ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 3, May2012

REMOVAL OF BYZANTINE ATTACKS IN ADHOC NETWORKS

G.JYOSHNA, K.YOGA PRASAD

***Abstract*— For the removal of byzantine attacks in adhoc networks and proposed in SMT protocol for secure data communication. To increase the security of data transmission of mobile adhoc networks [MANETS] is presented in this work. There is a massive increase in using MANETS for unmanned army system for both surveillance and future combat operations. An SMT protocol provides a way to secure message transmission by dispersing the message among several paths with minimal redundancy. Security and reliability are crucial aspects of MANET, especially in security sensitive applications like military. Secure Message Transmission SMT protocol secure the data transmission phase by tailoring an end-to-end secure data forwarding protocol to the MANET communication requirements and increases the reliability through transmitting the messages in multiple paths with minimal redundancy. This work increases the through the removal of Byzantine Faults in the multiple paths. A binary search probing technique which is resilient to Byzantine failures caused by individual or colluding nodes is incorporated in the SMT protocol to provide more secured transmission**.

***Index Term;* Mobile Ad Hoc Networks; Military; Byzantine Faults; Secure Transmission; SMT- Secure Message Transmission;**

I. INTRODUCTION

Mobile ad hoc networks are advantageous in situations where there are no network infrastructures available and when there is a need for people to communicate using mobile devices. Since MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data.

The intrinsic nature of wireless ad hoc networks makes them very vulnerable to attacks ranging from passive eavesdropping to active interference. However, most of the existing key management schemes are not feasible in ad hoc networks because public key infrastructures with a centralized certification authority are hard to deploy . However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory .

Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into external attacks and internal one. External attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network hence it is difficult to identify them.

Instead of transmitting in single path, the message will be transmitted in multiple paths to ensure reliability. It provides security based on the security association between the end nodes. It is not able to overcome the compromised nodes attacks..

Manuscript received May,2012

***G.JYOSHNA** E.C.E jntu/ sitams/ . india,*

***K.YOGA PRASAD**, ECE jntu/ sitams/ india,*

II. SECURE MESSAGE TRANSMISSION AND BYZANTINE ATTACKS

A. Secured Route Discovery by SMT

Secured routes are provided by establishing an End-to-End security association between the source and the destination. This scheme won't consider the intermediate nodes that may exhibit arbitrary and malicious behavior. The source node S and destination node T negotiate a shared secret key- $K_{S,T}$ with the knowledge of each other's public key. A pair of identifiers - query sequence number and query identifier is generated and used for the construction of the route request packet. The identifiers along with source and destination and $K_{S,T}$ are used for the calculation of Message Authentication Code (MAC). The identities of the traversed intermediate nodes are added in the route request packet. The route request is denoted as a list $\{Q_{S,T}: n_1, n_2 \ldots n_k\}$.The route reply is denoted as a list $\{R_{S,T} : n_1, n_2 \ldots n_k\}$.

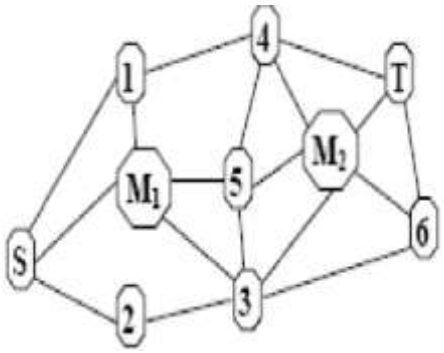

Figure 1.Sample Topology with two malicious nodes M1, M2

Scenario 1: Consider the case that when *M1* receives*{QS,T;S}*, it attempts to mislead *S* by generating *{RS,T;S,M1,T}*. Not only would *S* accept such a reply, if a regular routing protocol were used, but it would most probably choose this fake route, since *{S,M1,T}* would have fewer hops than any other legitimate reply. It would also be received with the least delay, because of the close distance between *M1* and *S*.

Scenario 2: Consider the case in which *M1* discards request packets arriving from its neighbors, excluding the one from node *1*. This type of malicious act cannot be countered, but the controlled flooding of the query packets provides the required robustness. By discarding route request packets, a malicious node partially narrows the topology view of *S* and, to some extend, impedes the network operation. In essence, the malicious node can always hide its incident links, but at the same time it practically removes itself from *S*'s view.

Scenario 3: As assumed above, *M1* sees and appropriately relays *{QS,T;S,1,M1}*; upon arrival of *{QS,T;S,1,M1,5,4}* at *T*, the reply is generated and routed over the reverse path. When *M1* receives *{RS,T;S,1,M1,5,4,T}*, it tampers with its content and relays *{RS,T;S,1,M1,Y,T}*, with *Y* being any invented sequence of nodes. *S* readily discards the reply, due to the integrity protection provided by the *MAC*.

Scenario 4: When *M2* receives *{QS,T;S,2,3}*, it corrupts the accumulated route and relays *{QS,T;S,X,3,M2}* to its neighbors, where *X* is a false, invented *IP* address (or, any sequence of *IP* addresses). This request arrives at *T*, which constructs the reply and routes it over *{T,M2,3,X,S}* towards *S*. When node *3* receives the reply, it cannot forward it any further, since *X* is not its neighbor, and the reply is dropped

Scenario 5: In order to consume network resources, *M1* replays route requests, which are discarded by intermediate nodes, since they maintain a list of query identifiers seen in the past. This is achieved by the underlying routing protocol itself, within the limitations imposed by the size of the query table. But queries replayed after a significant period of time, will propagate across the network and arrive at *T*. The *query sequence number*, used only by the end nodes for the query identification, allows *T* to discard such queries. If the request header were corrupted, the query would also be discarded. Similarly, *T* discards fabricated route requests, since malicious nodes cannot generate valid request *MAC*.

Scenario 6: Assume that *M1*, after observing a few route requests originating from *S*, fabricates several queries with the subsequent query identifiers. The goal of this attack is to make intermediate nodes store these identifiers and discard legitimate, future *{QS,T;n1,…,nj}* route requests. The cost of this attack is low (a single route request transmission per identifier) and, with the *Time-To-Live (TTL)* field of the query packet set to a high value, the affected network area may be significantly large

SECURE MESSAGE TRANSMISSION:

The SMT protocol [1] safeguards pair wise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior. The
scheme presented in this paper guarantee that a Byzantine fault will be identified and the fault link can be avoided in the data transmission phase. The current topological information will be gathered based on the network behavior such as transmission time, probability of lost packets and acknowledged packets. Based on the information gathered, the route metrics are updated and used in selecting the multiple paths [4]. In this way the reliability of the secured data transmission can be enhanced.

DATA TRANSMISSION IN MANETS:

In any type of manets ,reliable of information to the integrated destination is of major interest to users sending information across that network. The information on the network might not be delivered to the destination as it is network might not be delivered to the destination as it is disrupted by the system because of many reasons. These reasons can be grouped into two categories, network faults and security attacks. In the former, main problem is to detect abnormal changes in the network and categorize them. Security attacks can be protected and authenticated by cryptography.

However, cryptographic protection cannot be effective against network layer attacks especially like Byzantine attacksA compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packets on non optimal paths and selectively dropping packets are referred to as Byzantine attacks . Byzantine failures are hard to detect. The network would seem to be operating normally in the viewpoint of nodes, though it may actually be exhibiting Byzantine behavior .

Byzantine Attacks

Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and routing loops, carries out attacks such as creating routing packets on non optimal paths, and selectively dropping packets as in . This module provides the capability to simulate the black hole, Byzantine wormhole, and Byzantine overlay network wormhole attacks without modifying the routing protocol. It was not possible to simulate the flood rushing attack using this technique because it requires timing changes in the routing protocol code. Because this attack simulation module is potentially useful to the secure routing community, we make it publicly available below.

The modified LL has several commands that allow it to be configured from the simulation TCL setup script. The first command enables the black hole attack, which is executed by checking the packet type of any packet sent down by the routing agent, and silently dropping any packet which has an application data type (as opposed to a routing protocol type). The second command is used to setup the various wormhole configurations, and creates a back channel connection from one node to another *wormhole peer* node.

The attack module manages any number of these wormhole peer connections, thus allowing the setup TCL script to create either a simple point to point wormhole or the more complicated overlay network wormhole. If the next hop address of a uncast packet matches a wormhole peer address, the packet is sent directly to that peer. Otherwise, it is sent down the stack normally.

The various Byzantine attacks are listed down .

1)Black Hole Attack: It is the basic Byzantine Attack where the adversaries stop forwarding the data packets but still participates in the routing protocol correctly. As a result, whenever the adversarial node is selected as part of a path by the routing protocol, it prevents communication on that path from taking place.

In this attack ,a malicious node falsely advertise good paths (e.g., shortest path or stable path)to the destination node during the path finding process(in on-demand routing protocols0or in the route update messages. the intention of the malicious node could be to hinder the path finding process or to intercept all data packets being sent to the destination node concerned.

AODV PROTOCOL:

Adhoc on demand distance vector(AODV) routing protocol uses an on –demand approach for finding routes ,that is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path..the major difference between AODV and DSR stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed .however ,in AODV ,the source node floods the route request packet in the network when a route is not available for the desired destination. it may obtain multiple routes to different destination from a single destination. it may obtain multiple routes to different destination from a single

2)Flood Rushing Attack: If the adversaries reach some of its neighbours with its version of the flood packet before they receive a version through a legitimate route, then those nodes will ignore the legitimate version and forwards the adversarial version. This may

result in continual inability to establish an adversarial free route even if authentication mechanisms are used.

***3)Byzantine Worm Hole Attack*:** It is a more effective attack .The adversaries collude with each other and establish tunnel (worm hole) between them. The adversaries can use the low cost appearance of the wormhole links in order to increase the probability of being selected as part of the route, and then attempt to disrupt the network by dropping all of the data packets. The Byzantine wormhole attack is an extremely strong attack that can be performed even if only two nodes have been compromised. This allows the adversary to perform a more effective attack. Indeed, one such attack is a Byzantine wormhole, where two adversaries collude by tunneling packets between each other in order to create a wormhole in the network .

4) ***Byzantine Overlay Network Worm Hole Attack*:** A more general variant of the previous attack occurs when several nodes are compromised and form an overlay network. By tunneling packets through the overlay network, the adversaries make it appear to the routing protocol that they are all neighbors, which considerably increases their chances of being selected on routes. This is the strongest attack considered in this work. By forming an overlay network they will attack the network severely.

IMPROVING SECURITY, RELIABILITY AND DELAY

A. Overview

The work presented has two main phases:

1) Phase I *– Enhancing Security and Reliability::*Increasing the Security and Reliability of the message communication in MANETs. This phase is mostly needful for security sensitive applications like military. The security of the data transmission can be increased by selecting most secured routes in Active Path Set (APS).To improve the performance of the secured message transmission, most secured paths against Byzantine attacks are selected and included in Active Path Set. The overall view of Phase I is given in Figure 3. The reliability is also increased by dropping out only the links in the faulty path and not the whole path..

By selecting secured multiple paths with the removal of faulty links only and not the entire path, the reliability is enhanced and congestion gets reduced. Adaptive probe signals are used to find out the Byzantine Faults. Threshold is set based on the normal behaviour of the network. When the loss rate exceeds the threshold, probing will start to find the adversaries. The paths from source to destination are then rated and the most trusted ones are selected for further communication.

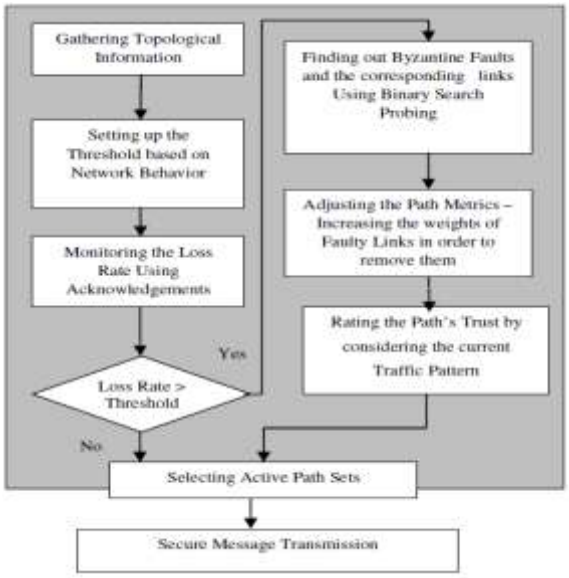

Figure 3: Overall Architecture of Phase I – Enhancing Security and Reliability

2) Phase II – Reducing Delay and Delay Variance:

Reducing the delay and delay variance by predicting the nodes behavior and location using knowledge mining techniques especially Spatial and Temporal mining. As the Army continues to evolve to a completely digital battlespace environment, particularly as found in the Future Combat Systems effort, the ability to gather and form useful information in this dynamic environment is becoming problematic..These two factors significantly reduce gaining useful knowledge from the networks .Further, processing speed will be of the essence as non-static analytics will require at or near real-time processing speeds in proxim*ity to the battlespace.*

B. Byzantine Fault Detection

The detection scheme is based on using acknowledgements of the data packets. The destination has to return an acknowledgement to the source for every successfully received data packet. Timeouts are set for receiving the valid acknowledgements. The delay in receipt may be due to either malicious or non malicious causes. A threshold is set to a tolerable loss rate. A fault is defined as a loss rate greater than or equal to the threshold. The source keeps track of the number of recent losses. If the number of recent losses is greater than the acceptable threshold then a fault is registered and a binary search starts between the source and the destination in order to find the faulty link.

The source controls the search by specifying a list of intermediate nodes on data packets. This scheme is able to detect all types of Byzantine attacks including network overlay attacks. Shared keys are used between the source and the probed nodes .

C. Binary Search Probing

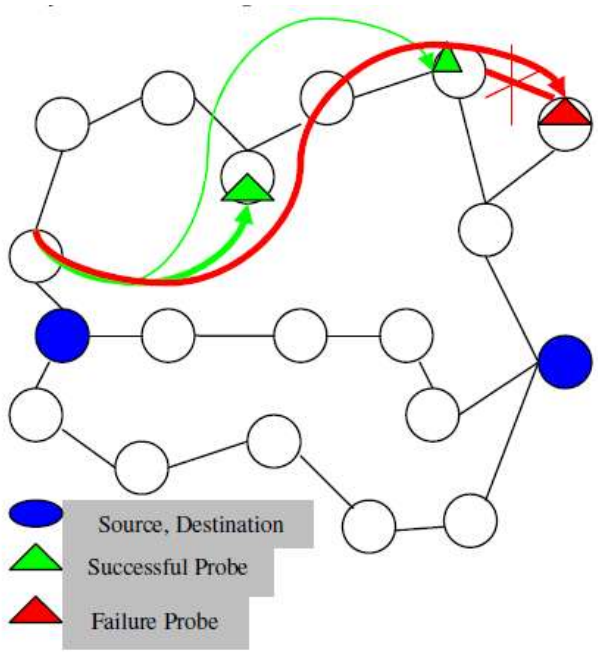

Fig. 4 Binary Search Probing for Finding Fault Links

The list of probes defines a set of non overlapping intervals that covers the whole path where each interval covers the sub path between the consecutive probes that forms its end points as in Fig 4. When a fault is detected on an interval, the interval will be divided into two by inserting a new probe. This new probe is added to the list of probes appended to future packets.

The process of subdivision continues until a fault is detected on the interval that corresponds to a single link. This result in finding log n faults where n is the length of the path.

D. Calculating the path metric

After a sender and a receiver start to exchange data packets, they build tables to keep traffic patterns. There is one table built by the sender and another one built by the receiver. The two tables have the same structure. Each table is composed of two fields: Packet identification number and time of action. Each time a packet is sent, the sender records the packet ID and the time. Each time a packet is received a receiver records the packet ID and the time.

Every five (or t) seconds based on network environment, the receiver sends the sender a table. Upon receipt of the table from the receiver, the sender merges it with its own table into an anomaly detection table.

1) ***Trip Time Variation:*** Trip time of each packet is the time a packet spends on the way, starting when it is transmitted, ending when it is received. That time is calculated using the sender's time stamp when a packet was sent and recipient's time stamps when a packet was received.

2) ***Change of packets frequency:*** *The* sender compares both the frequency at which packets were sent and the frequency at which packets were received, measured in packets per second. By comparing the two frequencies, delays of packets can be noticed.

3) Link Failures: Upon finding the link failure using binary search probes, all the paths containing that link will be discarded by decreasing the level of trust by half.

E. Trust Updation and Path Set Selection :

An intial value is assigned to the value of trust related to a path.a threshold is based on expected behavior of the networks environment.based on the observation the paths metrics are updated and are used as aparameter**.**

RESULTS AND PERFOMANCE EVALUATION

A. simulated implementation

Simulations were conducted using the NS2 network simulator. Nodes in the network were configured to use 802.11 radios with a bandwidth of 2 Mbps and a nominal range of 250 m. In order to simulate most of the proposed Byzantine attacks in NS2, a protocol independent Byzantine attack simulation module was developed. This module provides the capability to simulate the black hole, Byzantine wormhole, and Byzantine overlay network wormhole attacks without modifying the routing protocol.

For the purpose of performance analysis, NAM trace files are written and graphs are plotted using XGRAPH. The simulator can produce both the visualization trace (Nam) as well as an ASCII file trace corresponding to the events registered at the network. In the trace file the number of packets sent, received and lost is noted down. Graphs are drawn to compare the performance of the existing system with that of proposed one.

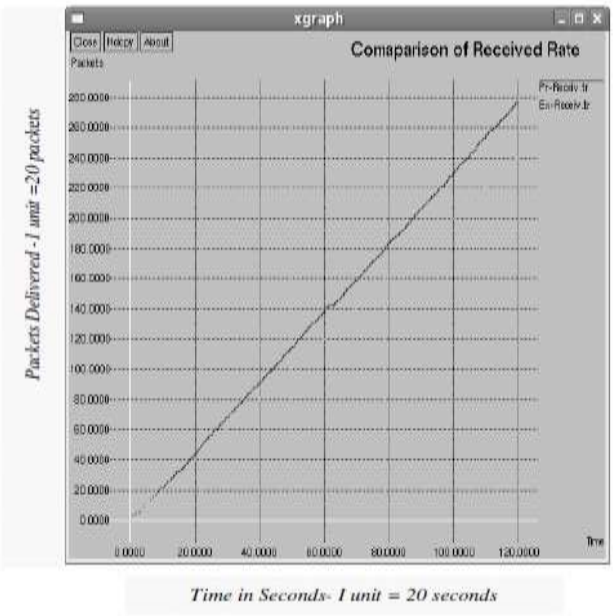

Figure 5. Comparison of Packets Received

B. Performance Evaluation

The Green line in Figure 5 shows the received rate of packets in multipath message transmission without any detection and removal of Byzantine Faults. The Red line in Figure 5 represents the received rate of packets of the proposed system after the removal of Byzantine attacked links. It shows a clear and constant increase in the throughput because of the removal of Byzantine Faulty links. Similarly comparative graphs are drawn for lost packets, delivery ratio and throughput. Delay is increased because of the additional overhead in probing.

This scheme is able to find out the faulty links within log n time where n is the length (number of nodes) of the path. Proposed scheme is effective in situations where reliability and security is most wanted in situations like MANET in military as suggested by recent research carried out in MANETS in Military Communications .

V.CONCLUSION AND FUTUREWORK

In this proposed system, a fixed threshold is used to identify the faults. Instead of fixed threshold, varying threshold considering dynamic changing networks can be set. The system can be compared with any of the multipath routing protocols like that given in . The additional delay due to probing might be reduced if the location of nodes after mobility especially destination node and adversaries can be predicted. This knowledge about nodes future location and behavior will be helpful in military applications and also in pervasive computing where mobile ad hoc networks plays a major role. Also this work with little variations along with service oriented architecture can be adapted for providing privacy and trust in pervasive computing.

REFERNCES:

[1] Papadimitratos, P. Haas, Z.J , "Secure data communication in mobile adhoc networks" , This paper appears in: Selected Areas in Communications, IEEE Journal on Publication Date: Feb. 2006,Volume: 24, Issue: 2,On page(s): 343- 356.

[2] Reza Curtmola Cristina Nita-Rotaru, " BSMR: Byzantine-Resilient Secure Multicast Routing in Multichip Wireless Networks" , IEEE Transactions on Mobile Computing, vol. 8 Issue. 4,pp. 445 - 459,February 2009.

[3] A.Tsirigos and Z.J.Hass (2004) , "Analysis of mulitipath routing, Part 1: The effects on the packet delivery ratio"IEEE Transactions on Wireless Communication., vol.3, no.2,pp:500-511

[4] Banner, R. Orda, A , "Multipath Routing Algorithms forCongestion Minimization". This paper appears in: Networking, IEEE/ACM Transactions on Publication Date: April 2007 Volume: 15, Issue: 2,On page(s): 413-424.

[5] P.Papadimitratos and Z.J.Hass, " Secure Routing For Mobile Ad Hoc Networks", in proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS-2002).

[6] Papadimitratos, P. Haas, Z.J and E.G.Sirer , " Path set selection in mobile ad hoc Networks" ,in Proc 3rd ACM MobiHoc , Lausanne, Switzerland, Jun 2002 ,pp 1-11.

[7] C.Siva Ram Murthy and B.S Manoj.,(2004), "Ad Hoc Wireless Networks- Architecutres and Protocols" , Pearson Education.

[8] L.Lamport, R.Shostak, M.Pease ," The Byzantine Generals Problem",ACM Tran.Program. Languages, Vol.4, no.3 ,pp -382-401, July 1982.

[9] Patwardhan, A.; Parker, J.; Joshi, A.; Iorga, M.; Karygiannis, T ,"Secure Routing and Intrusion Detection in Ad Hoc Networks",Pervasive Computing and Communications,PerCom 2005. Third IEEE International Conference, 8-12March 2005 Page(s):191 – 199

[10] Sebastien Berton, Hao Yin, Chuang Lin, Geyong Min,(2006) "Secure, Disjoint, Multipath Source Routing Protocol(SDMSR) for Mobile Ad-Hoc Networks,", Proc of the Fifth International Conference on Grid and Cooperative Computing (GCC'06), pp.387-394.

[11] Yu Liu,Yang Li and Hong Man(2007) "A hybrid data mining anomaly detection technique in ad hoc networks "International Journal on Wireless and Mobile Computing.

[12] Jun Peng, Biplab Sikdar and Liang Cheng(2009) "Multicasting with Localized Control in Wireless Ad Hoc Networks" IEEETransaction on Mobile Computing.

[13] Banner R. and Orda A.(2007)" Multipath Routing Algorithms for Congestion Minimization", IEEE/ACM journal onNetworking .

[14] Zhu Wei; Liu Ningning; Shan Weifeng; Fu Guobin ,"Design of the Next Generation Military Network Management System Based on NETCONF"- Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference Issue, 7-9 April 2008 Page(s):1216, 2008.

[15] Finds Frost & Sullivan ,"Advances in Radio Communications and Wireless Networking Fuel Innovations in MANETs", MANETs in Military Communications - Strategic Insights and the Road Ahead, Date of Published -11th March 2010.

[16] Jaydip Sen and Harihara Subramanyam , " An Efficien Certificate Authority for Ad Hoc Networks", on Distrbuted Compting and Internet Technology of SpringerLink- Lecture Notes in Computer Science, 2007, Volume 4882/2007, 97-109, DOI: 10.1007/978-3-540-77115-9_10

[17] Robert Castaneda and Samir R.Das, " Query Localization Techniques for On _Demand Routing Protocols in Ad Hoc Networks ",in ACM /IEEE International Conference on Mobile Computing and Networking(Mobicom) ,August 1999.

[18] LLias Michalarias,Christian Becker , " Multidimentional Querying in Wireless Ad Hoc Networks", ACM 2007, pages529-530.

[19] Takahiro Hara,Sanjay K.Madria, " Data Replicaiton for Improving Accessibility in Ad Hoc Networks" ,IEEE Transactions on Mobile Computing ,vol.5, No.11, November 2005 ,On Pages:1515 -1532.

[20] Dipankar Deb , Srijita Barman Roy, and Nabendu Chaki, "LACBER: A New Location Aideded Routing Protocol for GPS scarce MANET", in International Journal of Wireless & Mobile Networks (IJWMN), Vol 1, No 1, August 2009 on pages:22-37