International Journal For Technological Research In Engineering
Volume 2, Issue 7, March-2015 *ISSN (Online): 2347 - 4718*

REVIEW OF DETECTION, ELIMINATION AND SIMULATION ANALYSIS OF BLACK AND GRAY HOLE ON AD-HOC NETWORK BY ADVANCE AODV PROTOCOL

Priyanka[1], Professor Nasib Singh Gill[2]
[1]M.Tech (CSE), [2]HOD, Dept. Of Computer Science and Application
MDU Main Campus, Rohtak

ABSTRACT: ***MANETS can be used for easing of the collection of sensor data for data mining for a number of applications such as air pollution controlling and different types of models can be used for such type of application. This kind of data idleness due to the spatial link between sensors observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial link between data sampled by different antenna or sensors, a large group of specialized algorithms can be developed to develop more proficient spatial data mining algorithms as well as more proficient routing approach. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes by mean of ZRP protocol. The result has been quite significant for detection algorithm and less time for operation. Elimination procedure is also improved by the use of ZRP protocol due to its zonal feature of nodes. Shortest path to a Destination node and then purposely drops the packets. Further This attack terribly reduces the network performance. In this studies Black hole attack in AODV routing protocol. Study of literature indicates many alteration have been offered in the AODV protocol to detect and prevent Black hole attack. These methods are studied in the paper with their advantages & disadvantages and their future scope is also calculated. The performance of the network parameters like routing overhead, end to end delay, throughput, packet delivery ratio are compared in all the circumstances.***

Keywords-Mobile Ad-hoc Networks, Black Holes, Gray Holes, Routing, ZRP, Routing Table, Improved AODV

I. INTRODUCTION

In this modern world there is a huge requirement of the autonomous mobile system. Significant examples comprises of establishing survivable, proficient, dynamic communication for emergency/rescue operations, disaster liberation efforts, and military networks. Such network development cannot rely on centralized and organized connectivity, and can be visualized as applications of Mobile Ad Hoc Networks. A MANET is an independent collection of mobile users that correspond over relatively bandwidth constrained wireless links. As the nodes are independent and mobile, the network topology may change quickly and unexpected over time. The network is decentralized. Topology discovery, message delivering and all such network activity must be executed by the nodes i.e. The MANETs application is diverse, ranging from small, fix networks that are constrained by power sources, to huge-scale, mobile, highly movable networks. The design of network protocols for these type of networks is a complex concern. In spite of the application, MANETs need proficient distributed algorithms to determine network organization, link arrangment, and routing. However, determining doable routing paths and delivering messages in a decentralized milieu where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a constant or centralized network is usually the best route, such plan is not so convenience, to MANETs. The network should be able to adaptively change the routing paths to assuage any of these effects. Moreover, in latency, intentional jamming, preservation of security, reliability, and failure recovery are important concerns. The Military networks are modeled in such a way that to a low chances of intercept and/or a low chance of detection. Hence, nodes gave importance to radiate as little power as necessary and transmit as infrequently as they can, thus decreasing the probability of interception. if any fall occur in any of these essentials than it may degrade the performance and dependability of the network. A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that have the ability to correspond with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not handled by any other controlling entity, they can move independently and can connect to the other nodes. Network management and routing are done willingly by each other nodes. As just because of the mobility nature of it, they are less secure as compare to the centralized approach. ZRP is a source initiated on-demand routing protocol. Every mobile node coordinate a routing table that manage the next hop node information for a route to the destination node. If a source node wants to route to the destination node then need a fresh route from the routing table. If it not found a fresh route then it starts a route discovery process and broadcast the Route Demand (RREQ) message to its all neighbor , which is additional propagated until it reaches an midway node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. Each midway node receiving the RREQ and makes an entry in table for the node that forwarded the RREQ message, and the source node. The destination node or the midway node with a fresh enough route to the destination node, unicast the Route Response (RREP) message to the neighboring node from which it received the RREQ. A midway node makes an entry for the neighboring node from which it received the RREP, then forwards the RREP in the opposite direction

from destination to the source. Then after getting the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. Then after it the source node starts routing the data packet again to the destination node through the neighboring node that first responded with an RREP. A black hole is a malicious node that bogus replies for any Route Demands (RREQ) without having active route to specified destination and drops all the receiving packets. If malicious nodes works then the damage may be very critical . This attack is called cooperative black hole attack. A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. In this paper we present a mechanism to detect and remove the above two types of malicious nodes.

Improved AODV: This is a framework by using it we can take advantage of both table driven and on demand driven protocol according to the application. Disconnection of nodes, local neighborhood or near by nodes from the global topology of the entire network allows for applying different approaches and thus we can take advantage of each technique's features for a given situation. These local neighborhoods are called zones (hence the name) each node may be within multiple overlapping zones, and each zone may be of a different size. But the size of the zone is not a standard unit as determined by geographical measurement , as one might expect, but is given by a radius of length α where α is the number of hops to the perimeter of the zone.

II. LITERATURE SURVEY

1] A Study on Wormhole Attacks in MANET - Reshmi Maulik1 and Nabendu Chaki2

- In this paper, under wormhole attack we have analyzed the performance of Mobile Ad-hoc Networks (MANET) . Throughput, delay, packet delivery ratio, node energy and node density are some parameter that are considered here. The NS2 network simulator used and the reference point group mobility model (RPGM) is considered to study the effect of node density and the initial energy on the throughput.

2] Mobile Ad Hoc Networking: Imperatives and Challenges - Pravin Ghosekar, Girish Katka , Dr. Pradip Ghorpade- Pravin Ghosekar,

- This paper gave idea of comprehensive overview of this dynamic field. This paper explain the important role that MANETs play in the evolution of future wireless technologies. Then, it reviews areas of MANET_s, characteristics, capabilities and applications.

3] A Framework for Reliable Routing in Mobile Ad Hoc Networks- Zhenqiang Ye, Satish K. Troute ipathi, Srikanth V. Krishnamurthy,

- It shows the chances of setup a reliable path in between a random source and destination pair increases continuously even with a low percentage of reliable nodes when we control their positions and curve or path in accordance with our algorithm.

4] Analysis of TCP Performance over Mobile Ad Hoc Networks - Gavin Holland, Nitin Vaidya

- In this paper, we investigate the consequences that link breakage due to mobility has on TCP performance. Through simulation, we show that when nodes move, TCP throughput goes down due to TCP's inability to identify the difference in between link failure and jamming. We also study some particular examples, such as a situation where throughput is zero for a particular connection

5] MANET Routing Protocols and Wormhole Attack against ZRP - Rutvij H. Jhaveri1, Ashish D. Patel2, Jatin D. Parmar3

- In this paper we have studied some basic routing protocols in MANET like Destination Sequenced Distance Vector, Temporally-Ordered Routing Algorithm, Dynamic Source Routing and Ad-hoc On Demand Distance Vector. Security is a big issue in MANETs as they are infrastructure-less, non centralized and autonomous. Motive of this paper is to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. This concept will be a great helpful for the researchers conducting research on real world problems in MANET security.

6] An Proficient Wormhole Prevention in MANET through Digital Signature- Anil Kumar Fatehpuria1, Sandeep Raghuwanshi2.

- In this paper we represent apparatus which is helpful for prevention of wormhole attack, through observing the delay of different path to receiver and verification of digital signature. Our mechanisms detect pinpoint location of wormhole and prevent them. This method requires neither coordinated clocks nor special hardware equipped mobile nodes.

7] Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks- Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard

- This generic characteristic of MANET has turn into it vulnerable to security attacks. In this paper, we address the problem of direct attack by multiple black holes acting in multi pair. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route preventing supportive black hole attack.

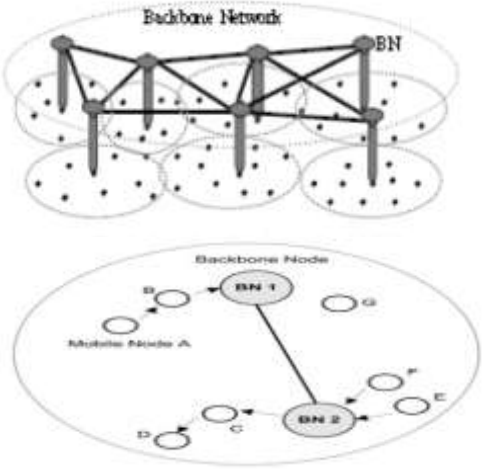
8] Prevention of Co-operative Black Hole Attack in MANET- Latha Tamilselvan, Dr. V Sankaranarayanan

- This approach to fight with the Black hole attack to make use of a 'Fidelity Table' wherein every entry node will be assigned a fidelity level which acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is removed. Computer simulation using GLOMOSIM shows that our protocol provides better security and also better performance in terms of packet delivery

than the conventional ZRP in the presence of Black holes with minimal packet drop ratio and reliability.

EXISTING METHOD TO DETECTION AND REMOVAL OF BLACK / GRAY HOLES

Initially when the source node wants to make a data transmission, it demands the nearest BBN for a restricted IP (ROUTE IP). The BBN on receiving the ROUTE IP answers to the source node with one of the unused IP addresses selected randomly out of the pool of unused IP addresses. Then the source node sends the RREQ for the destination as well as the ROUTE IP . Now if the Source Node (SOURCE NODE) gets the RREP only for the destination node(which is the normal case) and not the ROUTE IP, then the local network space is free from any of the black holes and currently free of any gray holes too. The source node reuses the ROUTE IP for a definite period of time for further data transmissions. Tell that time the BBN does not assign any other node, this recently given out ROUTE IP. However in case the SOURCE NODE gets an RREP for the ROUTE IP, then it means that, there is a black hole in that route. In this case the SOURCE NODE initiates the process of Black Hole detection. The SOURCE NODE initially alerts the neighbours of the node from which it got the RREP to ROUTE IP, to enter into promiscuous mode, so that they listen not only to the packet destined to them, but also to the packet destined to the specified Destination node. Now the SOURCE NODE sends a few dummy data packets to the destination, while the neighbouring nodes start monitoring the packet flow. These neighboring nodes further transmit the monitor message to the next hop of the dummy data packet & so on. when during monitoring nodes finds out that the dummy data packet loss is way more than the normal expected loss in a network, it informs the SOURCE NODE about this particular Midway Node(IN). Now depending on the information received by the various monitoring nodes, detects the location of the Black Hole. SOURCE NODE detects the location of the Black Hole. This information is propagated throughout the network leading to its listing as black hole and revocation of their certificates. Further all nodes reject any further responses from this black hole and looks for a valid substitute route to the destination.



The above technique also works for gray holes also, as we are not using any trust based relationship between nodes it is detected by normal Data transmission process by any of its neighboring normal nodes. Even in the case of cooperative black holes, the node that ultimately eats up the data packets, gets hold. As well as the Source Node decides the location of a black hole by the advice of more than just one neighboring node. Hence it will lead to the detection and elimination of the malicious node.

Figure 1. Pictorial Representation of an Ad hoc network with a back bone network.

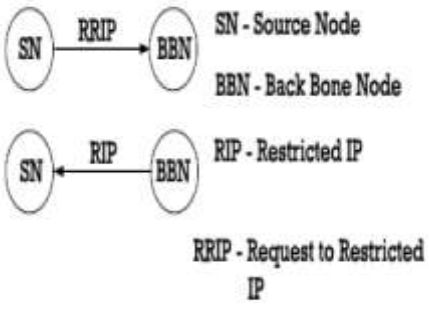


Figure 3. Nodes and their representation

RREQ - Route Request packet
RREP – Route Response packet

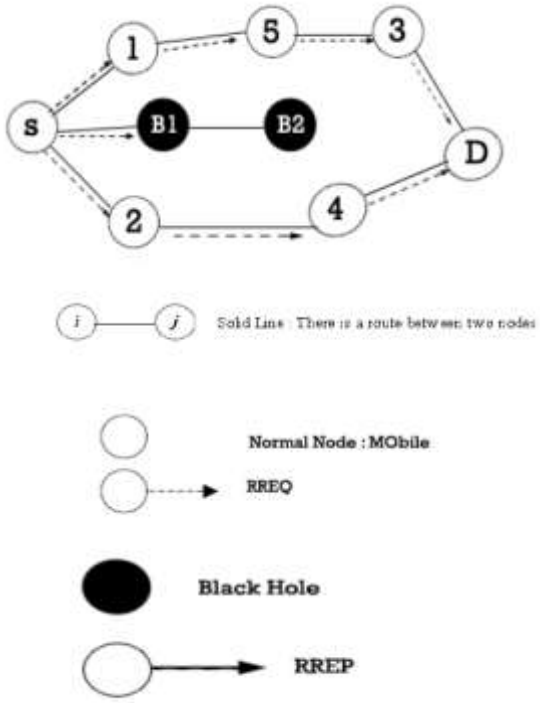


Figure 4. Propagation of RREQ message

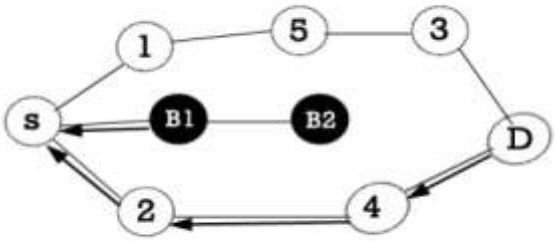


Figure 5. Propagation of RREP

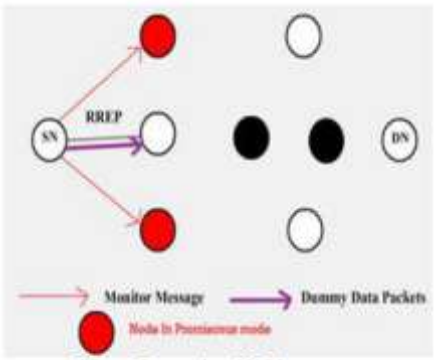


Figure 6. Propagation of Monitor message & dummy data packets

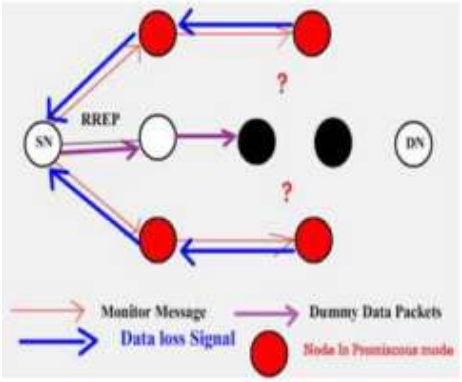


Figure 7. Identification of the Black Hole by promiscous nodes

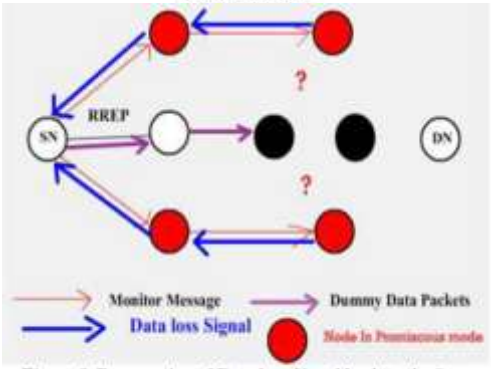


Figure 8. Propagation of Data loss Signal back to the Source Node

OUR PROPOSED TECHNIQUE METHODOLOGY & ALGORITHM

Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically demands one of the backbone nodes for a restricted (unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (ROUTE IP) also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

Network Model & Assumption

We approach this problem by selecting some nodes which are trustworthy and powerful in terms of battery power . These particular nodes which are submitted as Back Bone Nodes (BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes (BBN) and the Normal Nodes, it is assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations. It is also assumed that the number of normal nodes are more then the number of black/gray nodes at any point of time.

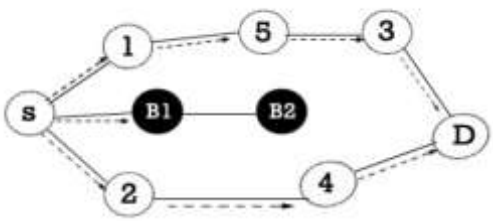
Allocation of IP address

The IP address configuration in case of MANETs can broadly be classified into- i.Stateless approach ii. State full approach In the stateless approach an unconfigured host must obtain its own IP address by self assignment. This stateless approach adopts random address assignment and is followed by duplicate address detection mechanism to achieve address uniqueness. Stateless approaches do not keep any allocation table. In the state full approach an unconfigured host asks its neighboring MANET to work as proxies to obtain an ip address. We have devised a new type of state-full approach viz. Core Maintenance of the Allocation Core Maintenance of the Allocation. In this approach only the backbone network in MANET is permitted to select the IP addresses for unconfigured hosts. The mechanism is based on allocating a conflict free address to all newly arrived nodes by using multiple disjoint address spaces[6]. Each BBN in MANET is responsible for allocating a range of addresses disjoint from the ranges of outer backbone node. In other words each BBN generates numbers that are unique for that host. Every hosts in the MANET must have the possibility to reach one of the Backbone Nodes (BBN) all the time.

Algo for Detection and Removal of Backhole and Grayhole Atttacks in Manet Roles assigned: Backbone (BBN) node: Its main responsibility is to carry on the actual detection of black/grayhole attack and coordinate with the neighbors of the nodes present in the RREP for black and grayhole node detection. It also provides ROUTE IP(Restricted IP) if demanded by the sender. Sender Node: Sends RROUTE IP (Demand for Restricted IP) to the BBN and the RREQ to the destination node D. Other nodes in the network: Maintain a Malicious Node table and Blacklist table and work in coordination with the BBN for black and grayhole detection. Abbreviations: BBN: Backbone Node ROUTE IP : restricted IP RROUTE IP: Demand for Restricted IP Nrrep : id of the node sending route reply message to S

Detection Algo
Step 1: Source Node(SOURCE NODE) sends a Demand to Restricted IP(RROUTE IP) to the Back Bone Node(BBN).
Step 2: On receiving the Restricted IP(ROUTE IP), from the BBN it sends the RREQ for the Destination as well as for the ROUTE IP simultaneously and awaits for reply (RREP)
Step 3: On receiving the RREP, each node forwarding the RREP to the sender matches the RREP nodes with the node entries present in the Malicious Node and Blacklist table maintained at each node in the network. If the nodes in the RREP do not match with the entries in the two tables then the RREP is forwarded towards the sender node S.
Removal process: Step 1: If the RREP is received only to the Destination & not to the Restricted IP (ROUTE IP), the node carries out the normal functioning by transmitting the data through the route.
Step 2 for the ROUTE IP, If the RREP is received then it will initiates the process of black hole/grayhole detection, by sending a demand to the BBN to enter into promiscuous mode.
Step 3: The BBN now starts the monitoring of the nodes in the RREP path and sends a PMODE_ON message to the sender node to notify that the promiscuous mode is ON for the BBN.
Step 4: On receiving the PMODE_ON message from BBN the sender node S sends a dummy packet through the same route reply(RREP) for the destination D.
Step 5: The BBN Inclucate all neighbors of Nrrep (of the node sending route reply message to S) to vote for the next node to which Nrrep is forwarding packets originating from S and destined to D.
Step 6:On receiving node ids from neighbors of Nrrep, BBN elects the next node to which Nrrep is forwarding the packets based on reported reference counts.
Step 7: To the next node if dummy packets are send in the path which is the same node as the elected node then we replace the elected node as the Nrrep node and we verify the next node for the new Nrrep node with the help of neighbous of new Nrrep.
Step 8: If the elected node is a null node, Nrrep is itself dropping all the packets. We cross verify the malicious behavior of the elected node with the simultaneous dropping of dummy packet by the same node in the network.
Step 9: On detection of the malicious node, its node ID is broadcasted to the remaining nodes in the network including the sender node. The other nodes in the network then append this malicious node entry in the Maliciousource nodeode table which is maintained at each node in the network and its count is set to 1.

EXAMPLE:



MaliciousNode Table

Malicious Node Entry	Count
4	5
5	2

Blacklist table

Blackhole/Grayhole Node
4

Step 10: when the node entry previously exist in the Malicious node table then increase its count by count+1.
Step 11: if the threshold value of any node increase in the malicious node table at any point of time then that node is detected as Black hole Node and its node ID is sent to the BBN.
Step12: the black hole node id is then broadcast by the BBN to all other nodes in the network and the node ID is affix in the Blacklist table maintained at each node.
Step 13: This Blacklist table is used by all the nodes in the network for all the future RREQ demands. If any node receives a RREP from a node present in the Blacklist table then that RREP is discarded and it is not forwarded to the sender node S.

III. SECURITY AND CONCERN

We take 4 most reliable nodes (based on packet dropping ratio and high battery power) out of which one node is selected as the Backbone Node (BBN) and the other nodes are candidate nodes. If the battery power of BBN node is down then it transfers the control to the second candidate node and that node becomes the new BBN node. The malicious node table and blacklist table are commonly shared between all the candidate nodes. The read/write access is available only with the active node, i.e. the BBN node.

IV. EXPECTED CONCLUSION

Blackhole Attack in Manet is a Denial of Service Attack which reduces the network performance. The study here shows different modified versions of AODV algorithms which have been proposed and implemented to prevent and detect Blackhole attack. A comparison table shows the performance of methods, their limitations and Future work. The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table i.e., whenever a new node joins the network, it sends a broadcast message as a demand for particular IP address. Then the backbone node after receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an grant to the BBN. Now since the allocation is only under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.As after the whole process we can get better result.

REFERENCES

[1] "Security Issues in Mobile Ad Hoc Networks- A Survey" Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.
[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.
[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.
[4] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA
[5] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.
[6] Sudath Indrasinghe, Rubem Pereira, John Haggerty,"Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)
[7] Mansoor Mohsin and Ravi Prakash,"IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016
[8] P. Agrawal, R. K. Ghosh, and S. K. Das. Localization of wireless sensor nodes using proximity information. In Proceedings of IEEE ICCCN07, pages 485–490, 2007.
[9] N. Bulusu, J. Heidemann, and D. Estrin. Gps-less low cost outdoor localization for very small devices. IEEE Personal Communications Magazine, 7(5):28–34, 2000.

