Abstract
This entry presents an overview of wireless networks and different aspects of mobile ad hoc network (MANET). The applications of MANETs are described with examples and how those applications work with different environments. Characteristic features are described. This entry also briefly covers the classification of MANETs.

INTRODUCTION
Wireless industry has seen exponential growth in the last few years. The advancement in growing availability of wireless networks and the emergence of handheld computers, personal digital assistants (PDAs), and cell phones is now playing a very important role in our daily routines. Surfing Internet from railway stations, airports, cafes, public locations, Internet browsing on cell phones, and information or file exchange between devices without wired connectivity are just a few examples. All this ease is the result of mobility of wireless devices while being connected to a gateway to access the Internet or information from fixed or wired infrastructure (called infrastructure-based wireless network) or ability to develop an on-demand, self-organizing wireless network without relying on any available fixed infrastructure (called ad hoc networks). A typical example of the first type of network is office wireless local area networks (WLANs), where a wireless access point serves all wireless devices within the radius. An example of mobile ad hoc networks (MANETs)\(^1\) can be described as a group of soldiers in a war zone, wirelessly connected to each other with the help of limited battery-powered devices and efficient ad hoc routing protocols that help them to maintain quality of communication while they are changing their positions rapidly. Therefore, routing in ad hoc wireless networks plays an important role of a data forwarder, where each mobile node can act as a relay in addition to being a source or destination node.

WIRELESS NETWORKS
Wireless networks can be broadly categorized into two classes: infrastructure-based wireless networks and infrastructure-less wireless networks (ad hoc wireless networks). Infrastructure-based wireless networks rely on an access point, which is a device that acts as a bridge between the wired and wireless networks. With the help of such an access point, wireless nodes can be connected to the existing wired networks. Examples of infrastructure-based wireless networks are wireless networks set up in airports, offices, homes, and hospitals, where clients connect to the Internet with the help of an access point. Fig. 1 shows an infrastructure mode wireless network.

The other type of wireless networks does not rely on fixed infrastructure, and it is more commonly called an ad hoc wireless network. The word ad hoc can be translated as “improvised” or “not organized,” which often has a negative meaning; however, in this context the sense is not negative, but it only describes the dynamic network situation. An ad hoc mode is used to connect wireless clients directly together, without the need for a wireless access point or a connection to an existing wired network. There are different examples of MANET in ad hoc mode such as building-to-building, vehicle-to-vehicle, ship-to-ship, etc.; they communicate with each other by relying on peer-to-peer routing. A typical ad hoc mode wireless network is shown in Fig. 2.

In wireless network communication, nodes communicate with other nodes via wireless channels. There are two important metrics that are used in the wireless networks: spectrum ranges and different radio frequencies. For example, IEEE 802.11a\(^2\) IEEE 802.11b\(^3\) and IEEE 802.11g\(^4\) use a radio frequency of 5.15–5.35, 2.4–2.58, and 2.4–2.58 GHz, respectively. The signal
strength in a wireless medium decreases when the signal travels further beyond a certain distance, and it reduces to the point where reception is not possible. Several medium access (MAC) layers are used in wireless networks to control the use of the wireless medium: Bluetooth MAC layer 802.15 and WLAN MAC layer 802.11. The topology of the wireless network can be different with time because of the mobility feature. Besides the concept of mobility, another type of mobility is defined and well-studied. For example, in wireless networks, the hosts or subnets may be moved from one place to another. Traditional networks require reconfiguration of the IP address used by these hosts or subnets at the new place. A network enabled with mobile IP allows these hosts or subnets to move without any manual IP address reconfiguration. The hosts can remain connected while they are moving around.

**MOBILE AD HOC NETWORK**

A wireless ad hoc network is a collection of two or more wireless devices having the capability to communicate with each other without the aid of any centralized administrator. Each node in a wireless ad hoc network functions as both a host and a router. The network topology is in general dynamic because the connectivity among nodes may vary with time due to node mobility, node departures, and new node arrivals. Hence, there is a need for efficient routing protocols to allow the nodes to communicate.

Ad hoc nodes or devices should be able to detect the presence of other such devices so as to allow communication and information sharing. Besides that, it should also be able to identify types of services and corresponding attributes. Since the number of wireless nodes changes on the fly, the routing information also changes to reflect changes in link connectivity. Hence, the topology of the network is much more dynamic and the changes are often unpredictable as compared to the fixed nature of existing wired networks.

The dynamic nature of the wireless medium, fast and unpredictable topological changes, limited battery power, and mobility raise many challenges for designing a routing protocol. Due to the immense challenge in designing a routing protocol for MANETs, a number of developments focus on providing an optimal solution for routing. However, a majority of these solutions attain a specific goal (e.g., minimizing delay and overhead) while compromising other factors (e.g., scalability and route reliability). Thus, an optimal routing protocol that can cover most of the applications or user requirements as well as cope up with the stringent behavior of the wireless medium is always desirable.

However, there is another kind of MANET nodes called the fixed network, in which the connection between the components is relatively static; the sensor network is the main example for this type of fixed network. All components used in the sensor network are wireless and deployed in a large area. The sensors can collect the information and route data back to a central processor or monitor. The topology for the sensor network may be changed if the sensors lose power. Therefore, the sensors network is considered to be a fixed ad hoc network.

Each of the nodes has a wireless interface and communicates with each other over either radio or infrared frequency. Laptop computers and PDAs that communicate directly with each other are some examples of nodes in an ad hoc network. Nodes in the ad hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet. Semi-mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily. Fig. 3 shows a
simple ad hoc network with three nodes. The outermost nodes are not within the transmitter range of each other. However, the middle node can be used to forward packets between the outermost nodes. Node B is acting as a router and nodes A, B, and C have formed an ad hoc network.

An ad hoc network uses no centralized administration. This ensures that the network would not collapse just because one of the mobile nodes moves out of the transmitter range of the other nodes. Nodes should be able to enter or leave the network as they wish. Because of the limited transmitter range of the nodes, multihops may be needed to reach other nodes. Every node wishing to participate in an ad hoc network must be willing to forward packets to other nodes. Thus, every node acts both as a host and as a router. A node can be viewed as an abstract entity consisting of a router and a set of affiliated mobile hosts. A router is an entity that, among other things, runs a routing protocol. A mobile host is simply an IP-addressable host or entity in the traditional sense.

Ad hoc networks are also capable of handling topology changes and malfunctions in nodes. They are fixed through network reconfiguration. For instance, if a node leaves the network and causes link breakages, affected nodes can easily request new routes and the problem will be solved. This will slightly increase the delay, but the network will still be operational.

**MOBILE AD HOC NETWORK HISTORY**

The history of wireless networks dates back to 1970s, and the interest has been growing ever since. Since the turn of the century, the interest has almost exploded, probably because of the fast-growing Internet. The tremendous growth of personal computers and the handy usage of mobile devices necessitate the need for ad-hoc connectivity.

The first generation goes back to 1972. At the time they were called PRNET (packet radio network). In conjunction with ALOHA (areal locations of hazardous atmospheres), approaches for MAC control and a type of distance vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad hoc networks emerged in 1980s, when the ad hoc network was further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) project that aimed at providing ad hoc networking with small, low-cost, low-power devices with efficient protocols for improved scalability and survivability. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure.

In the 1990s, the concept of commercial ad hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

The IEEE 802.11 subcommittee had adopted the term “ad hoc networks” and the research community had started to look into the possibility of deploying ad hoc networks in other areas of application. Meanwhile, work was going on to advance the previously built ad hoc networks. Global mobile information systems (GloMo) and the NTDR (near-term digital radio) are some of the results of these efforts. GloMo was designed to provide an office environment with Ethernet-type multimedia connectivity anywhere and anytime in handheld devices.

**MOBILE AD HOC NETWORK DEFINITION**

A clear definition of precisely what is meant by an ad hoc network is difficult to identify. In today’s scientific literature, the term “ad hoc network” is used in many different ways. There are many different definitions that describe ad hoc networks, but only three are presented here. The first one is given by the Internet Engineering Task Force group, the second one is given by National Institute of Standard and Technology, and the final definition is given by the INTEC Research group.

In MANETs, the wireless nodes are free to move and still connected using the multihop with no infrastructure support. The goal of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Ad hoc 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, and conventions in which a person wishes to make a quick connection for sharing information.

**MANET APPLICATIONS AND SCENARIOS**

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance because of its increasing number of widespread applications. Ad hoc networking can be applied anywhere at anytime without infrastructure and its flexible networks. Ad hoc networking allows the devices to maintain connections to the network as well
as easily adds and removes devices to and from the network. The set of applications of MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks to small and static networks that are constrained by limited power. Besides the legacy applications that move from traditional infrastructure environment to the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include the following:

- **Military battlefield:** Military equipment now routinely contains some sort of computer equipment. Ad hoc networking can be very useful in establishing communication among a group of soldiers for tactical operations and also for the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. Ad hoc networks also fulfill the requirements of communication mechanism very quickly because ad hoc network can be set up without planning and infrastructure, which makes it easy for the military troops to communicate with each other via the wireless link. The other important factor that makes MANET very useful and lets it fit in the military base is the fact that the military objects, such as airplanes, tanks, and warships, move at high speeds, and this application requires MANET’s quick and reliable communication. Because of the information that transfers between the troops, it is very critical that the other side receives secure communication, which can be found through ad hoc networks. At the end, the primary nature of the communication required in a military environment enforced certain important requirements on ad hoc networks, such as reliability, efficiency, secure, and support for multicast routing. Fig. 4 shows an example of the military ad hoc network.

- **Commercial sector:** The other kind of environment that uses an ad hoc network is emergency rescue operation. The ad hoc form of communications is especially useful in public-safety and search-and-rescue applications. Medical teams require fast and effective communications when they rush to a disaster area to treat victims. They cannot afford the time to run cabling and install networking hardware. The medical team can employ ad hoc networks (mobile nodes) such as laptops and PDAs and can communicate via the wireless link with the hospital and the medical team on-site. For example, a user on one side of the building can send a packet destined for another user on the far side of the facility, well beyond the point-to-point range of WLAN, by having the data routed from client device to client device until it gets to its destination. This can extend the range of the WLAN from hundreds of feet to miles, depending on the concentration of wireless users. Real-time communication is also important since the voice communication predominates data communication in such scenarios. Fig. 5 shows the ad hoc search-and-rescue application.

- **Local level:** Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at conferences, at meetings, or in classrooms. Another appropriate local level application might be in home networks, where devices can communicate directly to exchange information. Similarly, in other civilian environments such as taxicab, sports stadium, boat, and small aircraft, mobile ad hoc communications will have many applications.

- **Personal area network (PAN):** It is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 m. For example, a person traveling with a laptop, a PDA, and a portable printer could interconnect them without having to plug anything in by using some form of wireless technology. Typically, this type of PAN could also be interconnected without wires to the Internet or other networks. A wireless personal area network (WPAN) is virtually a synonym of PAN since almost any PAN would need to function wirelessly. Conceptually, the difference between a PAN and a WLAN is that the former tends to be centered around one person while the latter is a local area network (LAN) that is connected without wires and serve multiple users.
Bluetooth is an industrial specification for WPANs. A Bluetooth PAN is also called a piconet and is composed of up to eight active devices in a master–slave relationship (up to 255 devices can be connected in the “parked” mode). The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet has a range of 10 m that can reach up to 100 m under ideal circumstances, as shown in Fig. 6.

The other usage of the PAN technology is that it could enable wearable computer devices to communicate with nearby computers and exchange digital information using the electrical conductivity of the human body as a data network. Some concepts that belong to the PAN technology are considered in research papers, which present the reasons why those concepts might be useful:

- Small size of the device
- No need for huge power (lower power requirements)
- Not expensive
- Used specially for bodies and for sensitive information
- No methods for sharing data
- Networking can reduce function of input/output
- Allow new conveniences and services

**AD HOC NETWORK CHARACTERISTICS**

MANETs have the following features that are necessary to consider while suggesting or designing solutions for these types of networks:

- MANET has a feature of distributed operation because in MANET each node operates independently and there is no centralized server or computer to manage this network. Instead this job is distributed among all operating nodes. Each node works with another node in cooperation to implement functions such as security and routing.
- MANETs have lower bandwidth capacity as compared with wired networks. MANETs can experience a problem of bit error rate and lower bandwidth capacity because end-to-end link paths are used by several nodes in the network. Also, the channel used for communication can be affected by other factors such as fading and interference.
- Another feature of MANET that can be used is energy in mobile devices. As all mobile devices will get their energy from batteries, which is a limited resource, whatever energy the mobile nodes have, it has to be used very efficiently.
- Security is the most important concern in MANETs because the nodes and the information in MANETs are not secured from threats, for example, denial of service attacks. Also, mobile devices imply higher security risks compared with fixed operating devices, because portable devices may be stolen or their traffic may insecurely cross wireless links. Eavesdropping, spoofing, and denial of service attacks are the main threats for security.
- In MANETs the network topology is always changing because nodes in the ad hoc network change their positions randomly as they are free to move anywhere. Therefore, devices in a MANET should support dynamic topology. Each time the mobility of node causes a change in the topology and hence the links between the nodes are always changing in a random manner. This mobility of nodes creates frequent disconnection; hence, to deal with this problem the MANET should adapt to the traffic and transmission conditions according to the mobility patterns of the mobile network nodes.
- A MANET includes several advantages over wireless networks, including ease of deployment, speed of deployment, and decreased dependences on a fixed infrastructure. A MANET is attractive because it provides an instant network formation without the presence of fixed base stations and system administration.

**CLASSIFICATION OF AD HOC NETWORKS**

There is no generally recognized classification of ad hoc networks in the literature. However, there is a classification on the basis of the communication procedure (single hop/multihop), topology, node configuration, and network size (in terms of coverage area and the number of devices).
Classification According to the Communication

Depending on the configuration, communication in an ad hoc network can be either single hop or multihop.

Single-hop ad hoc network

Nodes are in their reachable area and can communicate directly, as shown in Fig. 7. Single hop ad hoc networks are the simplest type of ad hoc networks where all nodes are in their mutual range, which means that the individual nodes can communicate directly with each other, without any help of other intermediate nodes. The individual nodes do not have to be static; they must, however, remain within the range of all nodes, which means that the entire network could move as a group; this would not modify anything in the communication relations.

Multihop ad hoc network

This class in the literature is the most examined type of ad hoc networks. It differs from the first class in that some nodes are far and cannot communicate directly. Therefore, the traffic of these communication endpoints has to be forwarded by other intermediate nodes. Fig. 8 shows the communication path of far nodes as black lines. With this class also, one assumes that the nodes are mobile. The basic difficulty of the networks of this class is the node mobility, whereby the network topology is subjected to continuous modifications. The general problem in networks of this class is the assignment of a routing protocol. High-performance routing protocols must be adaptive to the fast topology modification.

Classification According to the Topology

Ad hoc networks can be classified according to the network topology. The individual nodes in an ad hoc network are divided into three different types with special functions: flat, hierarchical, and aggregate ad hoc networks.

Flat ad hoc networks

In flat ad hoc networks, all nodes carry the same responsibility and there is no distinction between the individual nodes, as shown in Fig. 9. All nodes are equivalent and can transfer all functions in the ad hoc network. Control messages have to be transmitted globally throughout the network, but they are appropriate for highly dynamic network topology. The scalability decreases when the number of nodes increases significantly.

Hierarchical ad hoc networks

Hierarchical ad hoc networks consist of several clusters, each one represents a network and all are linked together, as indicated in Fig. 10. The nodes in hierarchical ad hoc networks can be categorized into two types:
Master nodes: Administer the cluster and are responsible for passing the data on to the other cluster.

Normal nodes: Communicate within the cluster directly together and with nodes in other clusters with the help of the master node. Normal nodes are also called slave nodes.

One assumes that the majority of communication (control messages) takes place within the cluster and only a fraction between different clusters. During communication within a cluster, no forwarding of communication traffic is necessary. The master node is responsible for the switching of a connection between nodes in different clusters.

The no single point of failure is of great importance for a message to reach its destination. This means that if one node goes down, the rest of the network will still function properly. In the hierarchical approach, this is altogether different. If one of the cluster heads goes down, that section of the network will not be able to send or receive messages from other sections for the duration of the downtime of the cluster head.

Hierarchical architectures are more suitable for low-mobility cases. The flat architectures are more flexible and simpler than hierarchical ones; hierarchical architectures provide a more scalable approach.

Aggregate ad hoc networks

Aggregate ad hoc networks bring together a set of nodes into zones. Therefore, the network is partitioned into a set of zones as shown in Fig. 11. Each node belongs to two levels of topology: low-level (node-level) topology and high-level (zone-level) topology. Also, each node may be characterized by two ID numbers: node ID number and zone ID number. Normally, aggregate architectures are related to the notion of zone. In aggregate architectures, we find both intrazone and interzone architectures, which in turn can support either flat or hierarchical architectures.

Classification According to the Node Configuration

A further classification of ad hoc networks can be performed on the basis of the hardware configuration of the nodes. There are two types of node configurations: homogeneous networks and heterogeneous networks. The configuration of the nodes in a MANET is important and can depend very strongly on the actual application.

Homogeneous ad hoc networks

In homogeneous ad hoc networks, all nodes possess the same characteristics regarding the hardware configuration as processor, memory, display, and peripheral devices. Most well-known representatives of homogeneous ad hoc networks are wireless sensor networks. In homogeneous ad hoc networks, applications can proceed from certain prerequisites; for example, the localization is considerably facilitated by the presence of control components in each node, as shown in Fig. 12.
Heterogeneous ad hoc networks

In heterogeneous ad hoc networks, the nodes differ according to the hardware configuration. Each node has different characteristics, resources, and policies. In ad hoc networks of this class, all nodes cannot provide the same services, as shown in Fig. 13.

Classification According to the Coverage Area

As shown in Fig. 14, ad hoc networks can be categorized, depending on their coverage area, into several classes: body area network (BAN), personal area network (PAN), local area network (LAN), metropolitan area network (MAN), and wide area network (WAN).[13,14] WAN and MAN are mobile multihop wireless networks presenting many challenges that are still being solved (e.g., addressing, routing, location management, and security), and their availability is not on immediate horizon.

A BAN is strongly correlated with wearable computers. The components of a wearable computer are distributed on the body (e.g., head-mounted displays, microphones, and earphones), and a BAN provides the connectivity among these devices. The communicating range of a BAN corresponds to the human body range, i.e., 1–2 m. As wiring around a body is generally cumbersome, wireless technologies constitute the best solution for interconnecting wearable devices. The PAN connects mobile devices carried by users to other mobile and stationary devices, while BAN is devoted to the interconnection of one-person wearable devices. A PAN has a typical communication range of up to 10 m. WPAN technologies in the 2.4–10.6-GHz band are the most promising technologies for the widespread PAN deployment. Spread spectrum is typically employed to reduce interference and utilize the bandwidth.[15]

In the last few years, the application of wireless technologies in the LAN environment has become increasingly important, and WLAN can be found in
different environments such as homes, offices, urban roads, and public places. WLAN, also called wireless fidelity (Wi-Fi), is than the wired LANs. Most of the personal computers, laptops, phones, and PDAs are capable of connecting to the Internet via WLAN. There are five major specifications in the WLAN family 802.11 namely 802.11a, 802.11b, 802.11g, and 802.11n. All use CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) for medium sharing which are standardized in 802.11c, 802.11d, 802.11e, and 802.11f.

WIMAX is based on the 802.16 IEEE standard and defined as a wireless MAN technology that will provide a wireless alternative to wire and digital subscriber line (DSL) for last mile broadband access. WIMAX has a communication range of up to 50 km, which also allows the users to get broadband connections without directly connecting to the base station, and provides shared data rates of up to 70 Mbps, which is enough bandwidth to support more than 60 T1 link and hundreds of home and office DSL connections. Likewise, WIMAX fully supports the quality of service. Finally, the last but not the least wireless technology called mobile broadband wireless access (MBWA) is approved by the IEEE standard board and defined as 802.20. The MBWA is similar to the IEEE 802.16e in that it uses Orthogonal Frequency Division Multiple Access (OFDMA), provides very high mobility, and has a shared data rate of up to 100 Mbps. At present, no operator has committed to the MBWA technology.

CONCLUSION

This entry has presented the overview of wireless networks and different aspects of MANET, such as: definition, application, classification, special features, and various routing protocols. The applications of MANETs are described with examples and how those applications work with different environments. The MANET characteristic features are also pointed out such as distributed operation, lower bandwidth capacity, dynamic topology, and security. This entry also briefly covered the classification of MANETs in terms of communication procedure (single hop/multi hop), topology, (node configuration), and network size (coverage area and number of devices).

REFERENCES

1. Dressler, F. Self-Organization in Ad Hoc Networks: Overview and Classification Technical Report 02/06; Department of Computer Science 7 University of Erlangen.