Security in MANET using ACO

Shabnam Kumari[1], Neetu Sharma[2], Reema[3]
[1, 2, 3] Department of CSE
[1, 2, 3] Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India

Abstract- *MANET is a self-configuring infrastructureless network of mobile devices connected by wireless. Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. This paper presents an easy approach to the Ant Colony Algorithm, with appropriate vocabulary and global explanation, as well as details about its behavior with AODV protocol to detect the security attacks. Detection of Byzantine attacks using this algorithm is attempted and more adaptive values for threshold are to be explored.*

Keywords- MANET, ACO, AODV, Bynzatine Attack.

I. INTRODUCTION

1. MANET:

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals withwireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure [1]. MANET is a self-configuring infrastructurelessnetwork of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".

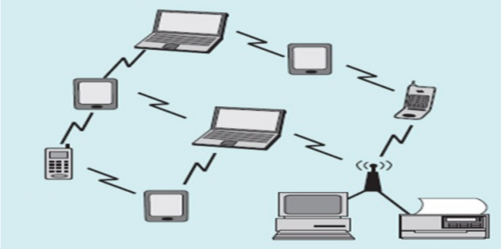


Figure 1. Mobile Ad Hoc Network (MANET).

The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc [2].

The MANET can be used in the applications such as rescue operations, tactical operations, environmental monitoring, conferences, connecting soldiers in battlefields and social or business application such as Public and Personal Area Networks [4]. The weaknesses of ad hoc networks are dynamic topology, lack of infrastructure, exposure of nodes and channels [5].

II. LITERATURE REVIEW

Vandana C. P (2013), studied on “Evaluation of Impact of Wormhole Attack on AODV”.[36]

Mobile Adhoc Networks (MANET) are self-organizing, decentralized networks and possess dynamic topology, which make them attractive for routing attacks. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. This author focuses on study of wormhole attack, its behavior and the performance impact of wormhole attack on AdhocOn Demand Distance Vector (AODV) routing protocol. The NS2 network simulator is used to evaluate the wormhole attack impact on AODV.

Thamilselvi C.P (2012) proposed “A Novel method to Detect Black Hole attack in MANET using Efficient ACO Strategy for SEAD Protocol”.[37]

It is highly essential to ensure security for data transmission. Number of such work is going on to ensure secure data transmission. Due to the high growth usage of mobile in this era, it is highly essential to make use of secure mechanism in mobile [37]. Author introduced an ant based novel approach reliability to detect anomalies. They used the strategy to fight against threats like Black hole attack using the fitness function generated from ACO (Ant Colony Optimization).Further it stops the fake route display generated from the malicious node which further declared as malicious node.

R.Gopinathan (2012) introduced "Efficient Secret Sharing Scheme for Mobile Ad Hoc Networks".[38]

In MANET, Black hole attacks may cause packet dropping, misrouting the information form source to destination. So the performance of the network is totally degraded. To overcome this issue, the authors proposed the modified proactive secret sharing scheme to ensure the data confidentiality, data integrity and authenticity.

Reshmi Maulikand Nabendu Chaki (2011) worked on "A Study on Wormhole Attacks in MANET".[40]

An Ad-hoc network is a self-organized network, without a central coordinator, and which frequently changes its topology. They had analyzed the performance of Mobile Ad-hoc Networks (MANET) under wormhole attack.

A. tiranuch, and W. Jie (2006) proposed "A survey on Intrusion Detection in Mobile Ad hoc Networks".[47]

A survey proposed by Tiranch A. et al [47] in ad hoc networks classified IDS in two categories viz. Standalone and Cooperative. Standalone IDS are those in which IDS agent runs on each node independently whereas in Cooperative IDS, a monitor agent observes the behaviour of neighbouring nodes and learn accordingly.

Baruch Awerbuchand Herbert Rubens (2004) introduced "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks".[48]

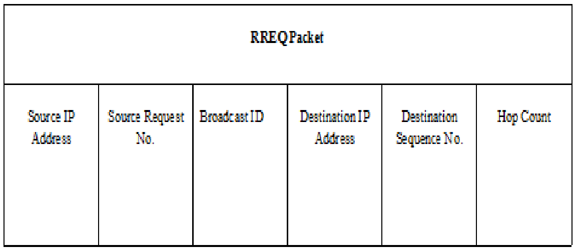
In this work, they presented a detailed description of several Byzantine attacks (black hole, flood rushing, wormhole and overlay network wormhole), analyse their mechanisms and describe the major mitigation techniques. Through simulation, perform a quantitative evaluation of the impact of these attacks on an insecure on-demand routing protocol. The relative strength of the attacks is analysed in terms of the magnitude of disruption caused per adversary.

III. PROPOSED WORK

1. ADHOC ON-DEMAND DISTANCE VECTOR PROTOCOL (AODV):

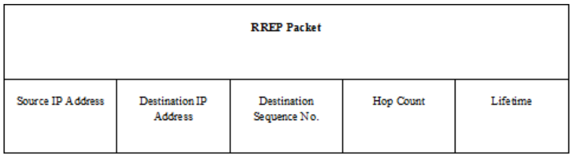
Ad hoc On-Demand Distance Vector (AODV) [49] is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deals with data transmission. This scenario decreases the memory overhead, minimize the use of network resources, and run well in high mobility situation. In AODV, the communication involves main three procedures, i.e. path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. The format of RREQ and RREP packets are shown in Table 1 and Table 2.

Table 1. RREQ Packet Format.



RREQ Packet					
Source IP Address	Source Request No.	Broadcast ID	Destination IP Address	Destination Sequence No.	Hop Count

Table 2. RREP Packet Format.



RREP Packet				
Source IP Address	Destination IP Address	Destination Sequence No.	Hop Count	Lifetime

When the source node wants to establish the communication with the destination node, it will issue the route discovery procedure. The source node broadcasts route request packets (RREQ) to all its accessible neighbors. The intermediate node that receive request (RREQ) will check the request. If the intermediate node is the destination, it will reply with a route reply message (RREP). If it is not the destination node, the request from the source will be forwarded to other neighbor nodes. Before forwarding the packet, each node will store the broadcast identifier and the previous node number from which the request came. Timer will be used by the intermediate nodes to delete the entry when no reply is received for the request. If there is a reply, intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from. The broadcast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same nodes.

The source node might get more than one reply, in which case it will determine later which message will be selected based on the hop counts. When a link breaks down, for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the link. It then creates a route error (RERR) message which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery if it still requires the route.

2. ANT COLONY OPTIMIZATION (ACO)

The main source of inspiration behind ACO is a behavior that is displayed by certain species of ants in nature during foraging. It has been observed that ants are able to find the shortest path between their nest and a food source. The only way that this difficult task can be realized is through the cooperation between the individuals in the colony. [50]

The key behind the colony level shortest path behavior is the use of pheromone. This is a volatile chemical substance that is secreted by the ants in order to influence the behavior of other ants and of it. Pheromone is not only used by ants to find shortest paths, but is in general an important tool that is used by many different species of ants.

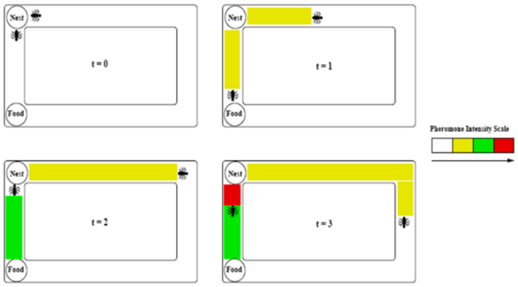


Figure 3. The Shortest Path Mechanism used by ants.

The different colours indicate increasing levels of pheromone intensity. From left to right and then from top to bottom, we see the situation in successive time steps.

1. Ant Colony Routing

The routing algorithms described so far have a flat organization and uniform structure: all the ants have the same characteristics and are at the same hierarchical level, while nodes are just seen as the repository of the data structures used by the ants. ACR defines the routing system as a distributed society of both static and mobile agents. The static agents, called node managers, are connected to the nodes and are involved in a continual process of adaptive learning of pheromone tables that is, of arrays of variables holding statistical estimates of the goodness of the different control actions locally available.[50] The control actions are expected to be issued on the basis of the application of stochastic decision policies relying on the local pheromone values. The mobile, ant-like agents play the role of either active perceptions or effectors for the static agents, and are generated proactively and on-demand. Node managers are expected to self-tune their internal parameters in order to adaptively regulate the generation and the characteristics of these subsidiary agents. In this way they are involved in two levels of learning activities. The active perceptions carry out exploratory tasks across the network and gather the collected non-local information back to the node managers. The effectors carry out ad hoc tasks, and base their actions on pre-compiled deterministic plans.

2. Why ant colony optimization algorithm suits to MANETs:

The simple ant colony optimization meta-heuristic shown illustrates different reasons why this kind of algorithms could perform well in mobile multi-hop ad hoc networks. We will discuss various reasons by considering important properties of mobile ad hoc networks [51].

a. Dynamic topology:

This property is responsible for the bad performance of several routing algorithms in mobile multi-hop ad hoc networks. The ant colony optimization meta-heuristic is based on agent systems and works with individual ants. This allows for a high adaptation to the current topology of the network.

b. Local work:

In contrast to other routing approaches, the ant colony optimization meta-heuristic is based only on local information; that is, no routing tables or other information blocks have to be transmitted to neighbors or to all nodes of the network.

c. Link quality:

It is possible to integrate the connection/link quality into the computation of the pheromone concentration, especially into the evaporation process. This will improve the decision process with respect to the link quality. It is here important to notice that the approach has to be modified so that nodes can also manipulate the pheromone concentration independent of the ants, that is, data packets. For this, a node has to monitor the link quality.

d. Support for multipath:

Each node has a routing table with entries for all its neighbors, which contains also the pheromone concentration. The decision rule, to select the next node, is based on the pheromone concentration on the current node, which is provided for each possible link. Thus, the approach supports multipath routing [51].

3. BYZANTINE ATTACK:

Many vulnerabilities are caused in network protocols (including wireless ad hoc routing protocols) by the lack of message integrity and authentication mechanisms, which allows an attacker to alter or fabricate packets. Significant research in securing ad hoc wireless routing protocols and wired routing protocols focused on this aspect. Authentication and integrity are required to protect a network protocol, since they ensure that a packet was generated by an authenticated node and has not been tampered with. However, they do not provide any guarantee about the legitimacy of actions taken by authenticated nodes.

Attacks where the adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system are referred to as Byzantine attacks. Research addressing this category of attacks is quite scarce. Below, we outline several Byzantine attacks that are considered in this work. All of them can be mounted against ad hoc wireless routing protocols.

Although many Byzantine attacks share certain features with the “selfish” node problem (e.g. not forwarding the data packets of others), the intentions of nodes under these two models are different. The goal of a selfish node is to reap the benefits of participating in the ad hoc network without having to expend its own resources in exchange. In contrast, the goal of a Byzantine node is to disrupt the communication of other nodes in the network, without regard to its own resource consumption [52].

A. Black Hole Attack:

A basic Byzantine attack is a black hole attack where the adversary stops forwarding 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. Most existing secure and insecure routing protocols are disrupted by black hole attacks because they render the normal methods of route maintenance useless.

B. Flood Rushing Attack:

A flood rushing attack exploits the flood duplicate suppression technique used by many routing protocols. This attack takes place during the propagation of a legitimate flood and can be seen as a “race” between the legitimate flood and the adversarial variant of it. If an adversary successfully reaches some of its neighbors with its own version of the flood packet before they receive a version through a legitimate route, then those nodes will ignore the legitimate version and will propagate the adversarial version. This may result in the continual inability to establish an adversarial-free route, even when authentication techniques are used.

C. Byzantine Wormhole Attack:

If more than one node is compromised, it is reasonable to assume that these nodes may interact in order to gain an additional advantage. 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 shortcut (or wormhole) in the network. This tunnel can be created either using a private communication channel, such as a pair of radios and directional antennas, or by using the existing ad hoc network infrastructure. The adversaries can send a route request and discover a route across the ad hoc network, then tunnel packets through the non-adversarial nodes to execute the attack. 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.

D. Byzantine Overlay Network Wormhole 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 [52].

4. WORKING OF BYZANTINE ATTACK:

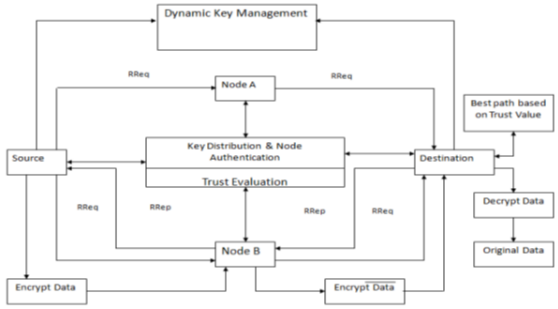


Figure 4. Structure of Byzantine Attack.

Byzantine attacks can be defined as attacks against routing protocols, in which two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services. First, how to detect and defend internal attacks against routing protocols, such as Byzantine attacks, has been a particularly challenging problem.

a. Byzantine Behavior to Attract Traffic:

In the presence of strong origin authentication mechanisms, malicious nodes can still misdirect traffic by sending false route information, i.e. they can exhibit Byzantine behaviour. In this case, a malicious node does not have to masquerade as another node. Instead, it can send control packets containing false routing information, using its own address. Alternatively, the node could modify control packets that it receives for forwarding. For example, the malicious node could advertise extra routes. To improve the likelihood of the false information being accepted by well-behaved nodes, the malicious node could falsely advertise favorable routing metrics to attract traffic. This is also known as the ‘black hole’ attack [14, 23, 49], by analogy to the celestial structure which sucks in all objects and matter. Possible Byzantine behaviour in proactive routing protocols includes the possibility of a malicious node:

- Advertising high willingness to forward control packets;
- Advertising false links in a Hello packet;
- Advertising false links in a topology control packet;
- Including itself in topology control packets it receives for forwarding, and
- Removing links from topology control packets.

b. Byzantine Behavior to Deflect Traffic:

The attacks designed to misdirect traffic to a malicious node; however a malicious node could also direct traffic away from itself. This has also been called a gratuitous detour attack [23], and results in the network discovering and using suboptimal routes. Here we use suboptimal in the sense that there are better, more optimal routes. Of course, this attack is not possible if a malicious node is on the only route between two end points. A malicious node could ref A malicious node could refuse to advertise connections or routes, or it could send or modify control packets so that they contain unappealing routing metrics.

In a proactive routing scheme, a malicious node could refuse to advertise a link when originating topology control packets. The effects of this will be minimal, as the malicious node’s neighbours will still advertise the link. The malicious node could also remove links from any topology control packets it receives for forwarding, manipulating the protocol so that nodes will calculate routes not involving the malicious node. A more effective attack would be for a malicious node to refuse to advertise links in a Hello message. Its neighbours would believe links with the malicious node are asymmetrical and, thus, would not advertise the link in their topology control packets.

In a reactive routing scheme, unless the malicious node is the target of a route request, in which case it can refuse to reply, it will need to wait for a rediscovery cycle to occur in order to misdirect traffic away from itself. Once a malicious node receives a route request, it can respond in a variety of ways:

- Modify the metric,
- Delay sending the route request, and
- Drop the route request without rebroadcasting it.

IV. BYZANTINE WORMHOLE ATTACK

If more than one node is compromised, it is reasonable to assume that these nodes may interact in order to gain an additional advantage. This allows the adversary to perform a more effective attack.Indeed, one such attack is a Byzantine wormhole, where two adversaries collude by tunnelling packets between each other in order to create a shortcut (or wormhole) in the network.

This tunnel can be created either using a private communication channel, such as a pair of radios and directional antennas, or by using the existing ad hoc network infrastructure. The adversaries can send a route request and discover a route across the ad hoc network, then tunnel packets through the non-adversarial nodes to execute the attack. 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.

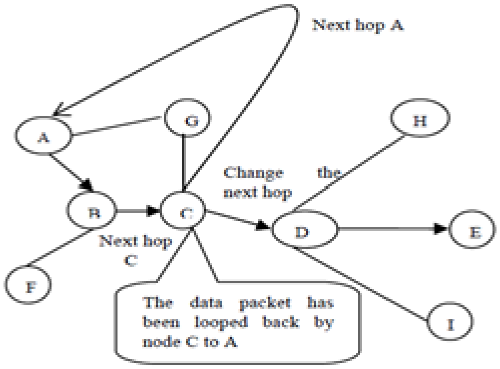


Figure 5. Byzantine Attack.

In the byzantine attack, a malicious node or a set of malicious node works in collusion and carries out attacks such as creating routing loops and routing packets on non-optimal paths. It consumes energy and bandwidth of the network. In Figure 2 in this, assume node B is source node, H is destination node and C is malicious node, which can commit routing loop attack. When node B wants to transmit a data packet to the destination node H, the malicious node C loops the information back to node A in Figure and the packet does not reach to the destination node H

V. RESULTS

In this section all the results are mentioned with the help of snapshots. From the existing system these results are compared and it is observed from the results that our scheme is better than the existing scheme. All the snapshots are as follows:

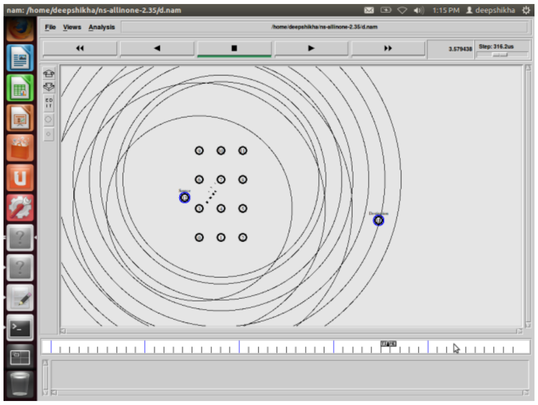

nam: /home/deepshikha/ns-allinone-2.35/d.nam
1:15 PM deepshikha
File Views Analysis
/home/deepshikha/ns-allinone-2.35/d.nam

Figure 6. Byzantine Attack (Routing Looping Attack)

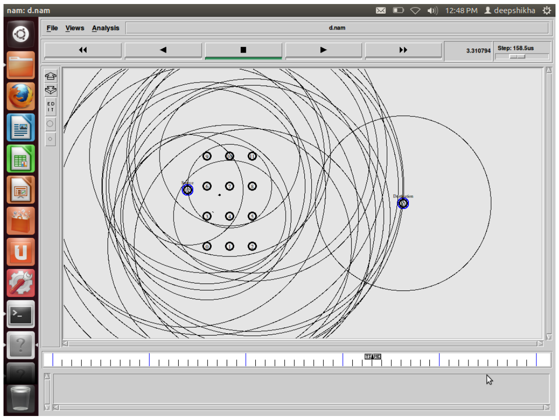


Figure 7. Byzantine Attack (Non-Optimal Path)

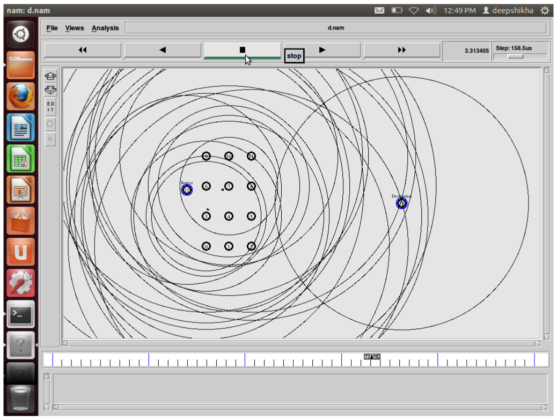


Figure 8. Packet Dropping With Selective Apporoach

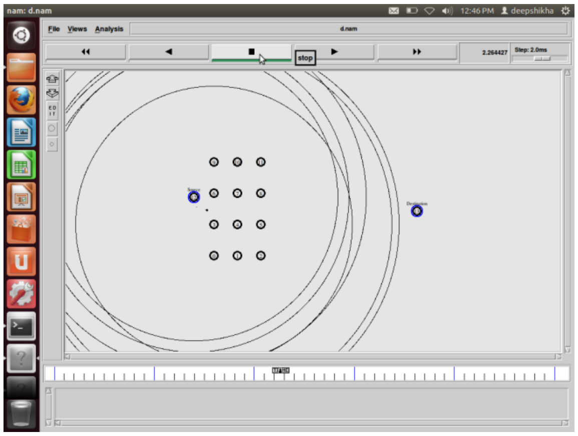


Figure 9. Using ACO Attacks Removed

REFERENCES

[1] Saleh Ali K. Al-Omari, Putra Sumari, “An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications”, Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (J GRAPH-HOC) Vol.2, No.1, March 2010

[2] www.en.wikipedia.org/wiki/Mobile_ad_hoc_network.html

[3] Mohit Kumar, Rashmi Mishra, “An Overview of MANET: History, Challenges and Applications”, Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3 No. 1 Feb-Mar 2012

[4] Sevil ¸ Sen, John A. Clark, “A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks”, Proceedings of the second ACM conference on Wireless network security, 2009

[5] Yian Huang, Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, International journal of computer applications, 2011

[6] http://wirnet.blogspot.in/2009/09/types-of-manet.html

[7] Saleh Ali Alomari and Putra Sumari, “Multimedia Applications for MANETs over Homogeneous and Heterogeneous Mobile Devices”

[8] IETF (1999) RFC 2501 - Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, www.faqs.org /rfcs/rfc-sidx26.html

[9] Hekmat, R. (2006) Ad-hoc Networks: Fundamental Properties and Network Topologies, A book published by Springer.

[10] M.S. Corson, J.P. Maker, J.H. Cernicione, Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) (1999) 63–70

[11] C.-F. Chiasserini, R.R. Rao, Pulsed battery discharge in communication devices, in: Proceedings of The Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM _99), August 15–19, 1999, Seattle, WA, pp. 88–95.

[12] I. Chlamtac, A. Lerner, Link allocation in mobile radio networks with noisy channel, in: IEEE INFOCOM, Bar Harbour, FL, April 1986.

[13] I. Chlamtac, A. Lerner, Fair algorithms for maximal link activation in multi-hop radio networks, IEEE Transactions on Communications COM-35 (7) (1987).

[14] James A. Freebersyser, Barry Leiner, A DoD perspective on mobile ad hoc networks, in: Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.

[15] FarooqAnjum and PetrosMouchtaris,” Security For Wireless ad Hoc Networks”, Wiley inter science. John Wiley & Sons, INC., publication.

[16] C.E. Perkins, P. Bhagwat, Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers, Computer Communications Review (October 1994) 234–244.

[17] P. Jacquet, P. Muhlethaler, A. Qayyum, Optimized Link State Routing Protocol, Internet Draft, draft-ietf-manetolsr-00.txt, November 1998

[18] B. Bellur, R.G. Ogier, F.L. Templin, Topology broadcast based on reverse-path forwarding (TBRPF), IETF Internet Draft, draft-ietf-manet-tbrpf-01.txt, March 2001

[19] D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181

[20] C.E. Perkins, E.M. Royer, Ad-hoc on-demand distance vector routing, in: Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[21] V.D. Park, M.S. Corson, A highly adaptive distributed routing algorithm for mobile wireless networks, in: Proceedings of INFOCOM97, April 1997

[22] R. Dube, C. Rais, K.-Y. Wang, S. Tripathi, Signal stability based adaptive routing for ad hoc mobile networks, IEEE Personal Communications, February 1997, pp. 36–45

[23] Mohammad Ilyas, “The Handbook of Ad Hoc Wireless Networks”

[24] Amitabh Mishra, “SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS”, (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook

[25] Ad hoc network specific attacks held by Adam Burg.