# CHALLENGES AND ISSUES of MANET

**Hewa Majeed Zangana**

*Department of Computer Science / College of Computer Science and IT / Nawroz University / Kurdistan Region of Iraq*

*e-mail: hewa.majeed@nawroz.edu.krd*

**Abstract:**
Mobile ad-hoc network's (MANET's) are infrastructure less mobile network's that has no fixed routers. All nodes are capable of movement and can be connected dynamically in an arbitrary manner using radio waves. This paper focuses on study of Mobile ad-hoc Networks (MANET'S), and its classification and characteristics. This paper also focuses on the issues and challenges that are imposed by Mobile ad-hoc Networks (MANET'S).

**Keywords:** Handoff, WLAN, MANET, VANET, PDA, Quality of Services (QoS), Denial of Service (DoS), Multi Hop Router, Non-Repudiation

## I. Introduction

Wireless networks have become increasingly popular in the computing industry, since their emergence in the 1970s. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. There are currently two variations of mobile wireless networks. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. As the mobile travels out of range of one base station and goes into the range of another, a "handoff" occurs from the old base station to the new, and the mobile is able to continue communication seamlessly throughout the network. Typical applications of this type of network include wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, commonly known as a Mobile ad-hoc network (MANET). Infrastructure less networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Example applications of ad-hoc networks are emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrains.

## II. Literature Review

Mobile ad hoc networks (MANETs) are complex distributed systems that comprise of wireless mobile nodes that can freely and dynamically organize themselves into arbitrary and temporary, 'ad-hoc' network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, as in case of disaster recovery environments. Ad hoc networking concept is not a new one, having been around in various forms for over 30
Years. Traditionally, tactical networks have been the only communication networking application that followed the ad hoc paradigm. With the introduction of new technologies such as the Bluetooth, IEEE 802.11, eventual commercial MANET deployments have been made outside the military domain. These recent evolutions have been generating a renewed

and growing interest in the research and development of MANET [1].

In recent years, the eminent growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has caused a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [2].

In the ubiquitous computing environment, individual users simultaneously utilize several electronic platforms through which they can access all the required information whenever and wherever they may be [3]. The ubiquitous nature of computing has made it mandatory to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to acquire wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted major thrust from many researchers [4].

A Mobile Ad hoc NETwork35 (MANET) is a system of wireless mobile nodes that dynamically organize themselves in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without an already communication infrastructure or when the use of such infrastructure requires wireless extension [5].

Perhaps the most widely accepted and acknowledged notion of a mobile ad hoc network is a network formed without any central administration, consisting of mobile nodes that use a wireless interface to send packet data. As the nodes in a network of this kind can serve as routers and hosts, they can forward packets on behalf of other nodes and run user applications [6].

Mobile ad hoc networks are systems that are autonomous, comprised of a number of mobile nodes that communicate through wireless means of communication. They are self-organized, self-configured and self-controlled infrastructure-less networks. These networks have the ability to be set up and deployed quickly because it has a simple infrastructure set-up and no central administration [7].

Mobile ad hoc networks (MANET's) are self-configuring and infrastructure-less networks that are comprised of mobile nodes which communicate over wireless links without any central control and on a peer-to-peer basis. These individual nodes act as routers to forward both their own data and also their neighbor's data by sending and receiving packets to and from other nodes in the network. The self configuration and the quick deployment make ad hoc networks suitable for emergency situations (such as human or natural disasters) and for military operations [8]. One scenario is establishing communication between different agents in a disaster recovery operation where e.g. fire fighters need to connect to local ambulances and traffic control, in circumstances where the normal communication infrastructure is destroyed or otherwise rendered unusable. In such situations a collection of mobile nodes with wireless network interface can form a transitory network [9].

Mobile ad hoc networks (MANET's) are autonomous systems of mobile nodes connected by wireless links. These nodes are therefore free to move arbitrarily. The topology of these networks changes dynamically and unpredictably. MANETs have many characteristics that make them different from other wireless and wired networks that are widely recognized [10, 11, 12, 13, and 14]:

1. Multi-hop communications: The communication between any two remote Nodes in MANET is performed by numerous intermediary nodes whose functions are to relay data-packets from one point to another. Thus, ad hoc

networks require the support of multi-hop communications.

2. Constrained Resources: Generally, MANET devices are small hand-held devices ranging from personal digital assistants (PDAs) and laptops down to cell phones. These devices indeed have limitations because of their restricted nature; they are often battery-operated, with small processing and storage facilities.

3. Infrastructure less: MANETs are formed based on the collaboration between autonomous nodes, peer-to-peer nodes that need to communicate with each other for special purpose, without any pre-planned infrastructure or base station.

4. Dynamic Topology: MANET nodes are free to move, hence the connectivity between nodes in MANET can change with time, because nodes can move arbitrarily; thus the nodes can be dynamically inside and outside the network, constantly changing their links and topology, leading to change in the routing information all the time due to the movement of the nodes. Therefore, the communicated links between nodes in MANET can be bi-directional or unidirectional.

5. Limited Device Security: MANET devices are usually small and can be transported from one place to another, and then they are not constrained by location. Unfortunately, as a result these devices could be easily lost, stolen or damaged.

6. Limited Physical Security: Generally, MANETs are more susceptible to physical layer attacks than wired network; the possibility of spoofing, eavesdropping, jamming and denial of service (DoS) attacks should be carefully considered. By contrast the decentralized nature of MANET makes them better protected against single failure points.

7. Short Range Connectivity: MANETs rely on radio frequency (RF) technology to connect, which is in general considered to be short range communication. For that reason, the nodes that want to communicate directly need to be in the close frequency range of each other. In order to deal with this limitation, multi-hop routing mechanisms have therefore to be used to connect distant nodes through intermediary ones that operate as routers.

## III. Characteristics

Mobile ad-hoc networks (MANET's) have following characteristics:

•No infrastructure – flat network •Radio communication – shared medium

•Every computer or device (node) is a router as well as end host

•Nodes are in general autonomous

•Mobility – dynamic topology

•Limited energy and computing resources. Unreliability of wireless links between nodes

.Lack of incorporation of security features in statically configured wireless routing Protocol not meant for ad hoc environments.

## IV. Issues In Mobile Ad-Hoc Networks:

There are several issues within ad hoc networks that make them very complicated to integrate with the existing global internet. The problems are addressed below:

❒Routing

Routing is one of the most complicated problems to solve as ad hoc networks have a seamless connectivity to other devices in its neighborhood. Because of multi hop routing no default route is available. Every node acts as a router and forwards each other's packets to enable information sharing between mobile nodes.

❒Security

Clearly a wireless link is much more vulnerable than a wired link. The science of cracking the encryption and Eaves dropping on radio links has gone on since the first encryption of radio links was established. The user can insert spurious information into routing packets and cause routing loops, long time-outs and advertisements of false or old routing table

updates. Security has several unsolved issues that are important to solve to make the ad hoc network into a good solution.

❒Quality of Service (QoS)

QoS is a difficult task for the developers, because the topology of an ad hoc network will constantly change. Reserving resources and sustaining a certain quality of service, while the network condition constantly changes, is very challenging.

## V. Challenges In Mobile Ad-Hoc Networks:

❒Host is no longer an end system - can also be an acting intermediate system
❒changing the network topology over time
❒Potentially frequent network partitions
❒Every node can be mobile
❒Limited power capacity
❒Limited wireless bandwidth
❒Presence of varying channel quality
❒No centralized entity – distributed
❒How to support routing?
❒How to support channel access?
❒How to deal with mobility?
❒How to conserve power?
❒How to use bandwidth efficiently?

The main challenge of MANETs is their vulnerability to security attacks and how to operate securely and efficiently while preserving its own resources [15]. MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. 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 [16].

The challenges of supporting Quality of Service in ad hoc networks are how to reserve bandwidth and how to guarantee the specified delay for real-time application data flows. For wireless transmissions, the channel is shared among neighbors. Therefore, the available bandwidth depends on the neighboring traffic status, as does the delay. Due to this characteristic, supporting QoS cannot be done by the host itself, but cooperation from the hosts within a node's interference range is needed. This requires an innovative design to coordinate the communication among the neighbors in order to support QoS in MANETs. Furthermore, the distributed organization of MANETs brings additional challenges to collaboration for supporting QoS [17, 18].

There are situations where user required networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge. More recently, new alternative ways to deliver the services have been emerging. These are focused around having the mobile devices connect to each other in the transmission range through automatic configuration, setting up an ad hoc mobile network that is both flexible and powerful. In this way, not only can mobile nodes communicate with each other, but can also receive Internet services through Internet gateway node, effectively extending Internet services to the non-infrastructure area. As the wireless network continues to evolve, these ad hoc capabilities are expected to become more important, the technology solutions used to support more critical and significant future research and development efforts can be expected in industry and academy [19].

Since security is an essential component in MANET, the striking features of mobile ad hoc networks raise both challenges and opportunities in achieving these security goals, Unlike other traditional networks (wired) where nodes must have physical access to the network or communicate through several defense perimeters like firewalls and gateways, MANET uses the wireless medium so attacks on a wireless network can come from all directions and target any node. This provides a larger surface of attack ranging from passive

attacks, such as "tapping" to active attacks, such as message replay, message leakage, contamination and distortion. This means that a MANET does not have a clear line of defense, and every node must be prepared to defend against the different kind of attacks [20]. The key challenges in MANETs design come from the decentralized nature, Self-organization, self-management, and also the fact that all communications are carried over wireless links in short-range communication [21]. The lack of centralized management in MANET makes the detection of attacks a very complicated issue. Mobile ad hoc networks are highly dynamic and large scale, and they cannot be easily monitored; benign (non-malignant) failures in MANETs are fairly common, e.g. transmission destructions and packet dropping. As a result, malicious failures will be more difficult to identify. Since security is an essential component in a hostile environment, these unique characteristics of mobile ad hoc networks raise challenges that security requirements must address [22,23].

## VI. Characteristic Issues of mobile ad hoc networks

1. Unreliable wireless communication between nodes: Mobile nodes do not consistently participate in communication, since their energy resource is extremely limited.
2. Non-repudiation: the inability of any node within a MANET to negate the fact that it is a sender of a message. This requirement is provided by producing a signature for every message. In a usual encryption procedure by the public key method, every node in a MANET signs a message by application of a private key. All other nodes verify the signed message with this node's public key, therefore he cannot negate that his signature is attached to the message.
3. Availability represents the availability of all network services and resources to legitimate network users, which is essential for preserving the network structure during the attacks.
4. Access control is a procedure for prevention of unauthorized access and use of network systems and resources.

## VII. Conclusion and Future Work

This paper discussed about Mobile Ad-hoc networks, their classification, their characteristics, and the issues and challenges that are posed by Mobile ad-hoc networks. This paper also gave a detailed review of literature about Mobile ad-hoc networks and the issues and challenges posed by them. The future work of this research paper is to improve the standard of Mobile ad hoc networks so as to overcome the issues and challenges posed by them.

## References

[1] Imrich Chlamtac a, Marco Conti b, Jennifer J.-N. Liu c, "Mobile ad hoc networking: Imperatives and Challenges", ELSEVIER, 2003, 13-64.

[2] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[3] M. Weiser, "The Computer for the Twenty-First Century", Scientific American, September 1991.

[4] Wenjia Li and Anupam Joshi, Security Issues in Mobile Ad Hoc Networks - A Survey. [5] M.S. Corson, J.P. Maker, and J.H. Cernicione, "Internet-based Mobile Ad Hoc Networking", IEEE Internet Computing, pages 63–70, July-August 1999.

[6] Magnus Frodigh, Per Johansson and Peter Larsson, "Wireless ad hoc networking— The art of networking without a network", Ericsson Review No. 4, 2000. 248

[7] Mehul, Ekata, and Vikram Limaye. Security in Mobile Ad Hoc Networks. Handbook Mobile Business, 2nd Ed. Bhuvan Unhelkar. Hershey: IGI Global, 2009. 541-58.

[8] Hamza Aldabbas, Tariq Alwada'n, Helge Janicke, Ali Al-Bayatti,"Data Confidentiality in Mobile Ad hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, February 2012

[9] Subir Kumar Sarkar, T. G. Basavaraju, and C. Puttamadappa. Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications. Auerbach Publications, Boston, MA, USA, 2007.

[10] Jameela Al-Jaroodi. Security issues at the network layer in wireless mobile ad hoc Networks at the network layer. Technical report, Faculty of Computer Science and Engineering, University of Nebraska-Lincoln, Nebraska, USA, 2002.

[11] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2004.

[12] C.K. Toh. Maximum battery life routing to support ubiquitous mobile computing in Wireless ad hoc networks. IEEE communications Magazine, 39 (6): 138–147, 2001.

[13] R. Chadha and L. Kant. Policy-driven mobile ad hoc network management. Wiley-IEEE Press, 2007.

[14] D. Djenouri, L. Khelladi, and N. Badache. A survey of security issues in mobile ad hoc Networks. IEEE communications surveys, 7 (4), 2005.

[15] DRAGAN MLADENOVIĆ, DANKO JOVANOVIĆ. "Mobile ad hoc networks Security", 5th International scientific Conference on defensive technologies, OTECH 2012.

[16] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges".

[17] Guerin R., Orda A., "QoS-based routing in networks with inaccurate information: Theory and algorithms", in Proc. IEEE INFOCOM'97, Japan, pp. 75-83.

[18] Broch J., Johnson D., Maltz A., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", draft-ietf-manet-dsr-03.txt, work in progress. October 1999.

[19] Pravin Ghosekar, Girish Katkar, Dr. Pradip Ghorpade. "Mobile Ad Hoc Networking: Imperatives and Challenges" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[20] Y. Zhang and W. Lee. Security in mobile ad-hoc networks. Ad hoc Networks, pages 249–268, Ed. Prasant mohapatra Srikanthv. Krishnamurthy. Springer, 2005.

[21] M. Carvalho. Security in mobile ad hoc networks. Security Privacy, IEEE, 6 (2): 72 – 75, 2008.

[22] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: Challenges and solutions. Wireless Communications, IEEE, 11 (1): 38–47, 2004.

[23] D. Djenouri, L. Khelladi, and N. Badache. A survey of security issues in mobile ad hoc networks. IEEE communications surveys, 7 (4), 2005

[24] Ismael Al-Sanjary, O., Abdullah Ahmed, A., Majeed Zangana, H., A.M Ali, M., Hazim Alkawaz, M., & Hameed Aldulaimi, S. (2018). An Investigation of the Characteristics and Performance of Hybrid Routing Protocol in (MANET). *International Journal of Engineering & Technology, 7*(4.22), 49-54. doi:http://dx.doi.org/10.14419/ijet.v7i4.22.22188

[25] H. M. Zangana, "Developing Data Warehouse for Student Information System ( IIUM as a Case Study )," *International Organization of Scientific Research,* vol. 20, no. 1, pp. 09-14, 2018.