ISSN:2231-0711

Secured Communication for MANETS in Military

N.Angayarkanni , P. Palaniyammal

Department of Electronics and Communication Engineering,
PGP College of Engineering &Technology
Namakkal-637207, India
angaipgpece@gmail.com

***Abstract*— A new way to increase the security of data transmission of mobile ad hoc 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. This has necessitated the development of innovative MANET solutions catering to the reliability, security and scalability needs of the defense communications environment. Security and reliability are crucial aspects of MANET, especially in security sensitive applications like military. Secure Message Transmission SMT[1] 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. The fault detection algorithm bounds logarithmically (log n –n the number of nodes in the path), so the delay is reduced drastically. The simulated implementation of the work in NS2 shows the marginal increase in the throughput. The delay and jitter variants can also be improved if the nodes location can be predicted. Predicting the nodes location and reducing the unnecessary traffic with the aid of Spatial and Temporal mining is the second phase of this work.**

Keywords- Mobile Ad Hoc Networks; Military; Byzantine Faults; Secure Transmission; SMT- Secure Message Transmission; Multipath Message Transmission, Binary Search Probing; Reliability; Spatial and Temporal Mining, Location Prediction.

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. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. The intrinsic nature of wireless ad hoc networks makes them very vulnerable to attacks ranging from passive eavesdropping to active interference. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies. 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[16],[7].Consequently mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network

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 [7].

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. Lot of works [1], [5], [9], [10] had been done in the area of identifying and removal of adversaries in the network. The SMT protocol [5] safeguards pair wise communication across an unknown frequently changing network, possibly in the presence of adversaries that may exhibit arbitrary behavior.

Instead of transmitting in single path, the message will be transmitted in multiple paths to ensure reliability. Considering the benefits over the overhead involved in utilizing the multiple paths are increased security, reliability and reduced congestion [4] that is mostly needed for MANETs in military.SMT protocol provides security based on the security association between the end nodes. It is not able to overcome the compromised nodes attacks. The work presented in this paper has two phases. The first phase is to improve the security and reliability of data transmission in mobile ad hoc networks by providing secured routes. The Byzantine faults are identified and those links will 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 correctly received –

acknowledged packets and a threshold is set which is used in binary search probing.

Based on the information gathered the route metrics are updated and used in selecting the multiple paths [3], [6]. The second phase is involved in predicting nodes location and behavior based on its past performance behavior [11], [12], [18]. A number of efforts [20], [21], [22] leverage the global positioning system (GPS) to reduce the search space. The nodes may exchange the current velocity vectors such as speed and direction to predict the location of the nodes. The spatial and temporal mining can be used to find the relative appropriateness of the location.

II.SECURE MESSAGE TRANSMISSION AND BYZANTINE ATTACKS

II.1. 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 …n_k}.The route reply is denoted as a list {$R_{S,\ T}$: n_1, n2 …n_k}.

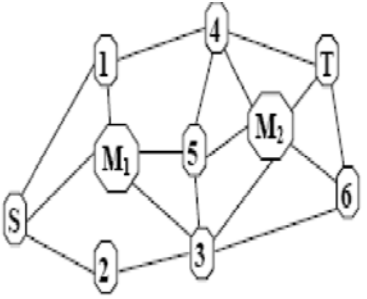

Fig 1: Sample Topology with two malicious nodes M1, M2

II.2. SECURITY PROVIDED BY SMT UNDER VARIOUS ATTACKS

1)*Fake Reply:* If M1 receives the request by S and reply a fake route to S, that false reply will be discarded by the source since M1 doesn’t know $K_{S,T}$ and not able to produce a valid MAC.

2) *Tampering Route Reply:* If the malicious nodes M1 or M2 changes the route reply send by T, S will discard it as the modified reply won’t integrate with the expected MAC of T.

3) *Resource Consumption Attack:* If the adversaries want to exhaust the network resources then they will replay the requests. On receiving the replayed requests, the nodes will drop the requests based on query identifiers.

4) *Fabricated Route Requests:* Malicious nodes after observing for some time the requests generated by source, it will fabricate several queries with subsequent query identifiers. The goal is the intermediate nodes will store this numbers and drop out the legitimate requests sent by the source. This type of attack can not be prevented by SMT.

5) *Spoofing Attack:* The nodes M1 and M2 may spoof an IP address and participate in the route requests. This attack can not be identified and they can hide their location by masking.

6) *Colluding nodes Attack:* If the nodes colluded during both the request and reply phase, the source will accept the false route information. For example in Fig1., M1 tunnels the route request to M2.M2 will broadcast the route request with route segment between M1 and M2 falsified. In the reverse direction ,T will consider this path and send the route reply back to the source through M2.Reply is reverse tunneled by M2 to M1.By this a false path will be included between S and T.

II.3. SECURED DATA COMMUNICATION OF SMT

1)Active Path Sets(APS) and Message Transmission: A set of active diverse, nde disjoint multiple paths are selected by applying secured route discovery protocol. The set of paths used for current data transmission are known as Active Path Sets as shown in Fig 3.The message is dispersed based on Robin's algorithm [23] and is transmitted in multiple paths by dispersing it into pieces and after encoding. Redundancy ensures successful reconstruction f data even if some loss occurs due to malicious nodes or breakage of routes.

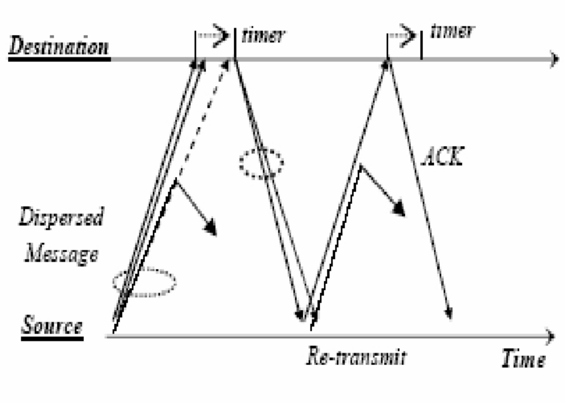

Fig 2: Message Dispersion in SMT

2) *Robust Feedback Mechanism:* Each dispersed piece is transmitted in different route and carries a Message Authentication Code and by that the integrity of the message and authenticity of the source is verified. After validation, the destination acknowledges every successful receipt. The feedback mechanism is also cryptographically protected and dispersed.

3) *APS Adaptation:* Successful receipt of ACKS

indicates operational routes while missing ACK implies that the route is either broken or compromised. The paths are rated based on short term and long term rating. The routes are selected or discarded based on their rates.

II.4. BYZANTINE ATTACKS

Here, a 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 as in [9]. 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 [7], [8]. As discussed above, SMT is able to avoid only the rooting loops attacks caused by colluding nodes. The various Byzantine attacks are listed down [7].

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.

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.

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.

III.IMPROVING SECURITY, RELIABILITY AND DELAY

III.1 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.

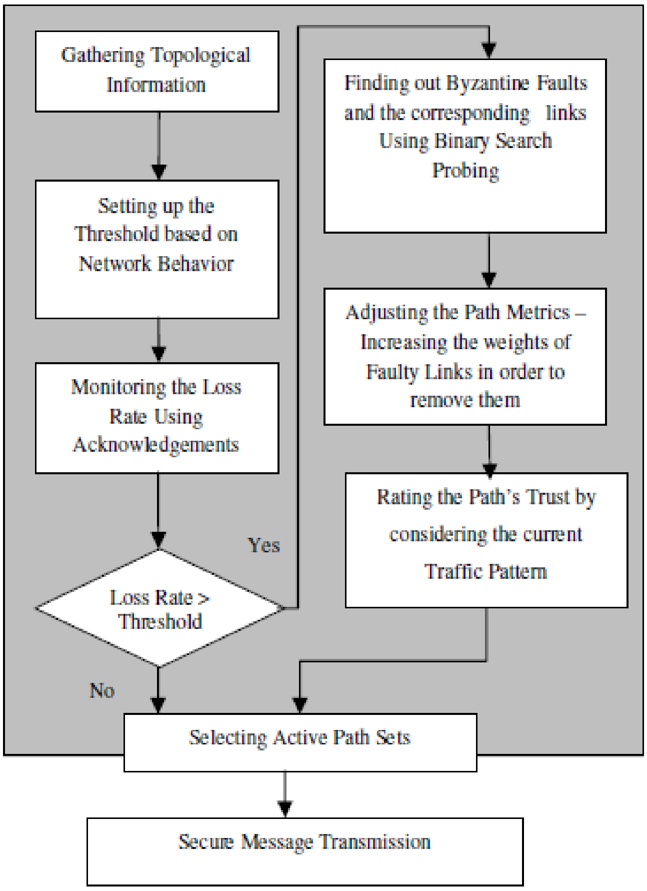
Gathering Topological Information
Setting up the Threshold based on Network Behavior
Monitoring the Loss Rate Using Acknowledgements
Loss Rate > Threshold
Yes
No
Finding out Byzantine Faults and the corresponding links Using Binary Search Probing
Adjusting the Path Metrics – Increasing the weights of Faulty Links in order to remove them
Rating the Path's Trust by considering the current Traffic Pattern
Selecting Active Path Sets
Secure Message Transmission

Fig 3: Over all 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 battle space 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. In battlefield or in border force any number of nodes may join or leave the network and there will be a rapid movement also. These two factors significantly reduce gaining useful knowledge from the network. Further, processing speed will be of the essence as non-static analytics will require at or near real-time processing speeds in proximity to the battle space. An efficient algorithm which predicts the nodes movement in dynamic environment with near proximity is needed.

III.2 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. Each node in the list in addition to the destination must send an acknowledgement to the source. The list of nodes those have to send acknowledgements are known as probe nodes. Since the list of probed nodes is specified on legitimate traffic, an adversary is unable to drop traffic without also dropping the list of probed nodes and finally being detected. 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 .This can be done by on demand Diffie-Hellmann key exchange algorithm. This key mechanism can be integrated into the route discovery protocol.

III.3 BINARY SEARCHING PROBING

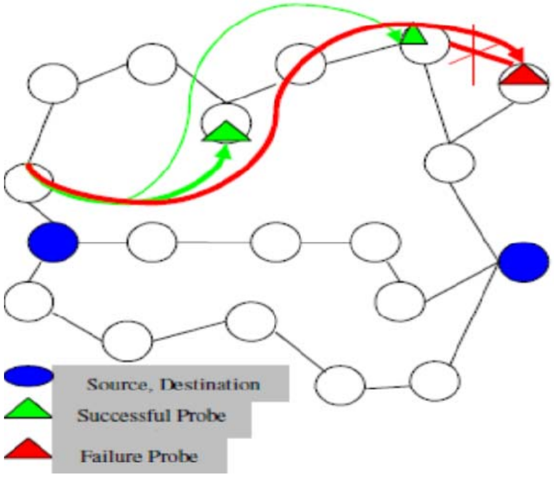

Fig.4: Binary search probing for finding faulty links

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.

III.4 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. The anomaly detection table contains packet identification, sending timestamp and receiving timestamp for each packet. Obviously, the sender gets the table refreshed every 5(or t) seconds. Using this information the sender can calculate the various values that will be mentioned in the following subsections and keep them in respective variables is received a receiver records the packet ID and the time.

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.

III.5 TRUST UPDATION AND PATH SET SELECTION

An initial value is assigned to the variable of trust related to a path. A threshold is set based on expected behavior of the network environment [6]. Based on the observation the paths metrics are updated and are used as a parameter while selecting the active path set.

IV.RESULTS AND PERFORMANCE EVALUATION

IV.1 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. It was not possible to simulate the flood rushing attack using this technique because it requires timing changes in the routing protocol code. The module is implemented as part of the NS2 Link Layer (LL) object which lies directly below the Routing Agent and directly above the MAC layer.

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. The throughput, packet delivery ratio, average end-to-end delay and total dropped packets are calculated based on the parameters from the trace file.

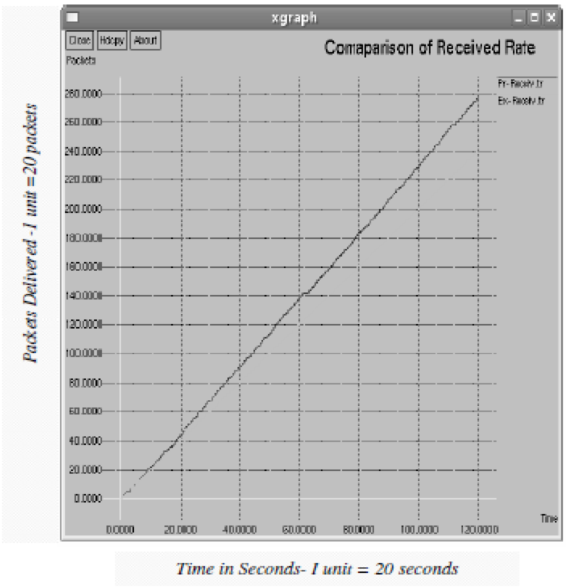

Fig 5: Comparison of packets received

IV.2 PERFORMANCE EVALUATION

The Green line in Figure 4 shows the received rate of packets in multipath message transmission without any detection and removal of Byzantine Faults. The Red line in fig 4 shows the received rate of packet soft he 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. The simulated result shows a 16% improvement over the existing system. 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. The highly successful delivery of message with the ability to disperse and avoidance of faulty links is more secured and reliable than ordinary secured data transmission mechanism. 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 [15].

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 [10]. 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 [24] and trust in pervasive computing.

VI.REFERNCES

[1] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure data communication in mobile adhoc networks", IEEE Journal on Selected Areas in Communications, Vol. 24, Issue. 2, pp: 343- 356, February 2006.

[2] Reza Curtmola and Cristina Nita-Rotaru , "BSMR: Byzantine-Resilient Secure Multicast Routing in Multihop Wireless Networks", IEEE Transactions on Mobile Computing, vol. 8, Issue. 04, pp: 445 - 459, February 2009.

[3] Hamid Reza Barzegar,, AbdolMajid Shahgholi and G.Praveen babu, "Secured Message Communication for Disaster Planning in Mobile Ad-Hoc Networks",International Journal of Scientific Research in Computer Science Applications and Management Studies vol.1Issue .o2, pp: 500-511, September 2012.

[4] R.Banner and A. Orda, "Multipath Routing Algorithms for Congestion Minimization". International journal of . Advanced Networking and Applications, Vol.03, Issue. 04, pp: 1292-1297, April 2012.

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

[6] Panagiotis Papadimitratos, Zygmunt J. Haas and E.G.Sirer , " Path Selection in mobile ad hoc Networks" ,in Proc MobiHoc, Lausanne, Switzerland, pp 1-11 ,Jun 2002.

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

[8] *L. Lamport, R. Shostak, and M. Pease,* "The Byzantine Generals Problem",SRI International *ACM* Transactions on Programming Languages and Systems, pp: 382-401, July 1982

[9]A. Patwardhan, J.Parker, A.Joshi M. Iorga T.Karygiannis "Secure Routing and Intrusion Detection in Ad Hoc Networks",Pervasive Computing and Communications, Third IEEE International

Conference, pp.191 –199. , 8-12 March 2005.

[10] Sebastien Berton, Hao Yin, Chuang Lin and Geyong Min, "Secure,Disjoint, Multipath SourceRouting Protocol(SDMSR) for Mobile Ad-Hoc Networks", Proc of Fifth International Conference Grid and Cooperative Computing, pp: 387 -394 ,21-26,Oct 2006.

[11]Yu Liu,Yang Li and Hong Man "A hybrid data mining anomaly detection technique in ad hoc networks ",International Journal of Wireless and Mobile Computing, Vol.2. Issue. 1, pp:37-46, May 2007 . [12]Jun Peng, Biplab Sikdar and Liang Cheng "Multicasting with Localized Control in Wireless Ad Hoc Networks" IEEE Transaction on Mobile Computing, vol. 8, Issue. 1, pp. 52-64, January 2009

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

[14] 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,Vol. 4882,pp:, 97-109, 2007.

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

[16] Llias Michalarias and Christian Becker ," Multi dimensional Querying in Wireless Ad Hoc Networks", In proceeding of: Proceedings of the 2007 ACM Symposium on Applied Computing (SAC), Seoul, Korea, March 11-15, 2007

[17] Takahiro Hara and Sanjay K.Madria, "Data Replicaiton for Improving Accessibility in Ad Hoc Networks", IEEE Transactions on Mobile Computing , vol.5, Issue.11, pp: 1515 – 1532, November 2006

[18] Dipankar Deb , Srijita Barman Roy, and Nabendu Chaki, "LACBER: A New Location Aideded Routing Protocol for GPS scarce MANET", International Journal of Wireless & Mobile Networks (IJWMN), Vol. 1, Issue. 1, pp: 22-37, August 2009.

[19]Young-Bae Ko and Nitin H. Vaidya "Location-Aided Routing (LAR) in mobile ad hoc network",WirelessNetworks, vol .6, pp. 307-321, 2000.

[20] Hung-Chi Chu, Rong-Hong Jan, "A GPS-less outdoor, self-positioning method for wireless sensor networks", Ad Hoc Networks, Elsevier Science, Vol. 5, Issue 5, pp.547-557, 2007.

[21] Michael O.Rabin "Efficient dispersal of information for security, load balancing, and fault tolerance" Journal of the ACM (JACM), Journal of ACM (JACM), Vol.36, Issue.1, PP-335-348, April 1989.

[22] Alastair R.Beresford and Frank Stajano, "Location Privacy in Pervasive Computing ", Journal of IEEE Pervasive Computing, Vol. 2 ,Issue. 1, pp: 46-55, January 2003