*International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*
**Web Site: www.ijettcs.org Email: editor@ijettcs.org**
**Volume 4, Issue 2, March-April 2015** **ISSN 2278-6856**

# A Study on the Behavior of MANET: Along with Research Challenges, Application and Security Attacks

**Anil Lamba [1], Dr. Sohan Garg [2]**

[1] Research Scholar Venkteshwara University,

[2] SCRIET- CCS University Meerut,

## Abstract

***A mobile ad-hoc network (MANET) is a self-configuring, infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and it means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must frontward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously withstand the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.***

***MANETs have the topographies like much lower mobility and much more rigorous energy requirements. We analyze security goals of MANETs and will describe the research challenges and evaluate open issues in development of routing techniques in MANETs.***

**Keywords:** QoS, MANETs, EMI, OSI, IP, TTL

## 1. INTRODUCTION

Wireless communication has become an ever-present part of modern life, from global cellular telephone systems to local and even personal-area networks. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network organization. Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network

With recent performance developments in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly prevalent use and application, much of which will comprise the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to sustain robust and efficient operation in mobile wireless networks by integrating routing functionality into mobile nodes. Such networks are proposed to have dynamic, sometimes rapidly-changing, random, multi-hop topologies which are likely dignified of relatively bandwidth-constrained wireless links. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network [1].

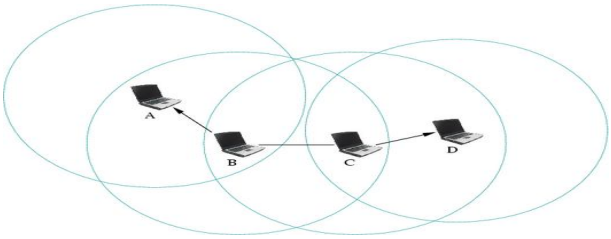


**Figure 1** example ad hoc network, with circles representing nodes [6].

Within the Internet community, routing support for mobile hosts is presently being articulated as "mobile IP" technology. This is a technology to support mobile host "roaming", where a roaming host may be connected through numerous means to the Internet other than its well known fixed-address domain space [2]. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility needs address management, protocol interoperability improvements and the like, but core network functions such as hop-by-hop routing still presently rely upon pre-existing routing protocols operating within the fixed network. In contrast, the objective of mobile ad hoc networking is to extend mobility into the region of autonomous, mobile, wireless domains, where a set of nodes--which may be incorporated routers and hosts-themselves form the network routing infrastructure in an ad hoc fashion.

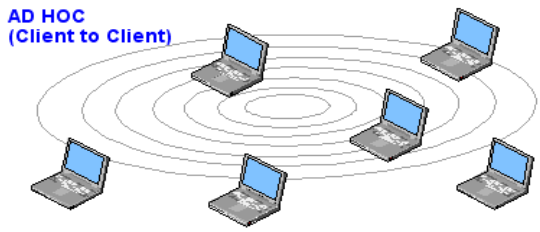


**Figure 2** example ad hoc networks, representing client to client communication [6].

During the last decade, extensive studies have been established on routing in mobile ad hoc networks, and have resulted in several mature routing protocols. However, in order to work properly, these protocols need trusted working environments, which are not always available. In many situations, the environment may be adversarial. For example, some nodes may be selfish, malicious, or compromised by attackers. To address these issues, many schemes have been proposed to secure the routing protocols in ad hoc networks. So, in order to make MANETs protected, all types of attacks are to be identified and solutions to be considered to make MANETs safe [3]. So security concerns in MANETs will remain a potential research area in near future.

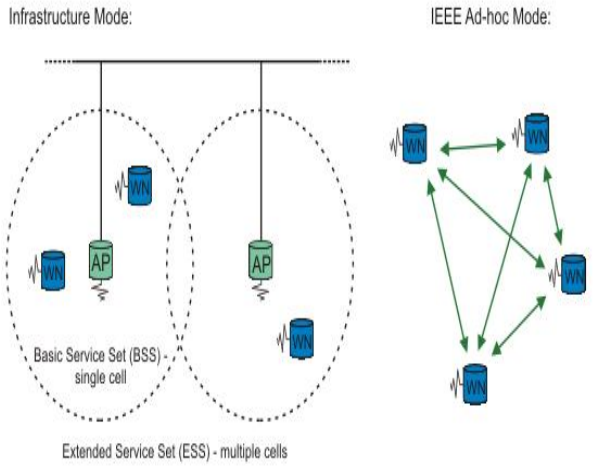


**Figure 3** example ad hoc networks, representing difference between Infrastructure mode and Ad-hoc mode [6].

In this paper we focused on the research challenges and evaluate open issues in development of routing techniques in MANETs. Due to mobility and ad hoc nature, security in mobile ad hoc networks is particularly hard to achieve: In MANETs3 communication between nodes is done through the wireless medium. Because nodes are mobile and may join or leave the network, MANETs have a dynamic topology. Nodes that are in transmission range of each other are called neighbors. Neighbors can send directly to each other [4,5]. However, when a node needs to send data to another non-neighboring node, the data is routed through a sequence of multiple hops, with intermediate nodes acting as routers.

## 2. SECURITY GOALS OF MANETs

The success of MANET strongly depends on whether its security can be trusted. Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging.

**2.1 The goals to evaluate if mobile ad-hoc network is secure or not are as follows**

Provides for effective operation over a wide range of mobile networking "contexts" (a context is a set of characteristics describing a mobile network and its environment);

- **Supports traditional, connectionless IP service:** Reacts efficiently to topological changes and traffic demands while maintaining effective routing in a mobile networking context.
- **IP-Layer Mobile Routing** An improved mobile routing capability at the IP layer can provide an advantage similar to the intention of the original Internet, viz. "an interoperable internetworking ability over a heterogeneous networking infrastructure". In this case, the infrastructure is wireless, rather than hardwired, comprising of multiple wireless technologies, channel access protocols, etc. Improved IP routing and related networking services provide the glue to preserve the integrity of the mobile internetwork segment in this more dynamic environment [7].
- **Interaction with Standard IP Routing** In the near term, it is currently envisioned that MANETs will function as stub networks, meaning that all traffic carried by MANET nodes will either be sourced or sinked within the MANET. Due to the bandwidth and possibly power constraints, MANETs are not presently envisioned to function as transit networks carrying traffic which enters and then leaves the MANET (although this restriction may be detached by succeeding technology advances).This substantially reduces the amount of route advertisement required for interoperation with the existing fixed Internet.

**2.2 The following is a list of desirable qualitative properties of MANET routing protocols:**

**Distributed operation:** This is an essential property, but it should be stated nonetheless.

**2.2.1 Loop-freedom:** Routing protocols must remain to correctly route data even as nodes appear, disappear, and move. It is required that they maintain loop freedom: the absence of cycles across different routing tables. The Ad hoc On-demand Distance Vector (AODV) routing protocol allows the nodes in a Mobile Ad hoc Network (MANET) or a Wireless Mesh Network (WMN) to know where to forward data packets. Such a protocol is “loop free” if it never approach to routing decisions that forward packets in circles.

**2.2.2 Demand-based operation:** Instead of assuming a uniform traffic distribution within the network and continuing routing between all nodes at all times, let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done perceptively, it can utilize

network energy and band width resources more proficiently, at the cost of increased route discovery delay.

**2.2.3 Proactive operation:** The flip-side of demand-based operation. In certain situations, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit; proactive operation is desirable in these contexts.

**2.2.4 Security:** Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs. Adequate security protection to prohibit disruption of modification of protocol operation is desired. This may be slightly orthogonal to any particular routing protocol approach, e.g. through the application of IP Security techniques.

**2.2.5 "Sleep" period operation:** As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocol through a standardized interface.

**2.2.6 Unidirectional link support:** Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links. Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, a sufficient number of duplex links exist so that usage of unidirectional links is of limited added value. However, in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable [8].

## 3. RESEARCH ISSUES IN MANETs

There are numerous issues to consider when deploying MANETs. The following are some of the main issues.

**3.1. Unpredictability of environment:** Ad hoc networks may be deployed in unknown terrains, hazardous conditions, and even hostile environments where interfering or the actual destruction of a node may be imminent. Depending on the environment, node failures may occur frequently.

**3.2. Unreliability of wireless medium:** Communication through the wireless medium is unreliable and subject to errors. Also, due to varying environmental conditions such as high levels of electro-magnetic interference (EMI) or inclement weather, the quality of the wireless link may be unpredictable. Additionally, in some applications, nodes may be resource-constrained and thus would not be able to support transport protocols needed to ensure reliable communication on a lossy link. Thus, link quality may fluctuate in a MANET.

**3.3. Resource-constrained nodes:** Nodes in a MANET are typically battery powered as well as limited in storage and processing abilities. Moreover, they may be situated in areas where it is not possible to re-charge and thus have limited lifetimes. Because of these limitations, they must have algorithms which are energy-efficient as well as operating with limited processing and memory resources. The available bandwidth of the wireless medium may also be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

**3.4. Dynamic topology:** The topology in an ad hoc network may change continuously due to the mobility of nodes. As nodes move in and out of range of each other, some links break while new links between nodes are created. As a result of these issues, MANETs are prone to numerous types of faults including.

**3.5 Transmission errors:** The unreliability of the wireless medium and the unpredictability of the environment may lead to transmitted packets being corrupted and thus received in error.

**Node failures:** Nodes may fail at any time due to different types of hazardous conditions in the environment. They may also drop out of the network either voluntarily or when their energy supply is depleted.

**Link failures**: Node failures as well as changing environmental conditions (e.g., increased levels of EMI) may cause links between nodes to break.

**Route breakages:** When the network topology changes due to node/link failures and/or node/link additions to the network, routes become out-of date and thus improper. Depending upon the network transport protocol, packets forwarded through stale routes may either eventually be dropped or be delayed; packets may take a circuitous route before eventually arriving at the destination node.

**Congested nodes or links:** Due to the topology of the network and the nature of the routing protocol, certain nodes or links may become over utilized, i.e., congested. This will lead to either larger delays or packet loss. Routing protocols for MANETs must deal with these issues to be effective.

## 4. MANETs VULNERABILITY

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before permitting data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

**4.1 Lack of centralized management:** MANET doesn't have a centralized monitor server. The absence of management makes the discovery of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of

centralized management will impede trust management for nodes [9].

**4.2 Resource availability**: Resource availability is a foremost issue in MANET. Providing protected communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

**4.3 Scalability:** Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

**4.4 Cooperativeness:** Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

**4.5 Dynamic topology:** Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

**4.6 Limited power supply:** The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

**4.7 Bandwidth constraint:** Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

**4.8 Adversary inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

**4.9 No predefined Boundary:** In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [10].

## 5. RESEARCH CHALLENGES OF MANETs

MAJOR CHALLENGES IN MANET Regardless of the attractive applications, the features of MANET introduces various challenges that must be studied carefully before a wide commercial deployment can be expected [11]. These include Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multi hop, may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

**5.1 Security and Reliability:** In addition to the common vulnerabilities of wireless connection, an ad hoc network has its specific security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors. Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered [12].

**5.2 Routing:** Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes be-comes a challenging task. Maximum protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

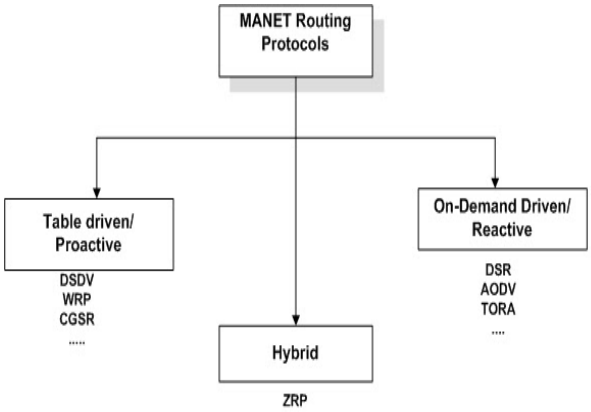


**Figure 4** representing MANET protocol classification [6].

**5.3 Device discovery:** Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection. Bandwidth-constrained-variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts.

**5.4 Power-constrained and operation:** Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

**5.5 Quality of Service (QoS):** Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services. Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management. Multicast: Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join) [13].

**5.6 IP-Layer Mobile Routing:** An improved mobile routing capability at the IP layer can provide a benefit similar to the intention of the original Internet, viz. "an interoperable internetworking capability over a heterogeneous networking infrastructure".

**5.7 Diffusion hole problem:** The nodes located on boundaries of holes may suffer from excessive energy consumption since the geographic routing tends to delivers data packets along the hole boundaries by perimeter routing if it needs to bypass the hole. This can enlarge the hole because of excessive energy consumption of the node boundaries nodes.

## 6. The major challenges faced by the MANETS can be broadly classified as

**6.1**. In incorporating emerging wireless network elements such as MDs, ad-hoc routers and embedded sensors in the existing protocol framework and

**6.2.** To provide end-to-end service abstractions that facilitates application development. These challenges are posed by a wide range of environments such as cellular data services, Wi Fi hot-spots, Info stations, mobile peer-to-peer, Ad-hoc mesh networks for broadband access, vehicular networks, sensor networks and pervasive systems. These wireless application scenarios lead to a diverse set of service requirements [14] for the future Internet as summarized below:

**a)** Naming and addressing flexibility.
**b)** Mobility sustenance for dynamic migration of end-users and network devices.
**c)** Location services that make available information on geographic position.
**d)** Self-organization and discovery for distributed control of network topology.
**e)** Security and privacy attentions for mobile nodes and open wireless channels.
**f)** Decentralized organization for remote monitoring and control.
**g)** Cross-layer sustenance for optimization of protocol performance.
**h)** Sensor network structures such as aggregation, content routing and in-network Processing.
**i)** Cognitive radio sustenance for networks with physical layer adaptation.
**j)** Economic incentives to inspire efficient sharing of resources.

**6.3 MANET requirements represent a spectrum of network challenges:**

During the last few years, more or less every aspect of MANET has been discovered to some level of detail. Yet, more questions have arisen than been answered. The major open difficulties are listed [15] as:

**(a) Autonomous:** No centralized administration entity is obtainable to manage the operation of the different mobile nodes.
**(b) Dynamic topology:** Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network fluctuate timely and are based on the closeness of one node to another node.
**(c) Device discovery:** Identifying relevant newly moved in nodes and informing about their presence need dynamic update to facilitate automatic optimal route selection.
**(d) Bandwidth optimization:** Wireless links have expressively lower capacity than the wired links.
**(e) Limited resources**: Mobile nodes trust on battery power, which is a scarce resource. Also storage capacity and power are severely limited.
**(f) Scalability:** Scalability can be broadly well-defined as whether the network is capable to provide an acceptable level of service even in the presence of a large number of nodes.
**(g) Limited physical security:** Mobility indicates higher security risks such as peer-to-peer network architecture or a shared wireless medium accessible to both legitimate network users and vindictive attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.
**(h) Infrastructure-less and self-operated:** Self-remedial feature demands MANET should realign itself to blanket any node moving out of its range.
**(i) Poor Transmission Quality:** This is an intrinsic problem of wireless communication caused by several error sources that effect in degradation of the received signal.
**(j) Ad hoc addressing:** Challenges in standard addressing arrangement to be implemented.
**(k) Network configuration:** The whole MANET infrastructure is dynamic and is the purpose for dynamic connection and disconnection of the variable links.
**(l) Topology maintenance:** Bring up-to-date information of dynamic links among nodes in MANETs is a foremost challenge.

## 7. CONCLUSION & FUTURE SCOPE

MANETs, the most spoken term in wireless technologies, approach to be the ruler of future airs provided the vision of “anytime, anywhere” communications. In this paper,

we have analyzed the security threats of an ad-hoc network faces. We emphasis on the security-sensitive applications of an ad-hoc networks require high degree of security and ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a necessity to make them more secure and robust to adapt to the demanding requirements of MANET for the future. We also overviewed the challenges and solutions of the security threats in mobile ad hoc networks. In this paper, we discuss MANET and its characteristics, challenges, advantages, application, security goals, various types of security attacks in its routing protocols.

In future more and more efficient routing protocols for MANET might come, which may take security and QoS (Quality of Service) as the major concerns. So far, the routing protocols mainly focused on the methods of routing, but in future a secured but QoS-aware routing protocol could be worked on. Ensuring both of these parameters at the same time might be difficult. A very secure routing protocol surely gains more overhead for routing, which might degrade the QoS level. So an optimal trade-off between these two parameters could be searched in future.

## References

[1] S.-J. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia, 2000: "A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols," In Proceedings of IEEE INFOCOM 2000, pp. 565–574..

[2] Changling Liu and Jorg Kaiser.,2005: "A Survey of Mobile ad hoc network routing protocols", University of Ulm Tech. Report Series.

[3] Yu-CheeTseng , Wen-Hua Liao and Shih-Lin Wu.,2002: "Mobile ad hoc networks and Routing Protocols" Handbook of wireless networks and mobile computing,pp.371-392.

[4] Banta Sigh. & Manish Kumar "Study on Security Issues & Challenges in MANET","PARIPEX - INDIAN JOURNAL OF RESEARCH", Volume: 3, Issue: 4,April 2014, pp. 54-57.

[5] C. Sreedhar, VarunVarmaSangaraju, "A Survey On Security Issues In Routing In MANETS", "International Journal of Computer & organization Trends(IJCOT)",V3(9):399-403 October 2013.ISSN2249-2593.www.ijcotjournal.org. Published by Seventh Sense Research Group,pp. 399-403

[6] http://www.yourdictionary.com/mobile-ad-hoc-network, http://www.mogi.bme.hu/TAMOP/ http://www.eexploria.com/routing-protocols-in-manets/, http://perso.crans.org/raffo/papers/phdthesis/thesisch1.html

[7] J. Godwin Ponsam, R. Srinivasan, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", " International Journal of Emerging Trends & Technology in Computer Science" Volume 3, Issue 1 January – February 2014 pp. 274-279.

[8] Royer, E., and Toh, C. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications, **6**(2), Apr. 1999, pp. 46–55.

[9] Ankur O. Bang, Prabhakar& L. Ramteke, "MANET : History, Challenges And Applications", "International Journal of Application or Innovation in Engineering & Management (IJAIEM)", Volume 2, Issue 9, September 2013 pp. 249-251.

[10] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–6.

[11] HaoYang, Haiyun & Fan Ye — "Security in mobile ad-hoc networks : Challenges and solutions", Pg. 38-47, Vol 11, issue 1, Feb 2004.

[12] Nilsson, A., and Tuominen, A. J. Internet Connectivity for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, **2**(5), Aug. 2002, pp. 465–482.

[13] Gupte, S., and Singhal, "M. Secure routing in mobile wireless ad hoc networks. Ad Hoc Networks", **1**(1), 2003, pp. 151–174.

[14] S. Tabatabaei and K. Tabatabaei "Routing and quality of service support for mobile Ad hoc networks"in proceeding of International conference on Computer Engineering and Technology, Chengdu, china,April 2010.

[15] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance issues and Evaluation Considerations", Network Working Group, RFC2501, January 1999.