IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 3, Ver. III (May - Jun. 2014), PP 30-37
www.iosrjournals.org

Avoiding Selfishness by Effective Routing Using Trust Based Mechanism

[1]Devika Adithya Das, [2]T K Parani
[1]Student, ME Communication Systems Engineering, Anna University DSCE Coimbatore, INDIA
[2]Assistant Professor, Dept of Electronics and Communication Engineering DSCE Coimbatore, INDIA

Abstract: *Communication in wireless sensor networks is through nodes. High quality network needs efficient communication between nodes. Here Order-Optimal Neighbour Discovery Using Feedback protocol is proposed for neighbour discovery .This protocol exploits the feedback from the receiving nodes. After certain transmissions some nodes loose energy and become selfish. The Trust Based Routing Algorithm routes the packets through optimal energy nodes and thus leads to a more efficient high quality network. The trust based routing algorithm is compared with the conventional routing protocols on the basis of mainly five parameters i.e. trust level, throughput , delay, packet delivery ratio and overhead.*

I. Introduction

1.1 Wireless Networks

A wireless network is a computer network that uses a wireless network connection. It uses radio waves just like cell phones, televisions etc .The most important advantage of this network is that it allows the costly procedure of introducing cables to diminish.[10].What differentiates wireless communication from wired communication is the nature of the communication channel.[10] Motion of the transmitter and the receiver, the environment, multipath propagation, and interference render the channel model more complex.

1.2 Neighbour Discovery

Communication in wireless network is through the nodes. Data's are transmitted in the form of packets from one node to another node. Usually upon deployment a node does not have knowledge about its specific neighbours. A high quality network means there must be an efficient packet transmission between nodes without any delay. In order to make a wireless network an efficient network, the neighbour nodes must be discovered.[8] Thus, neighbour discovery is the first important step in wireless networks.[7]

1.3 Selfishness

In a network, all nodes must have specific energy. This energy enables them to transfer or receive packet. All nodes in a network might not have enough energy to do this. Such nodes are known as selfish nodes.[8].In a network there will be two types of selfish nodes:-

1) Partially Selfish Nodes
2) Fully Selfish Nodes

Partially selfish nodes have energy to receive the data packet. But does not have enough energy to transfer the received packet. Fully selfish node means, it does not have enough energy to either receive or transfer a data packet. Non selfish nodes allocate their memory space completely for the purpose of other nodes. Selfish nodes do not allocate their memory space for the purpose of other nodes. Partially selfish nodes allocate minimum portion of their memory space for the purpose of other nodes and remaining for the benefit of own node.[8]

Data transmission is the main task in a wireless network, and this is done through nodes. In a wireless network there will be a limited transmission range for nodes. Therefore it depends on other intermediate nodes to transfer the packets to their intended destination. These intermediate nodes act as relays for the packet. This communication paradigram is known as multi hop where a node can act as a source, a destination and a relay. Data transmission occurs from source node to destination node through these multi-hop routing techniques. But the presence of the partially and fully selfish nodes affect the network transmission as these nodes disregard the incoming packets in the network .The performance of a wireless network depends on the cooperation of all nodes in the network. In this paper a routing algorithm is proposed through which data transmission from source to destination occurs through non-selfish nodes. Here, the numbers of neighbour nodes are discovered using order optimal algorithm for neighbour discovery. Using the trust based algorithm, the energy level of each node is being calculated and maintained in a table format. The routing is done from source to destination based on priority which is depending on energy level of the specific node. Thus high priority routes are selected by the trust based routing algorithm. The trust based routing algorithm is compared with the conventional routing protocols on the basis of mainly five parameters i.e. trust level, throughput , delay, packet delivery ratio and overhead.

II. Order-Optimal Neighbor Discovery Without Collision Detection

Order-optimal neighbour Discovery is achieved, when nodes cannot detect collisions. Algorithm 3 presents a neighbour discovery algorithm that achieves this goal. Node hears its ID during a round; it "drops out" of neighbour discovery at the end of the round. The neighbour discovery is done even when the nodes cannot detect collisions. Instead of providing a single bit of feedback, each node now includes in its discovery messages the ID of the most recently discovered neighbour in addition to its own ID. If a receiving node hears its ID during a round, it drops out of "neighbour discovery" at the end of the round.[8]

This algorithm compared to the other three algorithms discovers the neighbours without collision, therefore the congestion in the network arriving due to collisions can be reduced. These three algorithms are used for neighbour discovery. These algorithms are compared based on two aspects:-

1. Number of collisions
2. Time required for finding the neighbors

Number of collisions: Number of collisions are an important factor in determining neighbours .Even though collision helps in neighbour discovery, it causes congestion in the network. As a result the three algorithms i.e. Order-Optimal Neighbour Discovery Without Collision Detection, Asynchronous Collision detection based neighbour .The neighbour discovery is done even when the nodes cannot detect collisions.[8]

Instead of providing a single bit of feedback, each node now includes in its discovery messages the ID of the most recently discovered neighbour in addition to its own ID. If a receiving node hears its ID during a round, it drops out of "neighbour discovery" at the end of the round.[8]

Time required for finding the neighbours: Time required for finding the neighbour nodes are another important factor in discovering neighbours. The algorithm which takes the least time in discovering the neighbours is the most efficient algorithm among three.

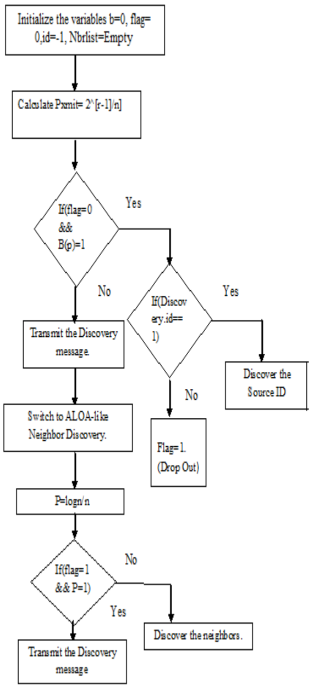

Initialize the variables b=0, flag= 0,id=-1, Nbrlist=Empty
Calculate Pxmit= 2^[r-1]/n]
If(flag=0 && B(p)=1
Yes
No
If(Discovery.id== 1)
Yes
Transmit the Discovery message.
Discover the Source ID
No
Switch to ALOA-like Neighbor Discovery.
Flag=1. (Drop Out)
P=logn/n
If(flag=1 && P=1)
No
Yes
Discover the neighbors.
Transmit the Discovery message

Fig 1: Order-Optimal Neighbour Discovery without Collision Detection

III. Trust Based Routing Algorithm

In a wireless sensor network, one of the important challenge is how to route the packets efficiently from source to destination. Many paths through nodes will be available from source to destination and the packets can be forwarded through many routes. Thus in a mobile network each node has to rely on other nodes. As the average number of hops between source to destination increases the energy of the nodes will get affected. This will result in creation of selfish nodes in the network. Selfish nodes are defined as the nodes which do not forward other packets thus maximizing their benefit in expense of all others. They always behave rationally.

Trust is viewed as nodes ability in providing the required service of the wireless networks. Establishing trust in a network has following benefits:-

1. Trust solves the problem of providing corresponding access control based on judging the quality of SNs and their services.
2. Trust solves the problem of providing reliable
routing paths that do not contain any malicious selfish, or faulty nodes.
3. Trust makes the traditional security services more robust and reliable by ensuring that all the communicating nodes are trusted during authentication.

These routes will contain selfish nodes which will ultimately degrade the network quality by drooping the packets or either not forwarding the packets. The challenge is to discover the optimal path between the source and the destination. It is very important to communicate with a trust worthy neighbour since communicating with selfish nodes results in degradation of the quality of the networks.

In the trust based routing algorithm the energy assigned to each node in the network is maintained by a table format, which contains mainly IP address, energy and priority of the nodes. The priority is based on the energy level of each node. This algorithm helps to select the proper route between the nodes from source to destination identifying the fully and partially selfish nodes. The fully and partially selfish nodes are being identified by maintaining a threshold energy level. Thus the role of the routing algorithm is not only finding a path from source to destination but finding an optimal one that satisfies the needed performance requirements from a set of optional paths.

Traditional trust management schemes is not suitable because small sensor nodes have limited bandwidth and have constrains about power and memory of the node. Finally the conventional routing algorithm is being compared with the trust based routing algorithm based on three parameters i.e. trust, delay and throughput.

Trust based routing algorithm is modified DSDV i.e. Destination sequence distance vector routing. It is a table driven scheme foe ad hoc mobile networks based on Bellman-Ford algorithm. In a wireless network when the topology changes, routing protocols between the nodes must be updated. Usually we choose shortest path between the source and the destination. But this includes mainly high message complexity. DSDV gives the best route from source to destination. Here a table s maintained which lists all available destinations, the next hop to each destination and sequence number generated by the destination tool.

IV. Network Model

The network considered here has twenty six nodes, the network area dimension is 1500 x 1500.Two way ground propagation is used as propagation model. The routing mechanism used here is trust based i.e. modified DSDV.

V. Related Work

The most conventional routing protocol is AODV also defined as the Ad Hoc on demand distance vector. It has the ability to defend the external attack and suggest secure routing in the network. Still they suffer from several disadvantages.

The next routing algorithm defined was URSA which is Ubiquitous and Robust Access Control proposed by Luo. Concurrently another routing protocol was proposed by Sanzgiri which defend the network from identified attacks. This is ARAN i.e. authenticated routing for ad hoc networks.

Papadimitratons and Hass requires security between nodes which is done by doing queries to the destination nodes and thus replaying the attacks.

On demand for routing protocol for Ad Hoc, here route discovery is using fault evidence .This protocol avoids the malicious links. Trust based algorithm to find the selfish nodes was proposed in different methods. Here when the packets are transferred through the nodes in the form of packets, each node eaves drops the packet weather it reaches the specific destination and formulates the trust value based on the reputation scheme. Here the trust mechanism is based on watchdog mechanism. Here the main disadvantage is trust evaluation based on nodes QOS property.

The next trust mechanism was developed to combine one or more trust component. It allows trust components to be added or deleted. Here there are mainly two types of trust level which is introduced i.e. data trust and communication trust. It is based on beta reputation methodology.

Another trust mechanism was introduced where the trust calculation is done by using routing, sensing and aggregation. These are the respective time stamped value.

The trust base mechanism based on beta repudiation methodology to improve the network lifetime and aggregated data. It uses the symmetric secret keys to assign keys to sensor nodes bases on their locations. It is similar to watchdog mechanism and reputation table consists of sensing, actuating, forward based reputation values.

An energy efficient trust based algorithm is proposed where concentration is given on aggregation and energy. The necessity to find the best path in a sensor node is the most important one. To find out the best path the two main aspects considered here are the link availability and the residual energy of the nodes. The main disadvantage is the delay caused by the congestion in the network.

A trust management model was also predicted previously defining the roles and the capabilities. This allows the information flow and flexibility in trust management process. Here mainly two approaches are taken into consideration i.e. the certificate based approach and the behavioural based approach.

Based on entropy models also trust based algorithms are proposed to detect the selfish or malicious nodes. This is the main framework to measure trust and thus defending it against attacks. It gives idea about the trust matrices, mathematical properties of trust and its respective dynamic properties. The main advantage of this system is that it improves the routing techniques and throughput of the network.

Another method is by using novel entropy model and evaluation of methods to find the trust. This is to find the trustworthiness between the nodes. Thus trust is established between nodes using graph describing the directed trust values.

VI. Evaluation And Result

6.1 Order-Optimal Neighbour Discovery without Collision Detection

The graph given above in fig 6 represents order-optimal neighbour discovery without collision detection. When the number of nodes discovered is 1000,the collision amount is 45000,but as the number of neighbours discovered goes on increasing example when it reaches 5000 ,the collision number will get reduced drastically. Thus giving zero probability for the network congestion.

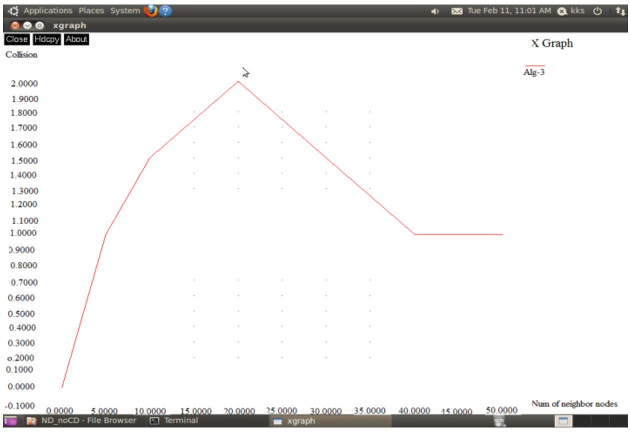


Fig 2: Order-Optimal Neighbour Discovery without Collision Detection

6.2 Trust

The concept of trust also has been attractive to communication and network protocol designers where trust relationships among participating nodes are critical in building cooperative and collaborative environments

6.2 Throughput

Throughput is defined as the average rate of successful message delivery over a communication channel. In WSN the successful delivery of packets is done from the source node to destination node is known as throughput.

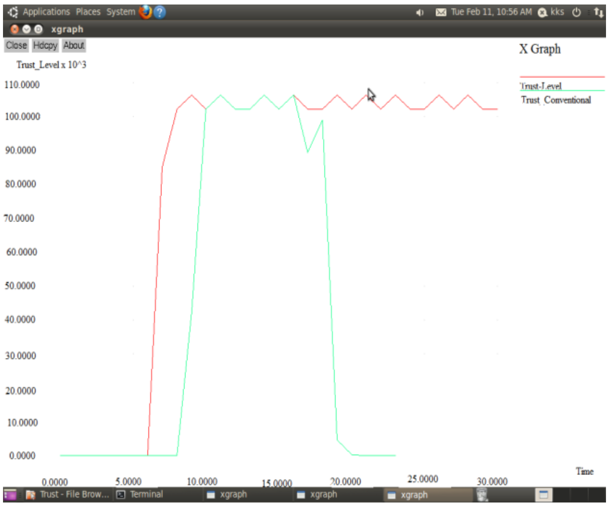


Fig 3: Trust Level

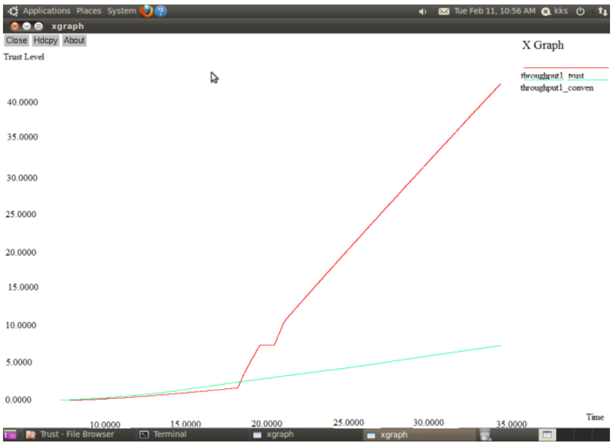


Fig 4: Throughput comparison

6.3 Overhead

A measure of the additional workload incurred in a parallel algorithm due to communication between the nodes of the parallel system. Data bits added to user-transmitted data, for carrying routing information and error correcting and operational instructions.[13]

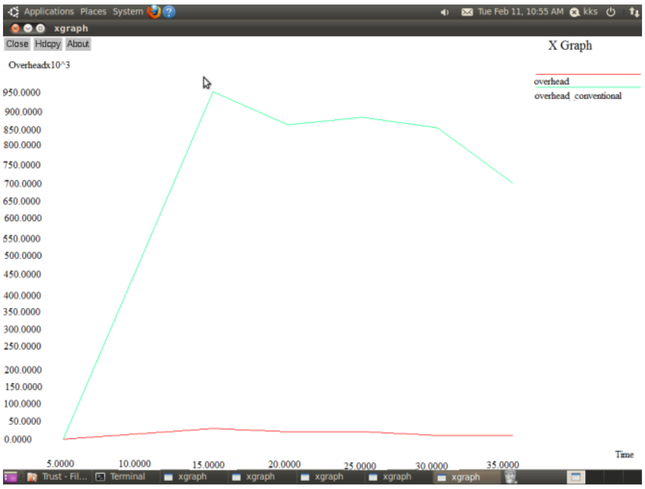


Fig 5: Overhead Comparison

6.4 Delay

The average time taken by a data packet to arrive from source to destination. It includes the delay caused by route discovery process and the queue in data packet transmission.

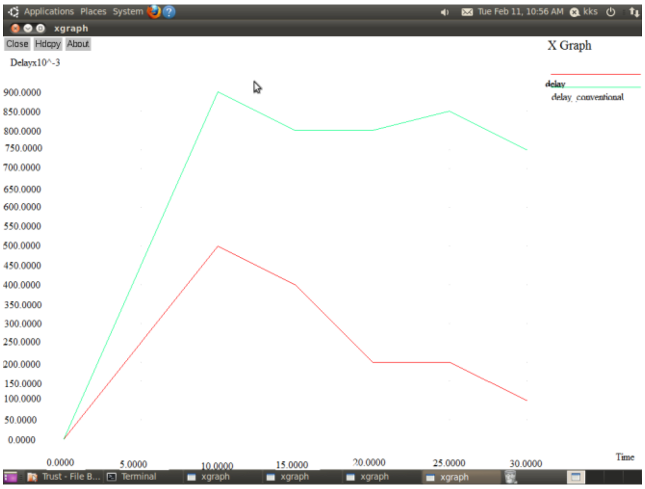


Fig 6: Delay Comparison

6.5 Packet Delivery Ratio

It is defined as the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been send out by the sender.[12]

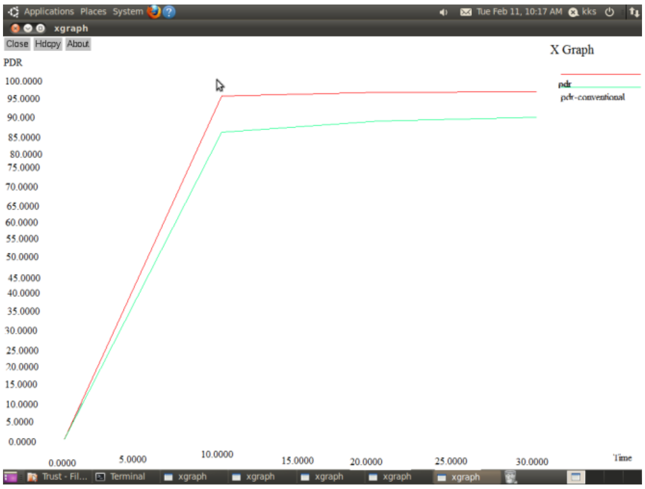
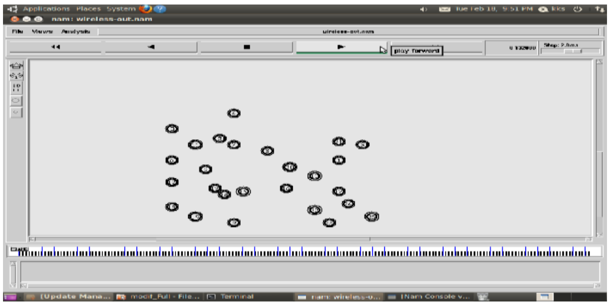


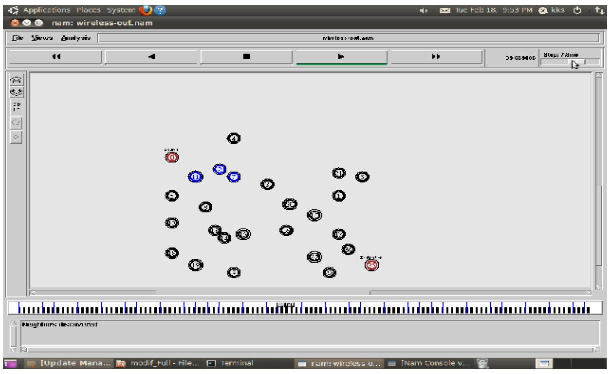
Fig 7: Packet Delivery Ratio Comparison

6.4.NAM window outputs

6.4.1 Neighbour Discovery

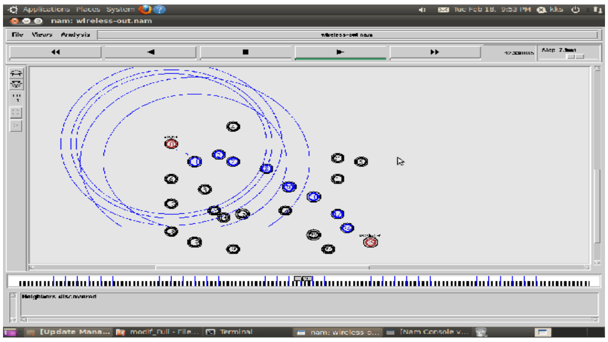


6.4.2:Pathfinding


nam: wireless-out.nam
File Views Analysis
wireless-out.nam
[Update Mana... modif_Full - File... Terminal nam: wireless-o... [Nam Console v...

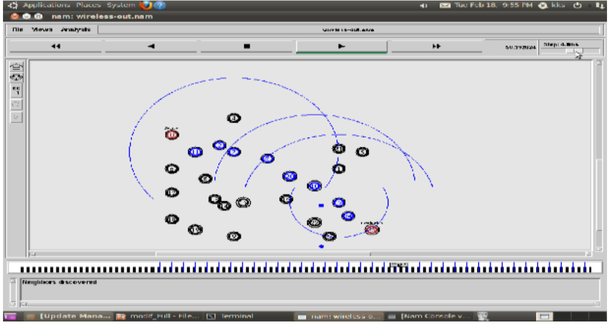
Neighbors discovered

6.4.3: Path found out transmission started


nam: wireless-out.nam
File Views Analysis
wireless-out.nam
[Update Mana... modif_Full - File... Terminal nam: wireless-o... [Nam Console v...

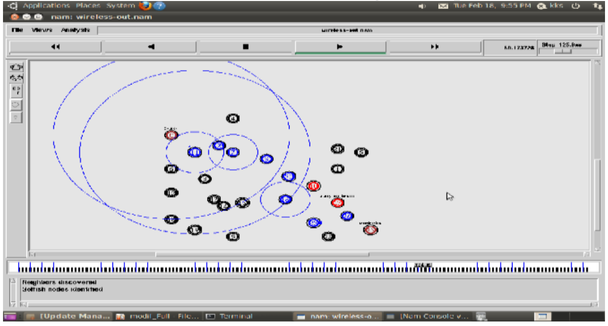
Neighbors discovered

6.4.4Dropping of packets happen in between


nam: wireless-out.nam
File Views Analysis
wireless-out.nam
[Update Mana... modif_Full - File... Terminal nam: wireless-o... [Nam Console v...

Neighbors discovered

6.4.5 Selfish nodes discovered transmission done through new path


nam: wireless-out.nam
File Views Analysis
wireless-out.nam
[Update Mana... modif_Full - File... Terminal nam: wireless-o... [Nam Console v...

Neighbors discovered
Selfish nodes identified

VII. Conclusion

Neighbour discovery is indispensable first step in wireless networks. Here the presented efficient neighbour discovery algorithms for wireless networks are being compared. These neighbour discovery algorithms do not require estimates of node density and allow asynchronous operation. Order-Optimal Neighbour Discovery Without Collision Detection takes the least amount of time and takes the least number of collisions to discover the neighbour nodes, it is considered to be the best algorithm for the process of neighbour discovery. Simultaneously using the trust based routing algorithms an appropriate route is being selected form source to destination identifying the fully and partially selfish nodes thereby enhancing the network quality.

References

[1] AbdulSattar, Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun,VijayVaradharajan2009 A Trust Management ArchitectureformmmmmmmHierarchicalWirelessSensorNetworks

[2] Sagar D. Padiya, Rakesh Pandit, Sachin Patel 2003 A System for MANET to Detect Selfish NodesUsing NS2

[3**]** Guoyou He 2004 Destination Sequence Distance Vector(dsdv) protocol,

[4] Hassan Jameel, Brian J. d'Auriol, Member, IEEE Computer Society,Heejo Lee, Member, IEEE, Sungyoung Lee, Member, IEEE, and Young-Jae Song, Riaz Ahmed Shaikh 2008Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks

[5] 172-185, IEEE Transactions On Network And Service Management, Vol. 7, No. 3, September 2010 Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model Pedro B. Velloso, Pujolle

[6] Jamming attacks and counter measures in Wireless Sensor Network

[7] Jun luo and Dongning Guo,(2005), " Neighbour discovery in wireless ad hoc networks based on group testing," in Proc.Annu,Allerton Conf.,2Volume 50,pp.794-797

[8**]** Sudarshan Vasudevan,Mich Adler,Dennis Gocckel And Don Towsley(2013)Efficient Algorithms For Neighbor Discovery In Wireless Networks Volume 20,pp 103-120.

[9] Sherin Abel Hamid,Hossam Hassanein,Glen Takahara, December2011,1to54 Routing for wireless melti hopnetworksuNIFYINGAND Distinguishing Features

[10] www.wikepedia.com

[11] www.cisco.com

[12] www.PacketDeliveryratio.awk.com

[13] http://www.businessdictionary.com/definition/overhead.html