



International Journal of Engineering, Business and Enterprise Applications (IJEBEA)

www.iasir.net

An efficient and Scalable approach to build a Robust Network using MANETs

Jaspreet Singh^{1,2} and C.S. Rai³

¹Research Scholar, USICT, Guru Gobind Singh Indraprastha University, New Delhi, INDIA.

²Sr. Assistant Professor, Department of Computer Applications, BCIIT, New Delhi, INDIA.

³Professor and Dean, University School of Information Technology,
Guru Gobind Singh Indraprastha University, Delhi, INDIA.

Abstract: Today, wireless networks are widely used in our day to day operations. A few years back, wireless networks existed only in labs, as they were typically expensive. However recently, there has been mass proliferation of inexpensive wireless devices. This has made wireless networks immensely popular and attractive. One such wireless network, where a lot of interest has generated, over last few years, is ad hoc networks. Ad hoc networks are self configuring, infrastructureless mobile networks, which are established on the fly. They are multi-hop in nature. This paper is an attempt to document major aspects concerning ad hoc networks and their suitability to become the preferred networks of the future. We bring to focus, potential applications of ad hoc networks and the benefits accrued from them. Implementation details of ad hoc networks, alongwith the underlying technology and various concerns of ad hoc networks, such as routing and security, are also discussed. There are several challenges concerning successful implementation of these networks commercially, which are highlighted. Despite these challenges, the importance of ad hoc networks in pervasive, ubiquitous computing is imminent and supported in this paper.

I. Introduction

Mobile Ad-hoc networks (MANETs) are self organizing, infrastructure-less and multi-hop packet forwarding networks. Contrary to wireless infrastructure networks such as cellular networks, wi-fi, WLANs, etc, there is complete absence of any infrastructure like base stations or any centralized control. So, each node in the network acts as a router to forward the packets to the next node. It is an autonomous association of mobile nodes that interact and communicate with each other, to form a network. Ad-hoc networks are capable of handling of topology changes and malfunctions in nodes.

Earlier, ad hoc networks were confined to military applications and research labs. But recent growth of wireless devices and their mass proliferation has created a new interest in commercial products based upon ad hoc networks. Suddenly, there is a spurt in availability of different wireless devices such as mobile phones, laptops, tablets, PDAs and the like. Many different networks such as cellular networks (2G and 3G), wi-fi, WLANs are already in operation. The convenience of using wireless devices clearly overweighs their limitations and security concerns. Now there is a need to integrate these technologies with ad hoc networks, to realize the benefits of these networks.

The following are the characteristics of mobile ad-hoc networks

- **Dynamic topology:** The nodes are mobile and connected to the network dynamically and arbitrarily. As a result, network topology changes randomly with time and is unpredictable. It may result in disconnection of nodes from the network.
- **Bandwidth constraints:** The less capacity of links will result in congestion and packet loss in the network.
- **Energy constraints:** The mobile nodes rely on the batteries as a source of power, which is always limited. It is invariably inadequate as per the needs of nodes.
- **Limited physical security:** Mobile network is more error prone to security threats because devices may be stolen or the data traffic may have to pass through the insecure links.
- **Autonomous and self-operating:** There can be no central entity to manage the nodes. All the nodes must be capable of managing themselves, as well as inter-node processes and communication.

These characteristics make working with ad hoc networks, a real challenge, as they impose severe restrictions on the network. These constraints have to be borne in mind, before designing any application. Ad hoc networks need not operate in isolation, as we can think of many applications where, they need to be connected to other networks and the Internet. For this, we need to enhance our solutions, before they can adequately answer such needs.

In areas where no infrastructure such as internet is available an Ad-hoc network could be used by a group of wireless mobile nodes. This can be the case in areas where network infrastructure may be undesirable due to reason such as crisis, cost and inconvenience, or simply unavailable. Examples of such situations include disaster recovery personnel or military troops in cases where normal infrastructure is either unavailable or destroyed. Other examples where ad hoc networks could be used, include business associates wishing to share files in airport terminals, meetings, conferences, etc. or students needing to interact during a lecture. If each mobile host is wishing to communicate is equipped with wireless local area network interface, the group of mobile hosts may form an ad-hoc network.



Fig. 1a: An Infrastructured Network

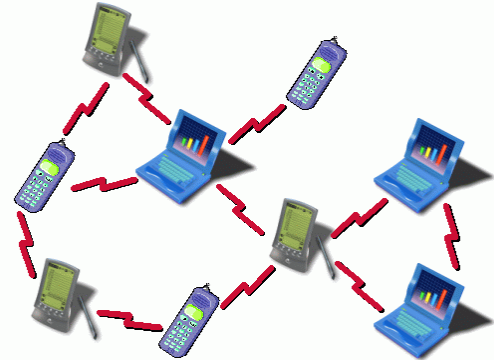


Fig. 1b: An Ad Hoc Network

Quality of Service (QoS) is the performance level of a service offered by the network to the user. The goal of QoS is to achieve a more deterministic network behaviour, so that information carried by the network can be better delivered and network resources can be better utilized. A service can be perceived by a set of measurable pre-specified service requirements such as minimum bandwidth, maximum delay, maximum delay variance (jitter) and maximum packet loss rate.

The key challenge in mobile ad hoc networks is to route the packets with low overheads even in dynamic conditions of node mobility, limited channel bandwidth and limited battery power of nodes. Overhead is defined as control messages, which consumes channel bandwidth as well as the battery power of nodes. The mobility of nodes changes the topology of network frequently. When a node becomes unavailable, alternate routes have to be searched. This increases the delay and also number of lost packets.

II. Key Applications

Ad hoc networks can virtually be used at any place. However, many constraints of ad hoc networks, restrict their usage at many places. But there are many applications, where ad hoc networks are the only apt choice and can be used very effectively. Some of the applications envisaged are:

1. **Military Operations:** Consider a scenario where a mobile network is to be built instantly for a military operation and without availability of any existing infrastructure such as base stations. One possibility is to use satellites for communication, if available. But satellites may not be the apt choice for any of the following reasons:

- Non availability of required bandwidth
- Possible security risks, due to high chances of data being intercepted. This may put a question on their vary use.
- Prohibitive costs of setting a local network using satellite.

Therefore, it makes sense to invest in such ad hoc networks, where networks can be built on the fly. Here, a network can be built in minimum time and with virtually very little cost. Data transfer within the network is virtually free of cost, as no public resources are consumed. If proper security mechanism is put in place, with encryption of data and proper authentication of devices, then security will also be high, as no public network is utilized.

2. **Emergency and Rescue Operations:** In the event of any calamity, natural or otherwise, such as floods, cyclone, earthquake, fire, accident, mishap, etc., ad hoc networks are the most preferable. In such cases, an effective communication is required and often at remote places. Existing infrastructure, if any, may have been destroyed during the calamity, or simply may not be available at all. Therefore, ad hoc networks become the apt choice and can be a boon. Such networks can be deployed and operated on the fly.

3. **Conferences and Meetings:** Consider a scenario where a group of persons collaborate for an event such as conference, business meeting, social gathering, etc. One option to connect them all would be to schedule the event at a designated place, with all networking facilities like access points or wired connections. However, such restrictions, incur high costs and limit the venue to specific destinations. A more favorable solution might be to use an ad hoc network instead. No dedicated infrastructure is required and such gatherings can even be conducted informally at places like lawns, open spaces, etc.
4. **Business Promotion at Malls/ Restaurants/Cafes:** It is possible for such service providers to offer their information on peer to peer networks, doing away with traditional information sharing through paper. Malls can offer dynamic information with respect to type of shops, their location and the products they offer. This information may be available, on their portable devices such as mobiles, tabs or laptops. Restaurants and shops can offer detailed information about their menus, products, etc. electronically, to their users.
5. **Smart Devices:** Ad hoc networks can be used to build smart devices. Think of a situation, where we send a simple message to control AC temperature, washing machine or to simply switch on television or geyser. It is easily possible if the device has appropriate interface for receiving radio signals from ad hoc networks.
6. **Personal area Networks:** Ad hoc networks can be easily used to setup personal area networks, where different users can freely exchange messages, files, data, etc.
7. **Classroom Setup:** Information, study material and other data can be exchanged conveniently, in a classroom setup. It is a boon for virtual classroom environment.
8. **Toll Plazas and Inter-Vehicular Communication:** Ad hoc networks can be utilized for applications such as paying of toll at toll plazas without stopping. They can also be used to setup inter-vehicular communication system on designated paths, such as a highway.

There are many other applications where ad hoc networks could be put to use very effectively. This list is endless. These applications would evolve, as ad hoc networks find their way commercially.

III. Advantages and ROI

MANETs do not require any fixed infrastructure for their implementation, unlike cellular networks and wi-fi networks, where base stations and hotspots are required. No such infrastructure is required for ad hoc networks. Here the network is built on the fly between different nodes wanting to communicate. Also, the nodes are free to move around due to their wireless nature. This reduces the cost of cabling and expensive maintenance. Therefore, ad hoc networks can be built with very low costs and can be a boon for spread of communication. MANETs offer several advantages over other networks. It makes a sound business sense, to invest in ad hoc networks, given the array of benefits, they offer. The investment cost of setting up ad hoc networks is minimal and includes only the cost of mobile devices fitted with a transceiver. Such devices are readily available and cost only a few thousand rupees.

Advantages of ad hoc networks:

- High security can be achieved, due to non use of any public network.
- Virtually free data transfer within the network. There is no limit or cost of any data exchange.
- Flexibility and ease of operation, as nodes are mobile.
- Virtually maintenance-free, as no cabling is required.
- Self-adaptable and self-configuring network.
- Low cost of implementation. Only cost is the cost of the mobile devices.
- On the fly configuration and deployment.
- No administration or running costs.
- Network is scalable, which can support upto hundreds of nodes.

IV. Building a Mobile Ad Hoc Network

We only require mobile nodes that will be a part of ad hoc network. No extra infrastructure, cables, routers are required. Each node should have some processing capability and must be fitted with a transmitter and a receiver. Each node has a transmission range and works in a frequency band ranging between 2 GHz to 5 GHz. Nodes can discover their neighbors by sending simple Hello messages. All nodes receiving the message respond by sending Acknowledgements.

V. Routing Issues in MANETs

Routing is the process of establishing routes between source and destination, in the dynamic ad hoc networks. Ad hoc network is a hop to hop network i.e., the network works by nodes forwarding the messages not intended for themselves. This means that every node also acts as a router, forwarding messages of other nodes as well. Each node has a communication range and communicates with other nodes in its vicinity, within this range. Once every node detects its neighbors, the topology of network can easily be built. This topology information is recorded in form of tables, where every node records path to other nodes. This path is then utilized to send to send data packets to a destination. Updation of these paths is required, whenever nodes move and the topology changes.

The routing decisions in MANETs, face considerable challenges, due to the characteristics and constraints of MANETs [13] [4]. Significant resources are consumed in the route discovery process. As the nodes are mobile, these routes have to be updated dynamically. MANET routing protocols are classified into three categories based on how routing information is acquired and maintained by the mobile nodes [13]. These are proactive routing, reactive routing and hybrid routing.

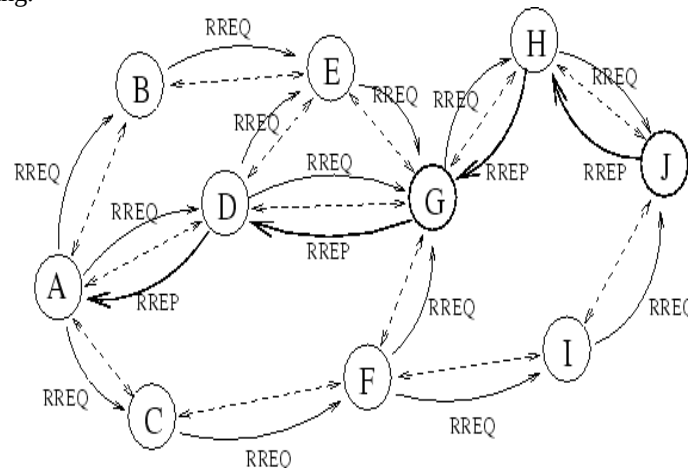


Fig. 2: An example of Routing process in ad hoc networks

- **Proactive routing:** Proactive routing protocols are also called table driven routing protocols. Using a proactive routing protocol, nodes in a mobile Ad-hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one. However, there are considerable overheads associated with them, as there is a need to continuously update the path. Some well known protocols under this category include Destination Sequenced Distance Vector Routing (DSDV) and Optimized Link State Routing Protocol (OLSR).
- **Reactive routing:** Reactive routing protocols for mobile Ad-hoc networks are also called on-demand routing protocols. Reactive routing protocols do not update the routing tables periodically through advertisement messages. Routing in reactive protocols preformed in two phases, route discovery phase and route maintenance phase. When a source node wants to communicate with destination node, firstly it checks for entry to the destination in its routing table. Then it starts sending data to the destination. If the source node is not able to find an entry to the destination in routing table, it starts the route discovery process by broadcasting a route request packet to its neighbors. Those Neighbors having route to the destination responds with sending a route reply to the source node. Routes may be disconnected due to the node mobility. In that case failure link's downstream node informs the failure notification to the source node. Some important Reactive protocols are Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector Routing (AODV) and Location Aided Routing (LAR).
- **Hybrid routing:** Hybrid routing protocols are proposed to combine the merits of both proactive and reactive routing protocols and overcome their shortcomings. Normally, hybrid routing protocols for mobile Ad-hoc networks exploit hierarchical network architectures. Proper proactive routing approach and reactive routing approach are exploited in different hierarchical levels. Nodes within a certain distance from the node concerned or within a particular geographical region are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For routing between nodes, that are located in different zones, a reactive, on-demand approach is used. Zone Routing Protocol (ZRP) is a famous hybrid routing protocol.

VI. Security Issues in Ad Hoc Networks

Security is a major concern in ad hoc networks. Due to wireless nature of the medium, chances of a node intruding into valid space of an ad hoc network, is always present. If a node intrudes into ad hoc network and intercepts important information, then security of whole network is compromised. Wireless medium, in addition to scarce resources of ad hoc networks, such as limited battery power and dynamic topology, make detecting all

threats, a real challenge. The objective of secure routing is to detect any malicious nodes within the network and block it. Therefore, it becomes utmost essential to use a robust encryption method, for all messages. This way, even if a message is intercepted, the chances of reading it meaningfully are really slim. Another important requirement is appropriate authentication of each node in the network, so that a malicious node is easily identified. Attacks on ad hoc networks are classified as either active or passive.

Passive Attacks: A passive attack does not disrupt normal operation of network. The attacker simply intercepts the data without altering it. Passive attacks are very difficult to detect, as the attacker does not harm the network in any way. But security of whole network is compromised, as the attacker, has access to vital information.

Active Attacks: An active attack disrupts normal functioning of network by altering or modifying data being exchanged. In active attack, the intruder can be internal or external. External attack means that the compromised node is not a part of the network, while internal attack means that the node is a part of the network. Internal attacks are harder to predict and control as the malicious node is a part of the network and receives all messages. Some of the common attacks in ad hoc networks are:

- **Wormhole Attack:** In wormhole attack, a malicious node collects packets at one end of network and tunnels them to another location in the network, from where they are again injected back into the network. This tunnel may be created using either wired or wireless link. This tunnel may divert packets to other location, away from the intended receiver.
- **Black Hole Attack:** In black hole attack, a malicious node advertises itself as having shortest path to a destination, when a Route Request is generated. As a result, the origin believes that there exists a shortest path, through this malicious node and sends all data packets to it. This malicious node can then affect the network by performing malicious activities, such as dropping of packets or changing contents of packets, etc.
- **Byzantine Attack:** Here, one or more nodes collude to reduce performance of network by either creating routing loops, or routing packets on paths that are not optimal or dropping some packets.
- **Denial of Service Attacks:** Here the attacker intends to disrupt availability of some service. As a result, the network does not perform normally and degrades. The service which could be blocked could be from any layer. E.g. services that network layer provides to upper layers may be stopped, by malicious node simply by participating in routing process and creating false entries in routing tables or routing table overflow.
- **Routing Attacks:** Here, the malicious node disrupts normal routing process by creating false routing information. Here the node may either create non-valid paths or enter them in routing tables, or alternately it may replicate packets. Replication of packets may consume precious bandwidth and energy of nodes by stale packets. There can be many other ways in which a malicious node can affect the routing process and disrupt services.

There exist many other types of attacks, which can be triggered. Using a robust security mechanism, most of these attacks can be prevented or reduced.

VII. Conclusion

Ad hoc networks are still in their infancy and their potentials are yet to be realized. Many challenges exist for building successful applications around ad hoc networks. But the advantages associated like mobility, flexibility, lack of infrastructure, fast deployment, decentralized control and low cost, far outweigh their limitations. There is little doubt that they will be an integral part of all future networks, where they will connect seamlessly with other networks such as the Internet, Cellular networks, etc. Many new and exciting applications based upon ad hoc networks are expected in the years to come. Work is already in progress to make efficient algorithms for varying requirements and many solutions are already available. But answers of many questions like Universal addressing, connectivity with other networks, foolproof security mechanisms, control mechanisms, etc. are yet to be realized effectively. There is a need to continuously enhance existing solutions for routing, security and decentralized control, to pave the way for their successful adoption.

References

- [1] C. Siva Ram Murthy, B.S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall, 2004.
- [2] S. Corson and J. Macker, "Mobile Ad-hoc networking: Routing protocol performances and evaluation considerations", In RFC 2501, 1999.
- [3] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication, IJCSS, vol. 4, pp 265-274.
- [4] Imrich Chlamtac, Marco Conti, Jennifer J. Liu, "Mobile ad hoc networking: imperatives and challenges", *Ad hoc networks* (Elsevier), vol.1, pp 13-64, 2003.
- [5] Comer D.E. *Internetworking With TCP/IP Volume I: Principles, Protocols, and Architectures*, fourth edition, 2000.
- [6] C. Toh, "Challenges in MANET", *IEEE Communication*, 2001.
- [7] S. Corson and J. Macker, "Mobile Ad-hoc networking: Routing protocol performances and evaluation considerations", In RFC 2501, 1999.
- [8] Subir Kumar Sarkar, T. G. Basavaraju, C. Puttamadappa, "Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications", CRC Press, 2007.