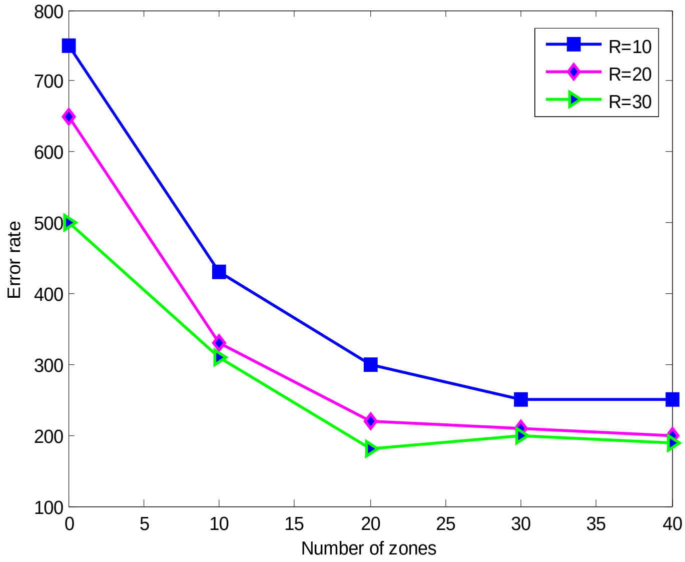


Fig.8 (Error rate)

We increase the zone size for small routing network so that it doesn’t result into path breakage. If the network size is larger than node will communicate less with the zone head. So it results into less wastage of energy. Means battery consumption also decreases.

VIII. CONCLUSION

In this paper when we are taking different radius i.e. when we are increasing the radius the error rate are decreasing. And with the increase in zone radius the number of received packet also increase. If we increase radius of a zone the zone size also increases. This result showing that our algorithm adapts well when the zone size increases.

REFRENCES

1.) Usama Ahmed and Faisal Bashir Hussain,”Energy Efficient Routing Protocol for Zone Based Mobile Sensor Networks” , Wireless Communications and Mobile Computing Conference(IEEE) , Pakistan, Pages 1081 - 1086, July 2011.

2.) Yudhvir Singh, Yogesh Chaba, Monika Jain and Prabha Rani,” Performance Evaluation of On-Demand Multicasting Routing Protocols in Mobile Adhoc Networks”, International Conference on Recent Trends in Information Telecommunication and computing, IEEE computer society,USA, Page(s): 298 – 301, March 2010

3.) Nidal Nasser, Anwar Al-Yatama and Kassem Saleh,” Zone-based routing protocol with mobility consideration for wireless sensor networks”, Telecommunication Systems, 8 March 2012,PP. 1-20,doi:10.1007/S.11235-011-9562-9

4.) Brijesh Patel and Sanjay Srivastava ,” Performance Analysis of Zone Routing Protocols in Mobile Ad Hoc Networks”, National Communication Conference, India, **Page(s):** 1 - 5 , Jan. 2010 IEEE

5.) Koyama, A., Honma, Y. ; Arai, J. and Barolli, L,” An enhanced zone-based routing protocol for mobile ad-hoc networks based on route reliability”, 20th International Conference on Advanced Information Networking and Applications,Japan ,Vol. 1, Pages 61 – 68, April 2006

6.) Sato, Y. , Koyama, A. and Barolli, L,“A Zone Based Routing Protocol for Ad Hoc Networks and Its Performance Improvement by Reduction of Control Packets.”, International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA),Japan , Page 17 – 24, Nov. 2010

7.) Wen Wei and Zhang Heng Yang,” Increasing Packet Delivery Ratio in GPSR Using Buffer Zone Based Greedy Forwarding Strategy”, Data Storage and Data Engineering (DSDE) International Conference ,China, page 178 – 182, Feb. 2010

8.) Wang, L and Olariu, S,” A two-zone hybrid routing protocol for mobile ad hoc networks “,Parallel and Distributed Systems, IEEE Transactions, vol-15 ,, Issue: 12, pages 1105 – 1116 ,Dec. 2004

9.) Amouris, K.N. and S. ; Miao Li,” A position-based multi-zone routing protocol for wide area mobile ad-hoc networks”, Vehicular Technology Conference, Eatontown, vol.2, Pages 1365 – 1369, 1999 IEEE

10.) Wendi Rabiner Heinzelman,” Energy-Efficient Communication Protocol for Wireless Micro sensor Networks”, System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference, MIT, Cambridge, MA, USA ,January 2000

11.) M. J. Handy, M. Haase and D. Timmermann,” Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection”, Mobile and Wireless Communications Network, 4th International Workshop, Rostock Univ., Germany **,** Page(s): 368 - 372 ,2002 IEEE

12.) Kamal Beydoun, Violeta Felea and Hervé Guyennet,” Wireless Sensor Network Infrastructure :Construction and Evaluation”, Fifth International Conference on Wireless and Mobile Communications, France, Page 279-284,Aug 2009

13.) Prince Samar, Marc R. Pearlman and Zygmunt J. Haas,” Independent Zone Routing: An Adaptive Hybrid Routing Framework for Ad Hoc Wireless Networks”, IEEE/ACM Transactions on networking, VOL. 12, NO. 4, Aug 2004

14.) Al-Sakib Khan Pathan , Hyung-Woo Lee and Choong Seon Hong,” Security in Wireless Sensor Networks: Issues and Challenges”, Advanced Communication Technology, ICACT 8th International Conference, Kyung Hee Univ., Seoul, Volume: **2,** Page(s): 6 pp. – 1048, Feb. 2006

15.) Kalpana Sharma and M K Ghose,” Wireless Sensor Networks: An Overview on its Security Threats”, IJCA Special Issue on Mobile Ad-hoc Networks ,MANETs, Sikkim, India, 2010

16.) V.Manjula1 and Dr.C.Chellappan ,”REPLICATION ATTACK MITIGATIONS FOR STATIC AND MOBILE WSN”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2,Pages: 122-133, 2011

17.) Pardeep Kumar and Hoon-Jae Lee,” Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, Sensors, vol 12, Page(s): 55-91, doi:10.3390/s120100055 ,2012