Mobile Ad Hoc Networking: Imperatives and Challenges

Sonarka Maini, Saurabh Jakhmola
Information Technology
Dronacharya College Of Engineering

***Abstract*- A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. It represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ''ad-hoc'' network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. Ad hoc networking concept is not a new one, having been around in various forms for over 20 years. Traditionally, tactical networks have been the only communication networking application that followed the adhoc paradigm. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET.So,we would like to propose the challenges and imperativels that the MANET is facing.**

***Index Terms*- Adhoc Network, Bluetooth, 4G, Routing, Security, Performance evaluation .**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".[1]

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 forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

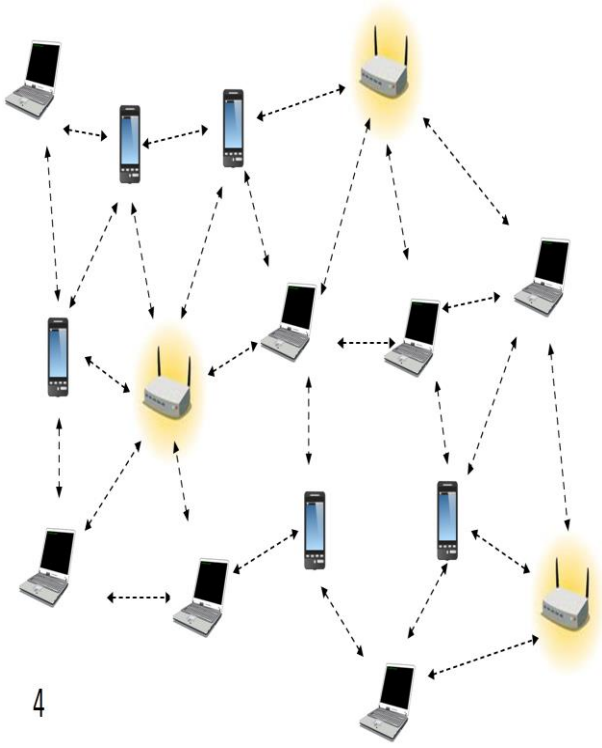
MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

The growth of laptops and 802.11/Wi-Fi wireless networking have 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 measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other.

The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

An Ad-hoc network is a collection of wireless mobile nodes which dynamically forming a temporary network without the aid of any established infrastructure or centralized administration.



There are, furthermore, 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.

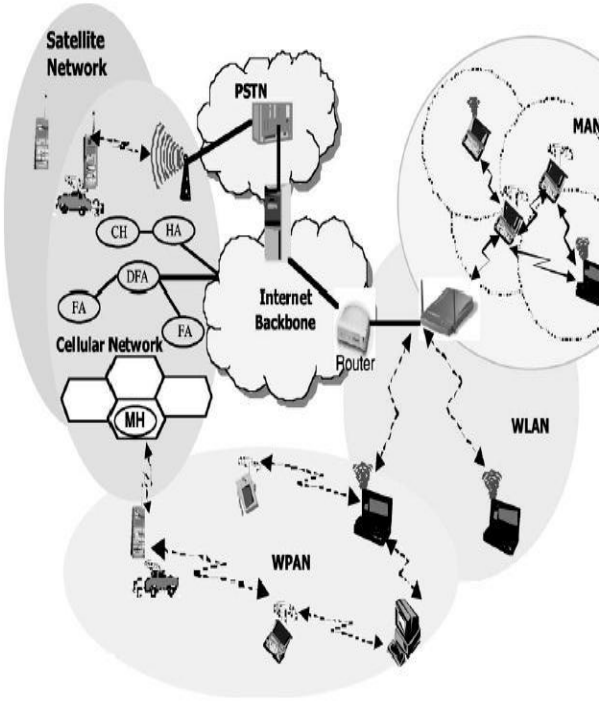
Inside the ad hoc networking field, wireless sensor networks take a special role. A sensor network is composed of a large number of small sensor nodes, which are typically densely (and randomly) deployed inside the area in which a phenomenon is being monitored. Wireless ad hoc networking techniques also constitute the basis for sensor networks. However, the special constraints imposed by the unique characteristics of sensing devices, and by the application requirements, make many of the solutions designed for multi-hop wireless networks (generally) not suitable for sensor networks. This places extensive literature dedicated to sensor networks beyond the scope of this paper; however, the interested reader can find an excellent and comprehensive coverage of sensor networks in a recent survey. This paper demonstrates the impetus behind mobile ad hoc networks, and presents a representative collection of technology solutions used at the different layers of the network.

II. AD HOC NETWORKING AND 4G

A major goal toward the 4G Wireless evolution is the providing of pervasive computing environments that can seamlessly and ubiquitously support users in accomplishing their tasks, in accessing information or communicating with other users at anytime, anywhere, and from any device. In this environment, computers get pushed further into background; computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves in our presence to find the information or software we need. The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the environment, without requiring any major change in the users behavior. This new philosophy is the basis of the Ambient Intelligence concept. The objective of ambient intelligence is the integration of digital devices and networks into the everyday environment, rendering accessible, through easy and ‘‘natural’’ interactions, a multitude of services and applications. Ambient intelligence places the user at the center of the information society. This view heavily relies on 4G wireless and mobile communications. 4G is all about an integrated, global network, based on an open systems approach. Integrating different types of wireless networks with wire-line backbone network seamlessly, and convergence of voice, multimedia and data traffic over a single

IP-based core network are the main foci of 4G. With the availability of ultra-high bandwidth of up to 100 Mbps, multimedia services can be supported efficiently; ubiquitous computing is enabled with

enhanced system mobility and portability support, and location-based services.



III. Evolution of MANET

In 1970, Normanl Abramson and his fellow researchers at the University of Hawaii invented ALOHA net. In 1972 DARPA Packet Radio Network (PR Net) In 1980 Survivable Radio Networks (SURAN).During 1980 emergence of Internet Emerging Task Force (IETF), termed the mobile ad hoc networking group. In 1994 emergence of Bluetooth by Ericsson.

IV. Characteristics of MANET

- Network is not depend on any fix infrastructure for its operation.
- Ease of deployment
- Speed of deployment
- Dynamic Changing Topology of nodes
- Multi-hop network
- Each node is working as intelligent node
- Not any mediator networking device is required for communications
- Each node is work as a DTE (Data Terminal Equipment) and DCE (Data Communication Equipment)

V. AD-HOC APPLICATIONS

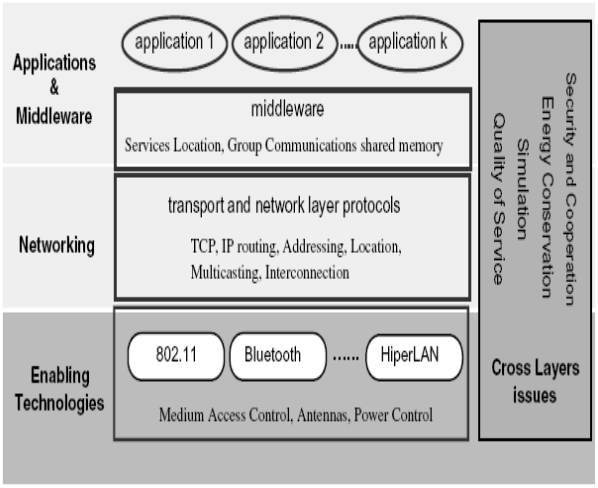
- Tactical networks : Military Communication automated Battle fields
- Sensor Network: Remote weathers for sensors, earth activities
- Emergency Services : Disaster recovery, earthquakes, crowd control and commando operations
- Educational Applications : Setup virtual class & conference rooms
- Entertainment : Multi-user games, robotics pets.
- Location Aware Services : Automatic Call forwarding, advertise location specific services, Location–dependent travel guide.

In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain. To present the huge amount of research activities on ad hoc networks in a systematic/organic way, we will

use, as a reference, the simplified architecture shown in as shown in the figure, the research activities will be grouped, according to a layered approach into three main areas:

• Enabling technologies;
• Networking;
• Middleware and applications.

MANET Architecture



In addition, as shown in the figure, several issues (energy management, security and cooperation, quality of service, network simulation) span all areas, and we discuss them separately.

Ad hoc networks can be classified, depending on their coverage area, as : Body (BAN), Personal (PAN), Local (LAN),Metropolitan (MAN) and Wide(WAN) area networks. Ad-hoc

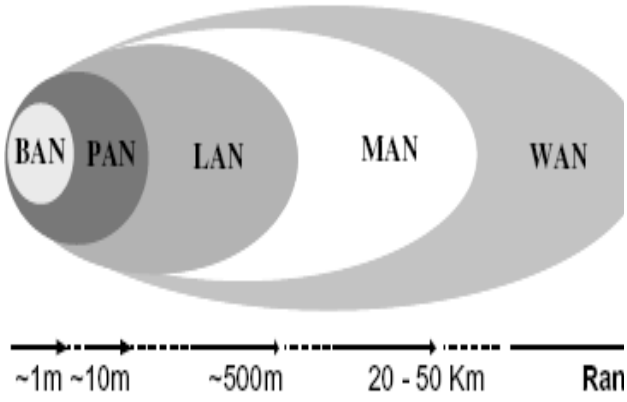
Single hop

BAN, PAN and LAN wireless technologies are already common on the market, these technologies constituting the building blocks for constructing small, multi-hop, ad hoc networks that extend their range over multiple radio hops. For these reasons, BAN, PAN

and LAN technologies constitute the Enabling technologies for ad hoc networking.

The success of a network technology is connected to the development of networking products at a competitive price. A major factor in achieving this goal is the availability of appropriate networking standards. Currently, two main standards are emerging for ad hoc wireless networks: the IEEE 802.11 standard for WLANs, and the Bluetooth specifications 3 for short-range wireless communications.

VI. BLUETOOTH



The Bluetooth technology is a de-facto standard for low-cost ,short-range radio links between mobile PCs, mobile phones, and other portable devices. The Bluetooth Special Interest Group (SIG)releases the Bluetooth specifications. Bluetooth specifications were

established by the joint effort from over two thousand industry leading companies including 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, Toshiba, etc. under the umbrella of Bluetooth SIG. In addition, the IEEE 802.15 Working Group for

Wireless Personal Area Networks approved its first WPAN standard derived from the Bluetooth Specification. The IEEE 802.15.1 standard is based on the lower portions of the Bluetooth specification.

A Bluetooth unit, integrated into a microchip, enables wireless ad hoc communications, of voice and data between portable and/or fixed electronic devices like computers, cellular phones, printers, and digital cameras. Due to its low-cost target, Bluetooth

microchips may become embedded in virtually all consumer electronic devices in the future.

VII. SECURITY ATTACKS

Securing wireless ad hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Ad hoc networks have to cope with the same kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the adhoc context The complexity and diversity of the field (different applications have different security constraints) led to a multitude of proposals that cannot be all surveyed in this article. Detailed analyses of ad hoc networking security issues and solutions can be found in. Below we summarize only the main directions of security in ad hoc networks. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network.

These attacks can be grouped in: Impersonation, Denial of service and Disclosure attack.

Secure routing : Secure routing protocols cope with malicious nodes that can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. Recent studies brought up also a new type of attack that goes under the name of wormhole attack mentioned earlier.

Cooperation enforcing : A basic requirement for keeping an ad hoc network operational is to enforce

ad hoc nodes contribution to basic network functions such as packet forwarding and routing. Unlike networks using dedicated nodes to support basic network functions including packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This difference is at the core of some of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. For example, routing is vulnerable in ad hoc networks because each device acts as a router. Forwarding mechanism is cooperative, as well. Communications between nodes, more than 1-hop away, are performed by exploiting intermediate relaying nodes. A node that does
not cooperate is called a misbehaving node. Routing–forwarding misbehaviors can be caused
by nodes that are malicious or selfish. A malicious node does not cooperate because it wants to intentionally damage network functioning by dropping packets. On the other hand, a selfish node does not intend to directly damage other nodes, but is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects *IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010* 157 others to forward packets on its behalf. Such a node uses the network but does not cooperate.

VIII. SIMULATION AND PERFORMANCE EVALUATION

There are two main approaches in system performance evaluation: the first uses measurements; the second is based on a representation of the system behavior via a model Measurement techniques are applied to real systems, and thus they can be applied only when a real system, or a prototype of it, is available. Currently, only few measurements studies on real ad hoc testbeds can be found in the literature. The Uppsala University APE testbed is one of the largest, having run tests with more than thirty nodes .The results from this testbed are very important as they are pointing out problems that were not detected by preceding simulation studies.

An important problem, related to the different transmission ranges for 802.11b control and data frames, is the so-called communication gray zones problem. This problem was revealed by a group of researchers at the Uppsala University, while measuring the performance of their own implementation of the AODV routing protocol in an IEEE 802.11b ad hoc network. Observing an unexpected large amount of packets_ losses, mainly during route changes, it was found that increase in packet loss occurred in some specific geographic areas termed called ‘‘communication gray zones’’. In such zones, the packet loss experienced by a station may be extremely high, up to 100%, thus severely affecting the performance of applications associated with a continuous packet flow (e.g., file transfers and multimedia streaming). It was also found that the reason for this phenomenon is that a station inside a gray zone is considered (using the routing information) reachable by a neighboring station, while actual data communication between the stations is not possible. The same problem was found to affect other routing protocols, such as OLSR. It is important to point out that communication gray zone problem cannot be revealed by commonly used simulation tools (e.g., NS-2, Glomosim), as in these 802.11 models both unicast and broadcast transmissions are performed at 2 Mbps, and hence have the same transmission range. Constructing a real ad hoc network test bed for a given scenario is typically expensive and remains limited in terms of working scenarios, mobility models, etc. Furthermore, measurements are generally non-repeatable. For these reasons, protocols scalability, sensitiveness to users mobility patterns and speeds are difficult to investigate on a real test bed. Using a simulation or analytic model, on the other hand, permits the study of system behavior by varying all its parameters, and considering a large spectrum of network scenarios.

Evaluating system performance via a model consists of two steps: (i) defining the system model, and (ii) solving the model using analytical and/or simulative techniques. Analytical methods are often not detailed enough for the ad hoc networks evaluation and in terms of accounting for mobility, in their infancy. On the other hand, simulation modeling is a more standardized, mature, and flexible tool for modeling various protocols and network scenarios, and allows (by running the simulation model) collection and

analyses that fully characterize the protocol performance in most cases.

Mobility models : The ability of ad hoc networks protocols to correctly behave in a dynamic environment, where devices position may continuously change, is a key issue.

Network simulators : Most MANET simulative studies are based on simulation tools. The main advantage of these tools is that they provide libraries containing predefined models for most communication protocols.

IX. QUALITY OF SERVICE

Providing Quality of Service (QoS), other than best effort, is a very complex problem in MANETs, and makes this area a challenging area of future MANET research. Network_ ability to provide QoS depends on the intrinsic characteristics of all the network components, from transmission links to the MAC and network layers. MANET characteristics generally lead to the conclusion that this type of network provides a weak support to QoS. Wireless links have a (relatively) low and highly variable capacity, and high loss rates. Topologies are highly dynamic with frequent links breakages. Random access-based MAC protocols, which are commonly used in this environment (e.g., 802.11b), have no QoS support. Finally, even after resource reservation, QoS still cannot be guaranteed due to the frequent disconnections and topology changes. Several QoS routing algorithms were published recently with a variety of QoS requirements and resource constraints, for example, CEDAR, ticket-based probing, Predictive Location-Based QoS Routing, Localized QoS routing and QoS routing based on bandwidth calculation.

X. CONCLUSIONS

In coming years, mobile computing will keep flourishing, and an eventual seamless integration of MANET with other wireless networks, and the fixed Internet infrastructure, appears inevitable. Ad hoc networking is at the center of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self-administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community. In moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology.

Finally, I would like to state that in the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Since network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-hoc Networks. So, it becomes the best solution of different problems of network.

REFERENCE

[1] J. Ahola, Ambient Intelligence, ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, October 2001.

[2] Ahuja et al., Performance of TCP over different routing protocols in mobile ad-hoc networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC 2000), Tokyo, Japan, May 2000.

[3] B. Kalaavathi, et. Al, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1470874Raj Kamal, Mobile Computing, Oxford University Press, 2009.

[4] Proceedings IT in Academics, Sinhgad Institute of Management, Pune, India, 2009.

[5] G. Anastasi, M. Conti, E. Gregori, A. Passarella, A power saving architecture for web access from mobile computers, in: Proceedings of the Networking 2002, Lecture Notes in Computer Science, vol. 2345, Springer, Berlin, 2002.

[6] S. Basagni, Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks, in: Proceedings of the IEEE Vehicular Technology Conference (VTC) 1999, Amsterdam, The Netherlands, September 19–22, 1999.

[7] C. Bisdikian, An overview of the Bluetooth wireless technology, IEEE Communication Magazine, December 2001.