IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 3 (Mar. - Apr. 2013), PP 82 -88
www.iosrjournals.org

Enhancement in Elimination of Security Threads using Trusted Proactive Routing

Shilpa Jaiswal[1], Anil Kumar Patidar[2]
[1]*Research Scholar, Computer science &Engineering, AITR Indore/RGPV Bhopal, India*
[2] *Asst. Prof., Computer science & Engineering,AITR Indore/RGPV Bhopal, India*

Abstract:*Ad hoc networks have been used in many applications which mandate a dynamic setup in the absence of fixed infrastructure. The design of ad hoc network has been mainly focuses on proper operation. It is possible that eventually a malicious node becomes easy to deploy in ad hoc n/w and they cause among other impact performance degradation. One attack that can deploy by malicious node is black hole attack. This paper reviews the problem of occurrence of black hole attack and its solution technique proposed enhancement in proactive routing protocol Destination Sequenced Distance Vector Routing protocol Using trust based and hop count method.*

Keywords: *ad hoc networks, black hole, security, routing, DSDV*

I. Introduction

Unlike a fixed wireless network, wireless ad hoc networks or on the fly networks are characterized by the lack of infrastructure. Nodes in the mobile ad hoc networks are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communicating with others. The path between each pair of the users may have the multiple links, and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. Mobile ad hoc networks can operate in a standalone fashion or cloud possibly be connected to a larger network such as the Internet.Ad hoc networks are suited for use in situations where an infrastructure is unavailable or deploying is not cost effective. One of many possible uses of mobile ad hoc networks is in some business environment, where the need of collaborative computing might be more important outside the office to brief clients on a given assignment. A mobile ad hoc network can also be used to provide crisis management services application, such as in disaster recovery, where the entire communication infrastructure is destroyed and resorting communication quickly is crucial. By using a mobile ad hoc network, an infrastructure could be set up in hours instead of weeks, as is required in the case of wired line communication. Another application example of a mobile ad hoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as sharable devices, printers, scanners, music systems and personal digital assistants. The IEEE 802.11 (for Wi-Fi) protocol also supports an ad hoc network system in the absence of a wireless access point.

1.1 Mobile Ad Hoc Networks

The mobile ad hoc networks have received tremendous attention because of their self-configuration and self-maintenance capabilities. Although security has long been an active research platform in wireless networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain.

There are basically two routing approaches to protecting MANET: proactive and reactive. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques. In contrast, the reactive approach seeks to detect security threats a posteriori and react accordingly. Due to the absence of a clear line defense, a complete security solution for MANETs should integrate both approaches and encompass all three components: prevention; detection and reaction. For example, the proactive approach can be used to ensure the correctness of routing states, while the reactive approach can be used to protect packet forwarding and packet dropping attacks.

With the advent of internal architecture of MANET, there are various applications found which reflects the infrastructure less scenario in good extent. Like:

- Autonomous terminal
- Distributed Operation
- Multi hop Routing

- Dynamic Network Topology
- Fluctuating Link Capacity
- Light Weight Terminals

1.2Black Hole Attack

General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count.

A black hole attack is one in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DOS) by dropping the received packets. In black hole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as shown in figure 1.2.

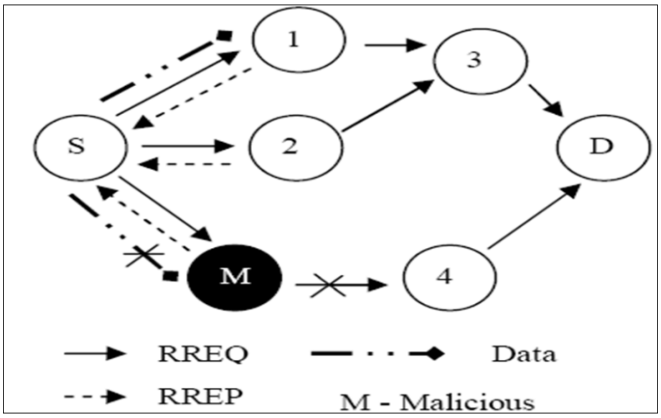


Figure 1.2. Black Hole Attack

II. Literature Survey

Many researchers have addressed the black hole attack problem in MANET. Most of the solutions proposed and implemented were based on AODV and DSDV protocol.

LathaTamils Elvan, Dr. V Sankaranarayanan [2] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is given to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated.

E.A Mary Anita et al [3] proposed a solution implemented on the top of ODMRP protocol. The authors proposed a certificate based authentication mechanism to counter the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority.

Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU [4] proposed an adaptive approach to detect black and gray hole attacks in ad hoc network based on a cross layer design. In network layer, a path-based method to overhear the next hop's action. This scheme does not send out extra control packets and saves the system resources of the detecting node. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. They choose DSR protocol to test algorithm and ns-2 as simulation tool.

Wei Gong1,2, Zhiyang You1,2, Danning Chen2, Xibin Zhao2, Ming Gu2, Kwok-Yan Lam2 [5]proposed use of trust vector model based routing protocols. Each node would evaluate its own trust vector parameters about neighbors through monitoring neighbors' pattern of traffic in network. At the same time, trust dynamics is included in term of robustness. Then the performance of the proposed mechanism by modifying Dynamic Source Routing (DSR) so that each node has a dynamic changing "trust vector" for its neighbors' behaviors.

N. Bhalaji1, Dr. A. Shanmugam2 [6] proposed an improvement of the Association based Route selection to be applied to the DSR protocol in order to enhance its routing security. The purpose of applying the association based route selection to the DSR protocol is to fortify the existing implementation by selecting the best and securest route in the network. In contrast to the current route selection in the DSR which involves selection of the shortest route to the destination node, our proposed protocol choose the most reliable and secure route to the destination based on the trust values of all nodes. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes.

K.SelvavinayakiK.K.Shyam Shankar Dr.E.Karthikeyan [7] proposed solution that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed method is to be adapted on DSR protocol and needs to be simulated and analyzed for different performance parameters .This method is capable of detecting and removing black hole nodes in the MANET.

III. Problem Domain

As discussed in the previous sections, most of the proposed solutions are built on a number of assumptions which are either hard to realize in a hostile and energy constrained environment like MANETs or not always available due to the network deployment constraints **[8]**. Due to these reasons, many challenges have to be carefully considered in order to design a robust solution to cope with the packet dropping attack. First, the attackers' behaviors are tailored to the specific routing protocol, making it impossible to build a general model for characterizing the attacker. Most of the solutions are firstly given on AODV protocol and then to DSR. Many other protocols have to be worked on. Secondly, how to use this model to achieve a high level resistance against these attacks while maintaining network performance. Also as known that the Trust Based Model needs to be implemented on grey- hole and cooperative gray hole attacks recently, most of the proposed solutions are focused on adding new components to the original protocol to assess the deviation of the neighboring nodes and monitor their behaviors. However the use of these additional components might remove an important performance optimization.

As till date most of the work has been done on the reactive routing protocols and various solutions are being proposed for mitigation of various types of attacks e.g. Black hole, wormhole, DOS and Rushing attacks as per literature review. Our main interest of work is to implement the prevention techniques for Proactive routing protocols e.g. DSDV and OLSR.

We might think that if some better protocols than DSDV are already their which have the sufficient solution to mitigate the black hole attack than why we have chosen this particular protocol for our proposed research area of concern the reason w.r.t Certain parameters are illustrated below:

Node Energy: While comparing reactive and proactive protocols on the basis of node energy obviously proactive protocols consumes more energy in compare with reactive routing protocols as we talk about battery power, Because in proactive protocols routing updates are being exchanged frequently but in reactive protocols this is not done they exchange routing table only on demand by node.

Timeliness: while talking about time for sending data that is End to end delay obviously proactive protocols are better than reactive routing protocols because proactive routing protocols have latest most routing table with its individual node while reactive routing protocols not.

Detection of black hole attack required latest information of every node. Disadvantage of Some routing algorithm is that Intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. For detecting malicious node we required root discovery mechanism.to detecting this type of attack fast we needed a mechanism that contains regularly updated routing table.it required a routing algorithm that has less latency factor.

IV. Related Work

4.1 Routing in Ad-Hoc Network

Routing in ad-hoc networks involves finding a path from the source to the destination, and delivering packets to the destination nodes while nodes in the network are moving freely. Due to node mobility, a path established by a source may not exist after a short interval of time. To cope with node mobility nodes need to maintain routes in the network. Depending on how nodes establish and maintain paths, routing protocols for ad-hoc networks broadly fall into pro-active [9], reactive [10, 11], hybrid [12], and location-based [13, 14, 15] categories.

4.2 Proactive Routing Protocols

Pro-active routing protocols are table-driven protocols that maintain up-to-date routing table using the routing information learnt from the neighbors on a continuous basis. Routing in such protocols involves selecting a path form the source to the destination, where the source node and each intermediate node selects a next hop, by routing table look up, and forwarding the packet to next hop until destination receives the packet. A drawback of such protocols is the proactive overhead due to route maintenance and frequent route updates to cope with node mobility. An example of this class is the DSDV [9].

DSDV:

The Destination-Sequenced Distance-Vector Routing protocol (DSDV) is an enhanced version of distributed Bellman-Ford algorithm, for mobile ad-hoc networks.It was developed by C. Perkins and P. Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. In this protocol, each node maintains a routing table that contains an entry for every node in the network. Each entry in the routing table consists of the destination ID, the next hop ID, a hop count, and a sequence number for that destination. The sequence number helps nodes maintain a fresh route to the destination(s) and avoid routing loops. To cope with frequently changing network topology, nodes periodically broadcast routing table updates thought-out the network.

When a node receives a route-update packet, it changes its routing table entries if the sequence number of the destination in the update packet is higher (fresh) than the one in its routing table. If the sequences numbers are the same, then the node selects a route with smaller metric (hop count). To reduce the network traffic due to large update packets, DSDV employs two types of updates –full dump and incremental. A full dump packet generated by a node contains all entries in its routing table. Whereas an incremental packet contains only the routing table entries that are changed by the node since the last full dump. A node triggers an update when either the metric for a destination changes or when the sequence number changes. In the later case, it is called DSDV-SQ.

4.3 Reactive Routing Protocols

Reactive routing protocols are demand-driven protocols that find path on-the-fly as and when necessary. In such protocols, establishing a new route involves a route discovery phase consisting of route request (flooding) and a route reply (by the destination node). Nodes maintain only the active routes until a desired period or until destination becomes inaccessible along every path from the source node. A drawback of such protocols is the delay due to route discovery on-the-fly. We briefly discuss the AODV and DSR protocols next.

DSR:

Dynamic Source Routing (DSR) [10] was one of the first reactive routing protocols for ad-hoc networks. In DSR, nodes use RREQ, RREP, and RERR packets to establish and maintain paths to the destination. However, unlike AODV, RREQ packet accumulates a list of node IDs along the path from the source to the destination and the corresponding RREP packet carries this list of IDs back to the source. Once the source node receives RREP packet, it starts transmitting data packets to the destination by embedding the route from the source to the destination in the packet header. The path in the data packet header is referred to as the “source route".

Every node in the network stores route to other nodes in the network by maintaining a dynamic route cache. A node learns routes to other nodes when it initiates a RREQ to a particular destination or when the node lies on an active path to that destination. In addition to these, a node may also learn a route by overhearing transmissions (in the promiscuous mode) along the routes of which it is not a part.

4.4 Hybrid Routing Protocols

Hybrid protocols combine the advantages of various approaches of routing protocols into a single protocol. The Zone Routing Protocol (ZRP) [12] is one such hybrid protocol that combines both the proactive and reactive routing approaches. ZRP takes advantage of pro-active discovery within a node’s local neighborhood, and uses a reactive protocol for communication between these neighborhoods. The local neighborhoods are called Zones, and each node may be within multiple overlapping zones.

ZRP is motivated by the fact that “the most communication takes place between nodes close to each other. Changes in the topology are most important in the vicinity of a node - the addition or the removal of a node on the other side of the network has only limited impact on the local neighborhoods". The performance of ZRP depends on choosing a radius, which decides the transition from pro-active to reactive behavior. With a carefully chosen radius, ZRP can achieve better efficiency and scalability over both pro-active and reactive routing protocols.

4*.5 Position-based Routing Protocols*

Position-based routing protocols utilize position of nodes in the network and make the least use of the topology information. Routing protocols using such a scheme eliminate drawbacks due to frequently changing network topology. DREAM [13], GPSR [14], and LAR [15] are some of the examples of position-based routing protocols.

In Position-based routing protocols nodes maintain local (one or two hop) topology information with the help of a hello protocol. To route a packet to the destination, the source node uses a greedy-forwarding to select a next hop towards the destination. In greedy-forwarding, a node selects a next-hop towards the destination that is geographically closest to the destination among its neighboring nodes. Since there is no pre-established route from a source to the destination, each packet may follow a different path depending on the network topology.

There are two parts to position-based routing: (a) given the position of the source, the position of the destination, and a local neighbor table of each node, delivering packets from the source to the destination, and (b) given that each node can determine its own position, using some positioning system like GPS, obtaining the position of any other node in the system. The former part is the position-based routing, examples include GFG [17], GPSR [14].

Position-based routing is typically greedy-forwarding along with a recovery mechanism to circumvent local optima due to greedy-forwarding, a condition where there is no node close to an intermediate node in its neighborhood than the node itself. The later part is called the location service. Some of the examples of location-service protocols are GLS [18], DLM [19], and RLS. Interestingly, most location-service protocols including GLS and DLM, rely on the underlying greedy forwarding algorithm (although there are few other variants of greedy forwarding exists) to send and receive control packets like location updates and location queries.

The advantage of these protocols is that nodes need not establish, maintain routes, and these protocols are more scalable compared to reactive and pro-active routing protocols.

V. Proposed Scheme

We propose a solution that is an enhancement of the basic DSDV routing protocol, which will be able to avoid black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer in the ‘Timer Expired Table’, for collecting the further requests from different nodes that having hop count equals to 2. It will store the ‘sequence number’, and the time at which the packet arrives, from those nodes to check which node is replying. The time for which every node will wait is proportional to its distance from the source. It calculates the ‘timeout’ value based on arriving time of the first route request. According to Trust Based DSDV the requesting node transmit request to the node having hop count 2, then calculate the ratio of their total reply and time taken by all reply and generate trust value between 0 to 10, for those the neighboring nodes who reply for the request will have trust value greater than 5, the neighboring node that are reply for some of the request will have reply ratio less than those neighbor who are good to reply, and these neighbor have trust value less than 5, based on these trust values we find neighbors who have trust value minimum and remove its entry from the routing table, and based on trust values a safe route to the destination to reduce the probability of Black Hole Attack is generated. After the trust value calculation, it first checks in Routing Table whether there is any entry for the node and its trust value for hop node. If any entry to next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

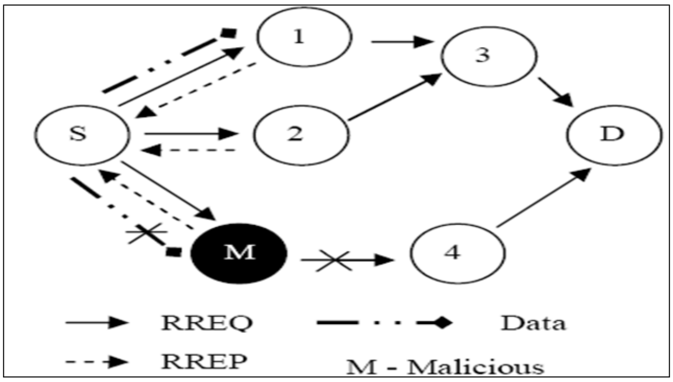
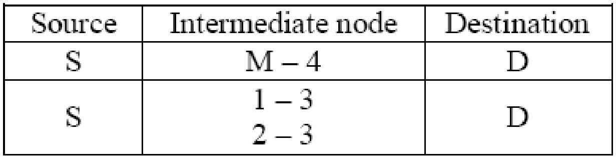


Figure 5.1: Solution to Black Hole

In the above figure 5.1, S wants to transmit to D. So it first transmits the route request to all the neighboring nodes. Here node 1, node M and node 2 receive this request. The malicious node M has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as (M – 4). Instead of transmitting the DATA packets immediately through M, S has to wait for the reply from the other nodes. After some time it will receive the reply from node 1 as (1 – 3), and node 2 as (2 – 3). According to this proposed solution it first checks the path in the routing table that contains trust value acceptable for next hop node to the destination. If there is a path node having trust than select that path and transmits the data through that path. The routing table from S to D is given in table 5.1.

Table 5.1: Routing Details



Source	Intermediate node	Destination
S	M – 4	D
S	1 – 3 2 – 3	D

In contrast to the current route selection in the DSDV which involves selection of the shortest route to the destination node, our proposed protocol choose the most reliable and secure route to the destination based on the trust values of all nodes. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes.

The trust values are calculated based on the following parameters of the nodes. We propose a very simple equation for the calculation of trust value.

5.1. Nature of Association & Association Estimator Technique

In our proposed scheme we classify the Association among the nodes and their neighboring nodes in to three types [18] as below. In an Ad-hoc network the Association between any node x and node y will be determined as Unknown, Known, Companion. These Associations are represented in an Association table which is part of every node in the Ad-hoc network. The Association status [16] [17] which we discussed in the previous section depends up on the trust value and threshold values. The trust values are calculated based on the following parameters of the nodes. We propose a very simple equation for the calculation of trust value.

$T = (R1+R2+A)$ (1)

Where

T = Trust value

R1= Ratio of number of packets actually forwarded by a node to the number of packets forwarded by that node.

R2 = Ratio of number of packets received from a node but originated from others to total number of packets received from it.

A = Acknowledgement bit. (0 or 1)

VI. Conclusion

Security of MANET is one of important feature for its deployment. This work concentrates on behavior and challenge in mobile ad hoc network with solution finding technique. The efforts are continues in terms of routing security. The attack analyzed is black hole attack and proposed technique is proactive in nature and based on the concept of enhancement in existing DSDV protocol using trust based method. It provides a solution for identification and removal of black hole attack.

Besides the study will helps to overcome the DSDV protocol flaws so that it could be made more robust against attack.The feature work involve simulations gave various results to actuate the problem of black hole attack occurrence and to motivate existing protocols update for removal of this attack.

References

[1] Umang Singh, "Secure Routing Protocols in Mobile Ad-hoc Networks-A Survey and Taxonomy" International Journal of Reviews in computing30th September 2011. Vol. 7

[2] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Black hole Attack in MANET",JournalOfNetworks, Vol.3, No.5, May2008

[3] E. A. Mary Anita and V. Vasudevan, Black Hole attack Prevention in multicast routing Protocols For MANETs Using Certificate Chaining, IJCA, Vol.1, No.12, pp. 22–29,2010

[4] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU , An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network . 2010 24th IEEE International Conference on Advanced Information Networking and Applications

[5] Wei Gong1,2, Zhiyang You1,2, Danning Chen2, Xibin Zhao2, Ming Gu2, Kwok-Yan Lam2,'Trust Based Malicious Nodes Detection in MANET' . 978-1-4244-4589-9/09/$25.00 ©2009 IEEE

[6] N. Bhalaji1, Dr. A. Shanmugam2, Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET .JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY, VOL. 2, NO. 2, MAY 2011

[7] K.SelvavinayakiK.K.Shyam Shankar Dr.E.Karthikeyan, Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs .International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[8] SoufieneDjahel, FaridNa¨ıt-abdesselam, and ZonghuaZhang , Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges . IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION.

[9] Routing Protocols to Enhance Security in MANETSRakeshVanaparthiα, Pragati.G Global Journal of Computer Science and Technology Volume 11 Issue 13 Version 1.0 August 2011

[10] K.P.Manikandan,Dr.R.Satyaprasad,Dr.K.Rajasekhararao "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks" International Journal of Advanced Computer Science and Applications,Vol. 2, No.3, March 2011 http://ijacsa.thesai.org/

[11] Santhosh Krishna B.V, Mrs.Vallikannu A.L [12] "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism "International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010

[12] Z. Haas and M. Pearlman.The performance of query control scheme for the zone routing protocol.*ACM/IEEE Transactions on Networking, 9(4) pages 427-438*, August 2001.

[13] S. Basagni, I. Chlamtac, V. Syroutik, and B.Woodward.Adistance effect routing algorithm for mobility (DREAM). *In proceedings of the 4th annualACM/IEEE Int. Conf. on Mobile Computing and networking (MOBICOM)*, pages 76-84, Dallas, TX, USA, 1998.

[14] Karp, B., and Kung. H. T. GPSR: Greedy Perimeter Stateless Routing forWireless Networks. *Proc. 6th Annual International Conference on Mobile Computing and Networking* (MOBICOM 2000), 243-254.

[15] Young-BaeKo ,Nitin H. Vaidya. Location-aided routing (LAR) in mobile ad-hoc networks.*ACM/Blatzer Wireless Networks journal*, 6(4)pages 307-321, 2000.

[16] Z. Haas and M. Pearlman.The performance of query control scheme for the zone routing protocol.*ACM/IEEE Transactions on Networking, 9(4) pages 427-438*, August 2001.

[17] Prosenjit Bose, Pat Morin, Ivan Stojmenovic, and Jorge Urrutia.Routing with Guaranteed Delivery in Ad Hoc Wireless Networks.*Wireless Networksi*7, 609-616, Kluwer Academic Publishers 2001.

[18] Jinyang Li, John Jannotti, Douglas S. J. De Couto, David R. Karger, Robert Morris.AScalable Location Service for Geographic Ad Hoc Routing. *Proceedings of 6th ACM International Conference on Mobile Computing and Networking (MOBICOM)* 2000.

[19] Y Xue, B Li and KNahrstedt.A scalable location management scheme in mobilead-hoc networks.*26th Annual IEEE Conference on Local Computer Networks* (LCN 2001).