International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-2, Issue-3, May-2015

Good Neighbour Node Detection Technique in Manets Using QOS GNDA

Pallavi Patil
Department of Computer Engineering
Pillai's College of Engineering and Technology,
Mumbai University, India
Pallavimahesh02@gmail.com

ABSTRACT

MOBILE Ad hoc Networks (MANETs) are wireless networks which are characterized by dynamic topologies and have no fixed infrastructure. Each node in a MANET is a computer that may be required to act as both a host and a router and may be required to forward packets between nodes which cannot directly communicate with one another. Generally in ad hoc networks each and every node acts as a router and forwards packets to the destination. Due to mobility of nodes there is possibility of some nodes being bad neighbors. When a neighbor node turns out to be a bad neighbor, it could lead to loss of data packets, degradation in performance of node mobility, degradation of performance of routing protocol, difficulty in maintaining routes and degraded performance of the network. These potentially cause delay in transmitting the data and may result in congestion in the network. Good Neighborhood Node Detection Algorithms (GNDA) helps us find the best route for the destination. However, they are not able to minimize delay in case of route failure. The dynamically changing nature of nodes makes it difficult to maintain a consistent route. Nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In Adhoc networks, nodes typically cooperate with each other, by forwarding packets for nodes which are not in the communication range of the source node. Nodes may be affected by dynamically changing topology, limited bandwidth, hidden terminals, transmission errors and battery constraints. As such detection of a good neighbor node is a necessity. In order to achieve this in this paper a new routing protocol called Quality of Service Good Neighborhood Node Detection Algorithms (QOS-GNDA) is proposed. This protocol finds a good neighbor node using parameters like Transmission range, Power of node, Signal strength, Capacity of node for packet forwarding and Relative position of node.

Keywords

MANETs, Adhoc routing, AODV, Signal strength, Flow capacity, Relative position.

1. INTRODUCTION

MANET is a collection of mobile devices which form a communication network with no pre-existing wiring or infrastructure. They allow the applications running on these wireless devices to share data of different types and characteristics. There are many applications of MANETs, each with different characteristics of network size (geographic range and number of nodes), node mobility, and rate of topological change, communication requirements, and data characteristics. Such applications are conferences, classroom, campus, military, and disaster recovery. Each node is directly connected to all nodes within its own effective transmission range. Nodes in the network are allowed to move in and out of range of each other. Communication between nodes that are not within range of each other is accomplished by establishing and using multi-hop routes that involve other nodes which act as routers. New nodes can join the network at any time and existing nodes can leave the network as well. The performance of network increases rapidly by considering good nodes into the account. Categorizations of good and bad nodes depend upon different parameter [1] used to find nodes. Moreover, how fast each node can receive the complete information. An Ad Hoc Network (MANET) is a wireless network consisting of mobile nodes, which can communicate with each other without any infrastructure support. In these networks, nodes typically cooperate with each other, by forwarding packets for nodes which are not in the communication range of the source node. Typically, routing protocols are classified according to the route discovery philosophy, into either reactive or proactive. Reactive protocols are on-demand. Route-discovery mechanisms are initiated only when a packet is available for transmission, and no route is available. On the other hand, proactive protocols are table-driven. Routes are precomputed and stored in a table, so that route will be available whenever a packet is available for transmission.

This paper is organized as follows. Section 2 describes the impact of bad neighbor nodes. In section 3, some of the good neighbor detection methods are reviewed. Section 4 presents proposed methodology for good neighbor node detection based on AODV using GNDA. Section 5 shows route establishment in AODV for proposed approach. Section 6 and 7 depicts calculation of current bandwidth and simulation results respectively and section 8 depicts consultation.

2. IMPACT OF BAD NEIGHBOUR NODES

The nodes in MANET have limited battery power and bandwidth, and each node needs the help of others to get its packets forwarded. The different protocols in MANETs assume that all the nodes are cooperative and whenever a node receives a request to relay traffic, it always does so truthfully. However the experience has shown that as the time passes there is a tendency in the nodes in an ad hoc network to become selfish. The selfish nodes are not malicious but are reluctant to spend their resources such as CPU time, memory and battery power for others. The problem is especially critical when with the passage of time the

nodes have little residual power and want to conserve it for their own purpose. Thus in MANET environment there is a strong motivation for a node to become selfish. The working of Adhoc network is based on packet forwarding using neighbor nodes, the source or the sender node must rely on intermediate nodes. The dynamic nature of network topology in Adhoc network leads the problem for nodes like, limited bandwidth, hidden terminals, transmission errors, and battery constraints, selfish nodes. The nodes affected by this gives poor performance ultimately the network throughput and network protocol affected and the performance of the network is decreases.

3. EXISTEM SYSTEMS

A Mobile Ad-hoc Network (MANET) is a temporary wireless network composed of mobile nodes, in which an infrastructure is absent. If two mobile nodes are within each other's transmission range, they can communicate with each other directly; otherwise, the nodes in between have to forward the packets for them. In such a case, every mobile node has to function as a router to forward the packets for others. Thus, routing is a basic operation for the MANET. Because traditional routing protocols cannot be directly applied in the MANET, a lot of routing protocols for unicast, multicast, and broadcast transmission have been proposed since the advent of the MANET.

Perkins Charles E. and E. M. Royer [1] Proposed an algorithm fro optimizing the routing issues by using AODV [1] while Umang Singh et.al, [2] suggest a GNDA algorithm. This protocol finds good neighbor node using parameters like Transmission range, Power of node, Signal strength, Capacity of node for packet forwarding and Relative position of node. But this protocol fails to reduce the congestion because packet forwarding is considered only for high bandwidth data. In reality, low bandwidth packets also exist which may lead the network towards congestion. Also, as the network size increases, cost also increases. Reddy et.al. [3] Proposed reliable AODV routing protocol which enhances network performance by selecting stable nodes (i.e., only good neighbor nodes) for network formation. All information related to reliable nodes are stored in routing table which improves performance of routing protocol in terms of good communication and stable route. Quorum-Based Neighbor Discovery is proposed by Sina et.al.,[4]. This approach is a deterministic handshake-based algorithm using quorum systems. A quorum is the minimum number of nodes to be present at an assembly. Quorum-based neighbor discovery allocates a quorum system for all elements of universal channel set. During each time interval one or two channels are selected for sending or receiving the advertised message. Transmission is done through available channels, thus skipping the unavailable channels. The size of quorum system used on the whole network is known as the upper band of discovery length. Biradar et.al.,[5] have effectively demonstrated the process of neighbor node selection in MANETs using reliability pair. The reliability pair formation and computation of reliability pair factor for every established reliability pair is triggered by jointly handling the parameters such as remaining battery power of nodes, mobility of nodes, distance between the nodes and differential received signal level of neighboring nodes. The reliability pair is formed such that link stability is maximized while link cost is minimized. For each node, whenever node changes its location, reliability factor is calculated. This will result into increased network overhead. Wang Gang et.al.,[6] uses phoenix network coordinate system which maps each node as incoming vector and dimensional outgoing vector. Network Coordinate (NC) which provides efficient distance prediction with scalable measurements brings benefits to various network applications. Phoenix Network Coordinate system is a recently proposed dot product based NC system with high prediction accuracy and better robustness. This system has considered only distance while ignoring other parameters like signal strength, flow capacity, battery power etc. Saleem Bhatti et.al.,[7] proposed Dynamic Timer Based on Multi-Increase Additive Decrease algorithm(DT_MAID) in which adaptive neighbor detection is done by minimizing the route discovery side effects. Pedro M. et.al.,[8] proposed a Geographic Multicast Routing(GMR) which is a cost based neighbour selection policy at each round trip. But this solution is applicable only for small number of destinations.

4. PROPOSED MEHODOLOGY

In the proposed system, we are finding good neighbor node at the time of link establishment only. Various parameters like Transmission range, Power of node, Signal strength, Capacity of node for low as well as high bandwidth packets forwarding and Relative position of node are utilized for finding good neighbor node. These parameters help in minimizing end to end delay and packet dropping ratio. It also removes congestion in network and improves performance of the routing protocol and hence performance of the network. In existing approach Umang Singh et.al., [1] decide a particular node to be good or bad based on Performance parameters such as Transmission range, Power

TYPE U_int8_t	RREP NODE CURRENT BANDWIDTH CAPACITY, CBC u_int16_t	HOP COUNT u_int8_t
DESTINATION IP ADDRESS nsaddr_t		
DESTINATION SEQUENCE NUMBER u_int32_t		
LIFE TIME double		
rp_timestamp double		

Figure.1: Data structure. (QOS_GNDA RREQ packet format)

of node, Signal strength, Capacity of node for high bandwidth packets Forwarding and Relative position of node. They calculate the capacity of current node for high bandwidth packets only. In actual situation many times there are nodes that are satisfying minimum bandwidth for packets and that may be causing delay. Thus we propose a new approach called QOS-GNDA where we are calculating "minimum satisfying bandwidth" of current, previous and next nodes and their delay to classify good or bad neighbor node. When a node wants to send a RREQ in our approach, we add a minimum bandwidth parameter to QOS. So from source to destination we have available bandwidth which is greater than or equal to minimum required bandwidth (BP). We can calculate current bandwidth capacity (CBC) by calculating session BP for particular session flow and taking sum of all these the data packet sent and received divided by total no of packets forwarded. If any node is not satisfying the minimum bandwidth

condition that node it broadcasts the condition to find out a node width required bandwidth. To include the user defined quality of service parameters (minimum bandwidth (BP) and maximum end to end delay (D)) the AODV RREQ packet is modified. The RESERVED field within the normal AODV RREQ packet is used

.TYPE nt8_t	RREQ QoS BANDWIDTH u_int16_t	HOP COUNT u_int8_t
RREQ BROADCAST ID u_int32_t		
DESTINATION IP ADDRESS nsaddr_t		
DESTINATION SEQUENCE NUMBER u_int32_t		
SOURCE IP ADDRESS nsaddr_t		
SOURCE SEQUENCE NUMBER u_int32_t		
rq_timestamp double		

Figure 2: Data structure. (QOS_GNDA RREP packet format)

to carry the information during the route establishing process. This extended version of AODV RREQ will be referred as QOS_GNDA RREQ (Figure.1). The RESERVED field has total length of 16 bits. The maximum value that can be passed in a QOS_GNDA RREQ packet is 65536. The RREP also has a 16-bit RESERVED field that is used to include Current Bandwidth Capacity (CBC) values for the intermediate nodes along the valid path.

5. ROUTE ESTABLISHEMENT

Here we describe how the QOS_GNDA system establishes the route consider a scenario in which a node , S wishes to communicate with another node, D. if node S has no valid path(s) to D in its routing table, then a route request is initiated. Node S broadcasts the extended AODV RREQ packet to its neighbors. Upon receiving these RREQ packets, the intermediate nodes (n1, n2,…,nj) compare the RREQ_QOS_BANDWITH field value, within the RREQ packet. Say x kbps with their Current Bandwidth Capacity CBC kbps. If these intermediate nodes are already engaged in other traffic sessions then their total available bandwidth capacity will vary. The nodes which cannot accommodate the user-specified minimum bandwidth, say x kbps, the "busy" nodes will discard the QOS-GNDA RREQ and do not unicast further. The nodes which satisfy the bandwidth requirement, broadcast the QOS-GNDA RREQ to their neighbors. A reverse route entry is added in the routing table of the QOS valid node that unicasts the QOS-GNDA RREQ packet. This process continues until a node receives the QOS-GNDA RREQ and has a fresh route to the destination node D. The intermediate nodes (n1, n2… nj) are QOS valid if they satisfied the minimum bandwidth condition.

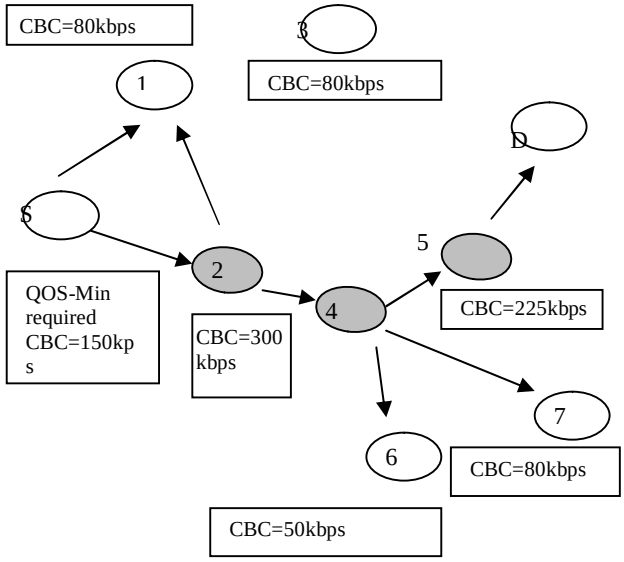

Figure 3: QOS-GNDA route establishment

Let's take a scenario: Figure 3 shows an example of how exactly our approach works. Suppose "S" the source node and this node wants to communicate, the node send a data packet or broadcasts a RREQ packet in which the minimum bandwidth is of 150kbps.The broadcasted data packets reach the nodes 1and 2 because these nodes are in communication range of node"S". Node 1 is not satisfying our minimum bandwidth condition because its CBC is 80kbps; so this node is discarded from communication. The Other node which receives the broadcast message is node 2 this node is satisfying the minimum bandwidth condition because its CBC is300kbps.Node 2 update its routing table with the details of the incoming packets. Node 2 again broadcasts message i.e. RREQ. This time nodes 1, 4 and 6 receive this RREQ packet. As nodes 1and 6 are not satisfying the minimum bandwidth condition, they will be discarded. However as node 4 is satisfying the minimum bandwidth condition, node 4 updates its routing table with the details of the incoming packets. Again node 4 broadcasts RREQ packet, node 5 and node 3 receives the broadcasts message. Both nodes satisfies the minimum bandwidth condition but using Euclidean distance calculation formula we find that node 5 is much closer than node 3 so we select node 5 and again maid entry in routing table of node 5.Again node 5 broadcasts RREQ packet and it will received by node D which is the required destination. If none of the closer nodes of source node will satisfy the minimum bandwidth condition the packet will be come back to source node.

6.CURRENT BANDWIDTH CALCULATION

For calculating the dynamic bandwidth of node we used the approach [8] here given bellow. The proposed method to monitor and update a nodes traffic status in based upon session flows. This will include keeping track of the various flow statistics over a period of time. The instance at which a traffic flow session is started at any given node, the start-time for every unique flow session is stored. As the data packets arrive and are processed by the nodes, other information necessary for the CBC calculation is

extracted from the IP data packets such as: packet size, flow id, source node, destination node, etc.For each individual session flowing through a node, the total number of bytes (calculated from the data packet size for each different flow) sent/forwarded by the node is monitored. The start-time for each flow is used to work out the interval between packets which are part of the same flow. The CBC is calculated and updated constantly and is a new addition to the nodes routing table. This approach is used in GNDA while calculating judge flow capacity. Here in GNDA author judge only in high packet capacity but in actual situation many times there are node who are satisfying minimum bandwidth or May required specific bandwidth.

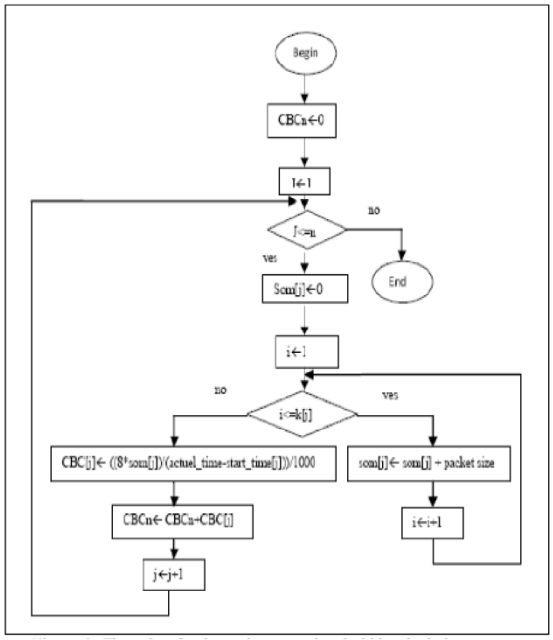

Figure 4.flow chart for dynamic CBC calculation

Where:

j: flow number

k[j]: byte max number of flow j

Som[j] : byte sum of all flow j packets

i: flow packet number

CBC[j]: current bandwidth capacity of flow j

CBCn: sum of current bandwidth capacity of all flows in Kbps.

Following algorithm shows the low(required bandwidth) packet forwarding capacity.

Algorithm

STEP 1: Initialize Total number of nodes in the network STEP 2: Initialize TTr of the network

STEP 3: Broadcast Hello message

STEP 3.1: Send MOCK packet

STEP 4: Receive Hello message

STEP 4.1: Receive MOCK packet

STEP 5: Calculate time, of reaching Hello message

STEP 6: Compare NTr and TTr

STEP 6.1: if NTr > TTr then Decrease the NTr and go to step: 6

STEP 6.2: else go to step 7

STEP 7: Calculate signal strength

STEP 7.1: I f signal strength > = Threshold then go to step: 8

STEP 7.2: else it is a weak signal so go to step: 4

STEP 8: Calculate flow capacity

STEP 8.1: If flow capacity is equal to CBC then store node address (Good node)

STEP 8.2: else Bad node

STEP 9: Send RREQ through good node

STEP 10: When RREQ reach the Destination, it stores the route.

STEP 11: Send Data if path available

STEP 12: Stop

Where NTr -is node transmission range and TTr –is total network transmission range.

7. SIMULATION RESULTS

Performance studies can be done under 6-10 numbers of node. We added the required bandwidth constraints in the QOSGNDA which will help to reduce the packet dropping ratio.

Table1: Simulation Parameters

Simulation Parameters	**Values**
Nodes	6-10
Simulation time	100sec
MAC Layer	IEEE 802.11
Packet Size	512
Pause Time	0-100sec
Initial energy	50
Transmission Range	250m
CS Range	550m
Transmission threshold power	4.4613 e-10

Figure 5 depicts that the packet delivery ratio is increase as compare to exiting system. The overall packet delivery ratio is increased. Figure 6 depicts average end to end delay ratio is increased when we are not sending the Mock packet. Figure 7 depicts that when we are sending the mock packet the end to end delay is increased because the overhead of

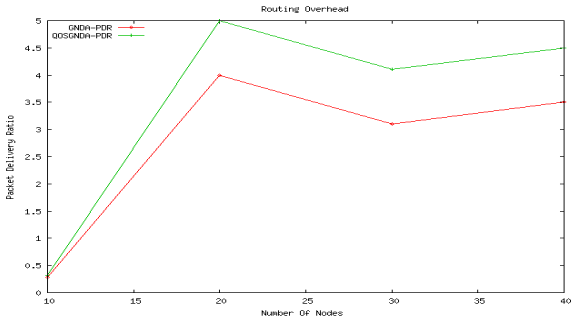

Figure 5: Packet delivery ratio between GNDA and QOSGNDA.

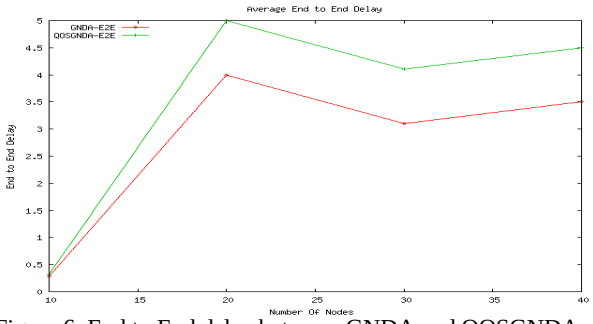

Figure 6: End to End delay between GNDA and QOSGNDA

.

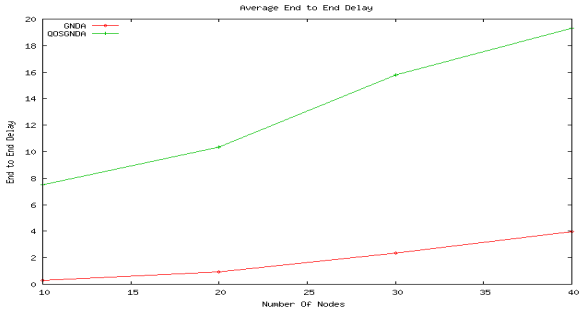

Figure 7: End to End delay between GNDA and QOSGNDA (with MOCK packet)

Hello and mock packets. We are sending this mock packet for checking our required bandwidth condition. Figure 8 shows that when we are not sending the mock packet we are getting the result as increased end to end delays. Figure 9 depicts that When we are sending the mock packet for finding required bandwidth the packet dropping is reduced as compare to the existing approach i.e. GNDA.

Packet delivery ratio: Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as: PDR=S2÷S1, Where S1 is number of packets delivered by source and S2 is number of packets received by destination [20]. From above figure we conclude that using QOSGNDA the packet delivery ratio is much better than the GNDA. When we send the MOCK packet the PDR is 0.99671 and in GNDA it is 3.9995205.

End-to-End Delay:

The average time it takes a data packet to reach the destination.

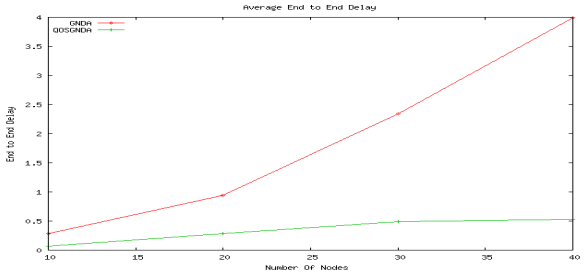

Figure 8: End to End delay between GNDA and QOSGNDA (without MOCK packet)

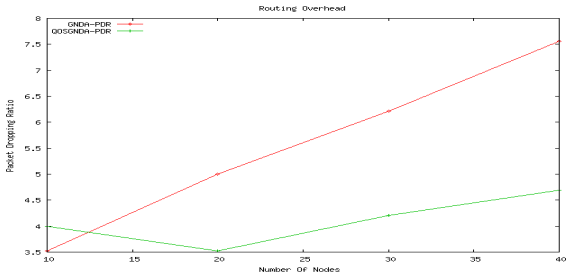

Figure 9: Packet dropping ratio of GNDA and QOSGNDA (with MOCK packet)

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as: Avg. EED=S/N

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination node [30].From above figures we conclude that using QOSGNDA the end to end delay is much better than the GNDA. When we use the MOCK packet in QOSGNDA the end to end delay is 7.50 whereas in GNDA it is 0.07.Altimately when we are sending the MOCK packet it show the end to end delay is increased.

8. SUMMARY

This protocol improves the performance of GNDA in terms of packet dropping ratio, end to end delay in network. This approach can be applicable for real time scenario. Although the promising results are shown, still there is much room for improvement. Limitation of this approach and proposes possible extensions of the research to improve the performance of this system and have this system more applicable to general application. For finding good node we are applying the proposed QOS-GNDA approach it find good node but it can't recognize the selfish or the hidden malicious node for this reason the proposed approach need to expand in terms of security purpose. This approach may be extended in terms of to defend from impersonation attack.

REFERENCES

[1] Perkins Charles E., and Elizabeth M. Royer. "Ad-hoc on-demandDistance Vector Routing." Second IEEE Workshop on Mobile Computing Systems and Applications,Pp. 90-100. IEEE1999.

[2] Singh Umang, B. V. R. Reddy, and M. N. Hoda . "GNDA: Detecting Good Neighbor Nodes in Adhoc Routing Protocol." Second International Conference on Emerging Applications of Information Technology (EAIT), Pp. 235-238. IEEE 2011.

[3] T. Rajamohan Reddy, N. Sobharani. "Selective On-demand Protocol for Finding Reliable Nodes to form Stable Paths in ADHOC Networks."International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Pp-21-24, vol-1, no. 5, 2012

[4] Khatibi Sina, and Ruhollah Rohani. "Quorum-based Neighbor Discovery in Self-organized Cognitive MANET." 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Pp. 2239-2243. IEEE 2010.

[5] Biradar Rajashekhar and Sunilkumar Manvi. "Channel Condition and Mobility Based Choice of Neighbor Node for Routing in MANET." International Conference on Advances in Computer Engineering (ACE), Pp. 74-78, IEEE, 2010.

[6] Wang Gang, Shining Wu, Guodong Wang, Beixing Deng, and Xing Li. "Experimental Study on Neighbor Selection Policy for Phoenix Network Coordinate System." International Conference on ultra modern telecommunication, pp. 1-5. IEEE, 2009.

[7] Huang Yangcheng, Saleem Bhatti, and Soren-Aksel Sorensen. "Adaptive Neighbor Detection for Mobile Ad Hoc Networks." UCL department of Computer science,RN7:17.

[8] Sanchez Juan A., Pedro M. Ruiz, and Ivan Stojmenovic. "GMR: Geographic Multicast Routing for Wireless Sensor Networks." 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, vol. 1, Pp. 20-29. IEEE 2006.

[9] Moussa A. C., F. M. Kamel, D. Noureddine, and K. Maamar. "Integration of Dynamic Current Bandwidth Capacity Calculation for Existing AODV." International Conference on Information Technology and e-Services (ICITeS), Pp. 1-7, IEEE 2012.

[10] Narayanan Uma, and Arun Soman. "Bandwidth Efficient GNDA." IOSR Journal of Engineering (IOSRJEN) ,Vol. 3, Issue 6, Pp40-43 , 2013