



A SURVEY REPORT: MOBILE AD-HOC NETWORK AND ITS USAGE

Pooja Tiwari, Anil Mishra, Sumit Dubey

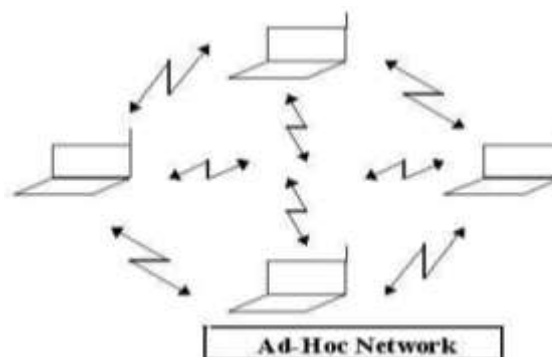
¹Student (M.Tech. ECE), ²HOD Dept. of ECE, ³Assistant Professor ECE

Abstract: In this paper, we have discussed the basic of mobile ad hoc network (MANET). Mobile Ad Hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration, in which individual nodes cooperate by forwarding packets to each other to allow nodes to communicate beyond direct wireless transmission range. Routing is a process of exchanging information from one station to other stations of the network. Routing protocols of mobile ad-hoc network tend to need different approaches from existing Internet protocols because of dynamic topology, mobile host, distributed environment, less bandwidth, less battery power.

Keywords: routing, topology, dynamic, bandwidth, exchange, transmission

I. Introduction

Mobile Ad-hoc network is a type of wireless network there are currently two variations of mobile wireless networks infrastructure and Infrastructure less networks. The infrastructure networks, also known as Cellular network, have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs). The other type of network, Infrastructure less network, is known as MANET. These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.



The interest in wireless ad hoc networks stems from of their well-known advantages for certain types of applications. Since, there is no fixed infrastructure; a wireless ad hoc network can be deployed quickly. Thus, such networks can be used in situations where either there is no other wireless communication infrastructure present or where such infrastructure cannot be used because of security, cost, or safety reasons.

II. Characteristics of MANET

Some of the main characteristics of MANET are as follows:

- **Dynamic Topologies:** Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times. The links may be unidirectional bidirectional.

- **Bandwidth constrained, variable capacity links:** Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.
- **Energy constrained operation:** Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.
- **Limited physical security:** 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. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches.
- **Security:** Security is the major issue in wireless Ad Hoc Networks and actually ought to receive a complete analysis of it than being presented as a part of the study on Ad Hoc Networks. The use of wireless links renders an ad hoc network susceptible to link attacks ranging from denial of service, passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation.

Nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted. An ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network. The denial of a service can be caused by such legitimate ways as a radio jamming or battery exhaustion. An attacker can cause a radio jamming by jamming a wider frequency band and in that way using more power. The latter can be of real threat, because once a battery runs out the attacker can walk away and leave the victim disabled. This kind of technique is called the sleep deprivation torture attack. Symmetric key cryptography is used to provide authenticity and integrity. Integrity means that no node has been maliciously changed. The devices themselves should be able to detect security breaches and plug them.

III. Future scope

There are a few areas that need to be given particular focus for improvement in Ad Hoc Networks.

- **Scalability:** Currently the size of Ad Hoc Networks are small and work needs to be done to identify to what size can these networks grow and further try to increase the size of these networks to what is that of the Internet today.
- **Quality of Service:** A quality of service is defined for the network with no losses and attempts should be made achieve that. QoS parameters will involve bandwidth considerations and savings of bandwidth will be implemented. Also finding the shortest path so as to save power in the devices as the source of power is very limited. Care should be taken so as to have no collision losses.
- **Power Control:** Reducing power to the communications interface and entering sleep state are ways of extending battery life of mobile units. But these techniques make communication difficult. Hence some efficient technique should be developed to make this viable. Research should also focus on getting battery technology growth on par with Ad Hoc Network Technology growth.
- **Security:** Security needs to be very widely investigated as they are imperative. Wireless networks are as such insecure and particularly so with Ad Hoc Networks. Implementations of current cryptography techniques are not good enough and also difficult.
- **Location Access:** User location could be incorporated into routing.

IV. Conclusion

In this paper we discussed about basic introduction of MANIT, its characteristics, advantages, security concepts, etc. The other type of network, Infrastructure less network, is known as Mobile Ad-hoc Network (MANET).

These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. And they have no fix area, boundation or infrastructure for communication.

References

- [1] A Brief Overview of Ad Hoc Networks: Challenges and Directions: Ram Ramanathan and Jason Redi, BBN Technologies. IEEE Communications Magazine, 50th Anniversary Commemorative Issue, May 2002
- [2] Ad Hoc Networking: Charles E. Perkins. Addison-Wesley, December 2000.
- [3] Mobile Ad Hoc Networking: Imperatives and challenges: Imrich Chlamtac, Marco Conti & Jennifer Liu. Ad Hoc Networks Publication, Volume 1, Issue 1, July 2003.
- [4] On reducing the Broadcast Redundancy in Ad Hoc Wireless Networks: Wei Lou & Jie Wu, IEEE transactions on mobile computing. April- June 2002.
- [5] Secure message transmission in mobile ad hoc networks: Yih-Chun Hu; David B. Johnson; Adrian Perrig. Proceedings of the 2003 ACM workshop on Wireless security
- [6] Security in Ad-hoc Networks: Anne Vanhala, University of Helsinki, Department of Computing Science, Research seminar on Security in Distributed Systems.
- [7] Securing Ad Hoc Networks: Lidong Zhou & Zygmunt J. Haas, Cornell University, Ithaca, NY. IEEE Networks Special Issue on Network Security. November/December, 1999