Wireless ad hoc networks

Wireless ad hoc networks can range from wireless mobile networks to sensor networks, allowing short-range and long-range communication. The network topology of these networks can be highly dynamic as the nodes may be mobile and the links may have to contend with the side effects of radio communication, such as noise, fading, and interference. Nodes i a true ad hoc network communicate directly with other nodes within their wireless range however, beyond their wireless range they can communicate with each other using multihop routes throughout the network

Quantitative Features

The quantitative features include:

1 Network settling time: Time is required for a collection of mobile wireless nodes to automatically organize themselves and to transmit the first task reliably. Settling time is extremely important when a network has not been in operation for a while, and then must start-up and send messages promptly.

2. Network join time: Time is required for an entering node or group of nodes to become integrated into the ad hoc network.
3. Network depart time: Time is required for the ad hoc network to recognize the loss of one or more nodes, and to reorganize itself to route around the departed nodes.

4. Network recovery time: Time is required for the network to recover after a condition that dictates reorganization of the network, specifically, (i) for a collapsed portion of the network, due to traffic overload or node failures, to become functional again once the traffic load is reduced or the nodes become operational, or (ii) for the network to reorganize because of node mobility and resume reliable communication.

5:Frequency of updates (overhead): In a given period, a number of control packets (bytes) or overhead bytes in a packet are required to maintain proper network operation.

6. Memory byte requirement: Storage space is required in bytes, including routing tables and other management tables.

7/ Network scalability: It is the number of nodes that the ad hoc network can scale to and reliably preserve communication. The network should be able to scale to thousands of nodes.

Qualitative Features

The quantitative features include:

1 Knowledge of nodal locations: Does the routing algorithm require local or global knowledge of the network

2. Effect to topology changes: Does the routing algorithm need complete restructuring or incremental updates?

3:Adaptation to radio communication environment. Do nodes use estimation knowledge of fading, shadowing, or multiuser interference on links in their routing decisions?

4: Power consciousness: Does the network employ routing mechanisms that consider the remaining battery life of a node?

5 :Single or multichannel: Does the routing algorithm utilize a separate control channel? In same applications, multichannel execution may make the network vulnerable.

6. Bidirectional or unidirectional links: Does the routing algorithm perform efficiently on unidirectional links, for example, if bidirectional links become unidirectional?

7. Preservation of network security: Does the routing algorithm uphold the fidelity of the network, for example, low probability of detection, low probability of intercept, and security?

8. Quality of service (QoS) routing and handling of priority messages: Does the routing algorithm support priority messaging and reduction of latency for delay-sensitive real-time traffic? Can the network send priority messages/voice even when it is overloaded with routine traffic levels?

9:Real-time voice services: Can the network support simultaneous real-time multicast voice while supporting routine traffic loads associated with situation awareness and other routine services

10. Real-time video services: Can the nodes receive or transmit video on demand, while still supporting traffic levels associated with situation awareness, voice conversations, and other routine services

Advantages

Some of the advantages of wireless ad hoc networks are as follows:

1. They can be set up very fast.

2. They are very resilient. No single point of failure, such as a base station. Even if individual node fails the network still functions.

3. They are spectrally more efficient than cellular networks. Every node can communicate

with any other node, so nodes can make better use of the channel.

4. They have potential for multiple concurrent communications.

5. They have cheap deployment because of non-requirement of base station, non requirement of backbone infrastructure, and easy adaptation to changing requirements.

Applications

The dynamic and self-organizing nature of wireless ad hoc networks makes them particularly useful in situations where either rapid network deployments are required or less cost to deploy and manage network infrastructure is an issue. Application areas of wireless ad hoc networks are as follows:

1:In military communications for search and rescue operations where the robustness and speed of deployment is critical.

2. Sensor networks: For sensing forest fires, monitoring buildings, studying wildlife, etc.

3. Networks in historical buildings where placing wires is not an option.

4. A mobile ad hoc network of satellites can be designed for emergency applications such as disaster management, rescue operations, and to have broadband communications in areas where no infrastructure is available.

5. Museums: To obtain the information of monuments.

6. E-commerce: To purchase or sell goods in shopping malls.

7. Campus networks: To share educational information among the students and staff.

8. To have broadband Internet with mobility in fourth-generation (4G) wireless networks.

Ad hoc networks	*Cellular networks*
No fixed infrastructure, very rapid deployment	Fixed, prelocated cell sites and base stations
Highly dynamic topologies with multihop	Static backbone network topology
Sporadic connectivity	Stable connectivity
Automatically forms the network and adapts to changes	Detailed planning before base stations can be installed

Mobile Ad Hoc Networks

A MANET is a self-configuring network of mobile routers (and associated hosts) connected by wireless links the union of which form an arbitrary topology. Owing to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves.

Network Architecture

MANET topology is dynamic, decentralized, and ever changing with the ability and possibility of nodes moving arbitrarily. Their usage has become increasingly prevalent in emergencies such as in the cases of disasters and wars) and also in daily life such as university

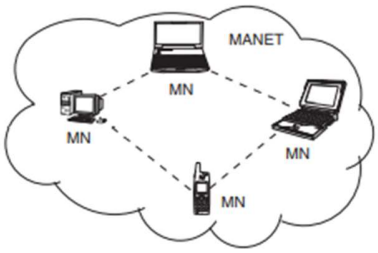

Figure 8.1 | MANET single-hop architecture. MN: mobile node; ––: wireless link.

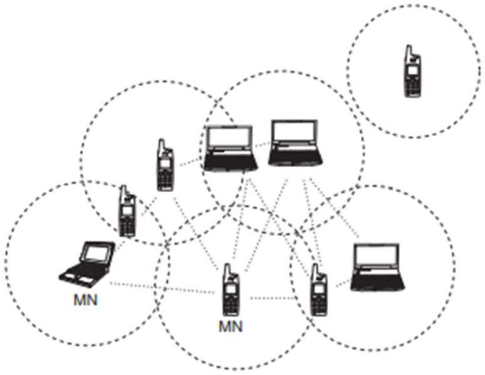

Figure 8.2 | MANET multihop architecture. ---: coverage area; ·····: wireless link; MN: mobile node.

The architecture for MANET is as shown in Figs. 8.1 and 8.2. MANET is formed by a set of MNS, such as laptops, mobile phones, and desktop machine with wireless interface capability. and by communicating among themselves by means of the air as a communication media. MANETS can use either single-hop or multihop communication. In single-hop communication, all the hosts are in one coverage area, thus communication is direct from host to host. On the other hand, in multihop communication, hosts communicate by using intermediate hosts such as in Internet communications.

The hosts establish their own network dynamically without relying on the support of infrastructure or a central administration, and cooperate to forward data in a multihop fashion. MANET's hosts must ensure functionalities and guarantees provided by the support of structures in wired networks.

As the mobile devices form a MANET without a network infrastructure, network can change constantly. First, the devices can freely move in the network. Second, the devices can leave and join the network at any time. Finally, the network disappears when the last devices leave the network.

The characteristics of MANETS are as follows:

1. Spontaneous established networks.

2. Self-organizing and adaptive.

3;Accommodate communication between diverse devices.

4:Devices can communicate directly with neighbor devices.

5. Single-hop or multihop communication may be employed.

ROUTING PROTOCOLS

(i) Table-driven routing protocols (proactive).

. These protocols are also called as proactive protocols, as they maintain the routing information even before it is needed. Each and every node in the network provides routing information to every other node in the network. Routing information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. There exist some differences between the protocols that come under this category depending on the routing information being

updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table, leading to consumption of more bandwidth. We discuss some of the existing table-driven ad hoc routing protocols

(ii) On demand routing protocols (reactive).

These protocols are also called reactive protocols because they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node, then this protocol searches for the route in an on-demand manner and establishes the connection to transmit and receive the packet. The route discovery usually occurs by flooding the route request (RREQ) packets throughout the network

(iii) Ad hoc on-demand distance vector (AODV)

AODV is a method of routing messages between MNs. It allows the MNs to pass messages through their neighbors to the nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed. ADDV makes sure that these routes do not contain loops and tries to find the shortest route possible. ADDV is also able to handle changes in routes and can create new routes if there is an error,

To explain the operation of AODV, consider a setup of four MNs as shown in Fig: 8.8. In the example, node 1 to send a message to node 3. Node 1's neighbors are nodes 2 and 4. As node 1 cannot directly communicate with node 3, node 1 sends out an RREQ. The RREQ is heard by nodes 4 and 2.

When node 1's neighbors (nodes 2 and 4) receive the RREQ message then they have two choices: if they know a route to the destination or if they are the destination then they can send an RREP message back to hode 1, otherwise they will have to rebroadcast the RREQ to their set of neighbors) The message keeps getting rebroadcast until its lifespan is over.

If node 1 does not receive à reply in a set amount of time, it will rebroadcast the REQ except this time the RREQ message will have a longer lifespan and a new ID number. All of the nodes use the sequence number in the RREQ to ensure that they do not rebroadcast an RREQ

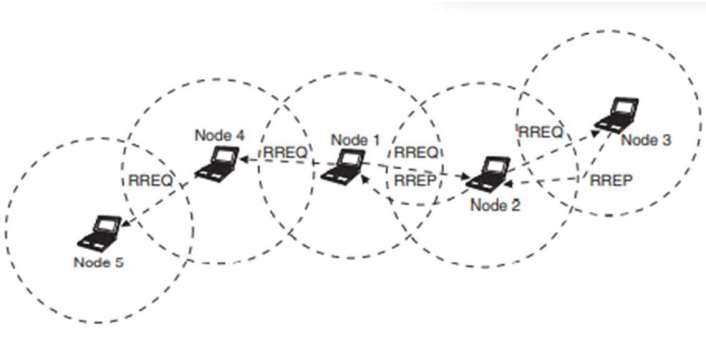

Figure 8.8 | AODV scenario.

(iv) DYNAMIC SOURCE ROUTING [DSRI]

DSR is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of MNs. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The two major phases of the DSR protocol are: route discovery and route maintenance.

When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a RREQ packet. The RREQ packet contains the addresses of the source and the destination, and a unique identification number.

Each intermediate node checks whether or not it knows a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of RREQs propagated, a node processes the RREQ packet only if it has not already seen the packet and its address is not present in the route record of the packet. An RREP is generated when either the destination or an intermediate node with current information about the destination receives the RREQ packet. An RREQ packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.

(v) GLOBAL STATE ROUTING PROTOCOL[GSRI]

In GSR, each node maintains a neighbor list: a topology table, a next hop table, and a distance table. Neighbor list of a node contains the list of its neighbors (here all nodes that can be heard by a node are assumed to be its neighbors). For each destination node, the topology table contains the link state information as reported by the destination and the time stamp of the information. For each destination, the next hop table contains the next hop to which the packets for this destination must be forwarded.

The distance table contains the shortest distance to each destination node. The routing messages are generated on a link change such as in link state protocols. On receiving a routing message, the node updates its topology table if the sequence number of the message is newer than that stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbors

Technologies

Some of the hardware technologies, required for the MANETS are as follows.

1. Smart wireless sensors: Smart wireless sensors have added substantially to the applica tions that MANETS execute. Sensor-based MANETS can be used in applications such as detecting chemicals, explosives, and toxins in hazardous areas; military reconnaissance; gathering geological data in difficult terrain; etc.

2. Smart batteries: Smart batteries have low discharge rates, a long cycle life, a wide operating temperature range, and high-energy density. Nickel cadmium (NiCad), nickel hydride (NiMH), and lithium ion (Li ion) are the most commonly used for mobile 5.9 devices. Li-ion batteries have the highest energy density among these technologies.

3. Software-defined radio: Software-defined radio (SDR, or software radio) is a radio that can be controlled using software. In SDR systems, waveform generation, modulation techniques, wideband or narrowband operation, security functions, and frequency of operation can be adjusted in software based on the requirements. SDR systems, in essence, provide programmable hardware that increases the flexibility of use and deve lopment.

4. Global positioning system (GPS): (GPS consists of a group of satellites that continuously broadcast location and timing information while orbiting the Earth. Using position triangulation, GPS receivers on the Earth calculate the exact location of the receiver on an absolute global scale. Thus, the location information calculated is in reference to the latitude and longitude coordinate system.

Applications

With the increase of portable devices as well as progress in wireless communication, MANET is gaining importance with the increasing number of widespread applications MANETS can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. MANETS allow the devices to maintain connections to the network as well as easily adding and removing devices to and from the network.

1. Military battlefield: (Military equipment now routinely contains some sort of computer equipment.MANETS allow the military to maintain information among the soldiers, vehicles, and military information headquarters . MANET-possible scenario in war condition

2. Commercial sector: MANETS can be used in emergency/rescue operations for disaster relief efforts, for example, in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network are needed. Information is relayed from one rescue team member to another over a small handheld device.

3. Creating personal network: MANET can simplify the intercommunication between various mobile devices (eg, a personal digital assistant (PDA), a laptop, and a cellular phonel Tedious wired cables are replaced with wireless connections. Such MANET extends the access to the Internet or other networks by mechanisms such as WLAN, general packet radio service (GPRS), and universal mobile telecommunications system (UMTS).

4. Local level: (MANETS can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference or classroom,

S. Message-oriented applications: (If one or more terminals that are members of a MANET are also connected to Internet, it is possible to define an application with which another generic device of the MANET can create a multimedia message: audio, video, and text synchronized and formatted according to predefined templates.

Wireless Sensor Networks

Wireless sensor networks (WSNS) have a great long-term economic potential, ability to transform our lives, and pose many new system-building challenges. Sensor networks also pose a number of new conceptual and optimization problems, such as location, deployment, and tracking, that are fundamental issues. Some of the differences between WSNS and ad hoc networks are as follows:

1. The number of sensor nodes in a sensor network can be several orders of magnitude higher than those in an ad hoc network.

2. Sensor nodes are densely deployed.

3. Sensor nodes are prone to failures.

4. The topology of a sensor network changes very frequently.

5.Sensor nodes are limited in power, computational capacities, and memory.

6. Sensor nodes may not have identification (ID) because of the large amount of overhead and large number of sensors.

Network Architecture

The sensor nodes are usually scattered in a sensor field as shown in Fig. 8.12. A sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit, and a power unit. Sensor nodes also have additional application-dependent components, such as a location finding system, power generator, and mobilizer.

Sensing units are usually composed of two subunits: sensors and analog-to-digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit.

The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network.

One of the most important components of a sensor node is the power unit. There are also other subunits that are application-dependent. A mobilizer may some times be needed to move sensor nodes when it is required to carry out the assigned tasks

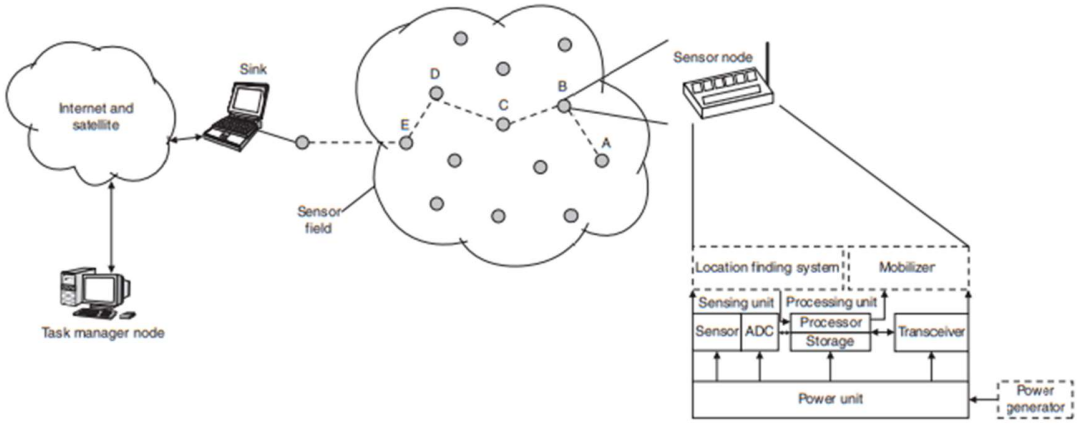

Figure 8.12 | Sensor node architecture and sensor node components.

Figure 8.12 shows WSN consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, at different locations.

Sink is also a wireless sensor node, which is connected to the central monitoring station such as the task manager node where it is connected to the Internet/satellite link to access the data remotely. Sink node's basic function is to collect the data from the sensor network and act as a gateway to the central monitoring station.

Routing Protocols

Flooding.- In flooding, each node receiving a data or management packet repeats it by broadcasting, unless a maximum number of hops for the packet is reached or the destination of the packet is the node itself. Flooding is a reactive technique, and it does not require costly topology maintenance and complex route discovery algorithms

Gossiping. derivation of flooding is gossiping in which nodes do not broadcast but send the incoming packets to a randomly selected neighbor. A sensor node randomly selects one of its neighbors to send the data. Once the neighbor node receives the data, it randomly selects another sensor node.

Sensor protocol for information via negotiation (SPIN). SPIN is designed to address the deficiencies of classic flooding by negotiation and resource adaptation. The SPIN family of protocols is designed based on two basic ideas: sensor nodes operate more efficiently and conserve energy by sending data that describe the sensor data instead of sending all the data.

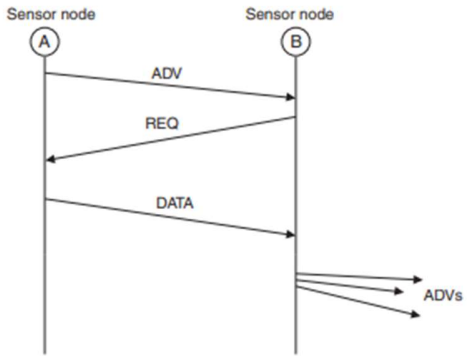

Figure 8.17 | SPIN protocol.

SPIN has three types of messages, namely, advertisement (ADV), request (REQ), and DATA as shown in Fig. 8.17. Before sending a DATA message, sensor node A broadcasts an ADV message containing a descriptor (i.e., metadata) of the DATA. If a neighbor (here node B) is interested in the data, it sends an REQ message for the DATA and DATA is sent to sensor node B.

Sensor nade B then repeats this process to its neighbors. As a result, the sensor nodes in the entire sensor network which are interested in the data will get a copy. In SPIN, sensor nodes broadcast an advertisement for the available data and wait for an REQ from interested sinks.

Low energy adaptive clustering hierarchy (LEACH).-. The purpose of LEACH is to randomly select sensor nodes as CHs, so the high energy dissipation in communicating with the base station is spread to all sensor nodes in the sensor network

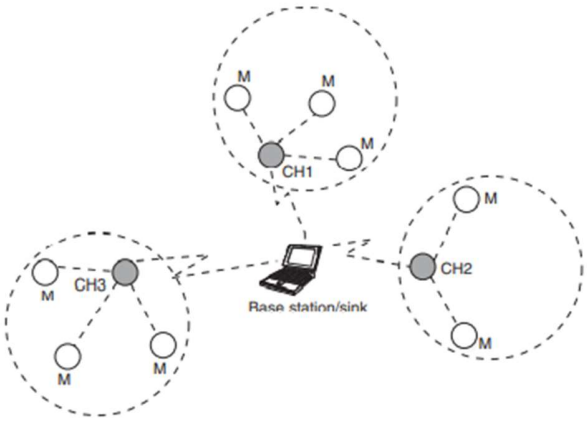

Figure 8.18 | LEACH architecture. CH: cluster head; M: cluster member.

The operation of LEACH is separated into two phases, the setup phase and the steady-state phase. Each setup phase consists of CH selection and cluster formation. Steady-state phase consists of the data transmission. The duration of the steady-state phase is longer than that of the setup phase to minimize overhead. The setup phase procedure is as follows:

1. At the beginning of each round, each node advertises its probability (depending upon its current energy level), to be the CH, to all other nodes.

2. Nodes with higher probabilities are chosen as the CHS.

3. CHs broadcast an advertisement message (ADV) using CSMA MAC protocol. 4. Based on the received signal strength, each non-CH node determines its CH for this round.

4:Each non-CH transmits a join-request message (Join-REQ) back to its chosen CH using a CSMA MAC protocol. 6 EH node sets up a time division multiple access (TDMA) schedule for data transmission coordination within the cluster.

The steady-state phase procedure for data transmission is as follows

1. TOMA schedule is used to send data from node-to-head cluster.

2:Head cluster aggregates the data received from node clusters.

3. Communication is via direct-sequence spread spectrum (DSSS) and each cluster uses a unique spreading code to reduce inter-cluster interference.

4. Data are sent from the CH nodes to the BS using a fixed spreading code and CSMA.

After a certain period of time spent on the steady-state phase, the network goes into the setup phase again and enters another round of selecting CHs.

Directed diffusion. In directed diffusion, the sink sends out interest, which is a task description, to all sensors. The task descriptors are named by assigning attribute-value pairs that describe the task. Each sensor node then stores the interest entry in its cache. The interest entry contains a time stamp field and several gradient fields.

As the interest is propagated throughout the sensor network, the gradients from the source back to the sink are set up. When the source has data for the interest, the source sends the data along the interest's gradient path

Applications

Brief explanation for some of the applications of WSN is as follows:

1. To determine the value of some parameter at a given location. In an environmental network, one might want to know the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations.

2. Detect the occurrence of events of interest and estimate parameters of the detected event or events. In the traffic sensor network, one would like to detect a vehicle moving through an intersection and estimate the speed and direction of the vehicle.

3:Classify a detected object. One should known whether a vehicle in a traffic sensor network is a car, a mini-van, a light truck, a bus, etc.

4: Track an object. In a military sensor network, track an enemy tank as it moves through the geographic area covered by the network.

5:Military sensor networks to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest.

6:Detect and characterize chemical, biological, radiological, nuclear, and explosive (CBRNE) attacks and material.

7. Detect and monitor environmental changes in plains, forests, oceans, etc

8:Wireless traffic sensor networks to monitor vehicle traffic on highways or in congested parts of a city.

9:Wireless surveillance sensor networks for providing security in shopping malls, parking garages, and other facilities.

10. Wireless parking lot sensor networks to determine which spots are occupied and which are free.

Wireless Mesh Networks

A WMN is a communication network made up of radio nodes organized in a mesh topology. The coverage area of the radio nodes working as a single network is sometimes called a "mesh cloud."

Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. A WMN can be seen as a type of wireless ad hoc network, where all radio nodes are static and do not experience direct mobility.

WMNS have a relatively stable topology except for the occasional failure of nodes or addition of new nodes

The characteristics of WMNs are as follows:

1:WMNs support ad hoc networking, and have the capability of self-forming self-healing. and self-organization.

2:WMNS are multihop wireless networks, but with a wireless infrastructure/backbone provided by mesh routers. Mesh routers are used to direct data traffic from one place, or node, to another.

3. Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes.

4. Mobility of end nodes is supported easily through the wireless infrastructure.

5. Mesh routers integrate heterogeneous networks, including both wired and wireless networks. Thus, multiple types of network access existí n WMNs.

6. Power consumption constraints are different! or mesh routers and mesh clients.

7. WMNS are not stand-alone and need to be compatible and interoperable with other wireless networks.

Network Architecture

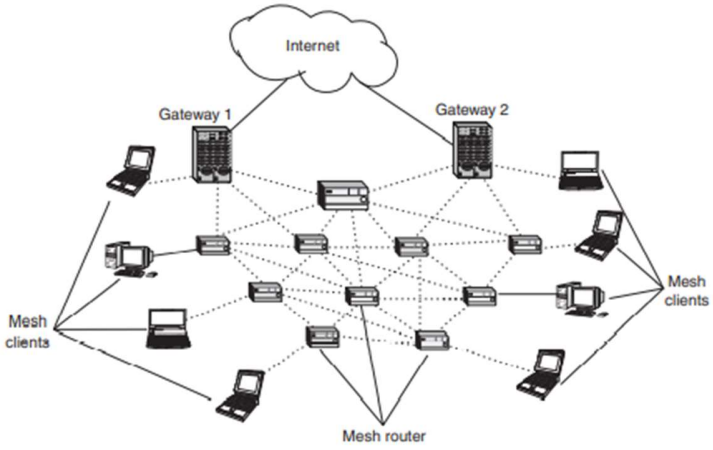

Figure 8.19 | WMN architecture.

In a typical WMN architecture, there are mesh routers and mesh clients as shown in Fig. 8.19. The mesh clients are the terminal devices to which the WMN backbone provides connectivity. The mesh routers, which are usually stationary, are connected with each other by wireless link in an ad hoc manner to form the network backbone. Generally, mesh routers have enhanced capabilities in comparison to mesh clients such as higher transmit power, multiple receive/transmit interfaces, unlimited power supply, etc.

1: Infrastructure/backbone WMNs: in this architecture, mesh routers form an infrastructure for clients. The WMN infrastructure/backbone can be built using various types of radio technologies, in addition to the mostly used IEEE 802.11 technologies. Figure shown below

The mesh routers form a mesh of self-configuring, self-healing links among themselves. With gateway functionality, mesh routers can be connected to the Internet. This approach, also referred to as infrastructure meshing, provides a backbone for conventional clients and enables integration of WMNS with existing wireless networks, through gateway/bridge functionalities in mesh routers

2. Client WMNS: Client meshing provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end-user applications to customers. Hence, a mesh router is not required for these types of networks. Client WMNs are usually formed using one type of radios on devices. Thus, a client WMN is actually the same as a conventional ad hoc network.

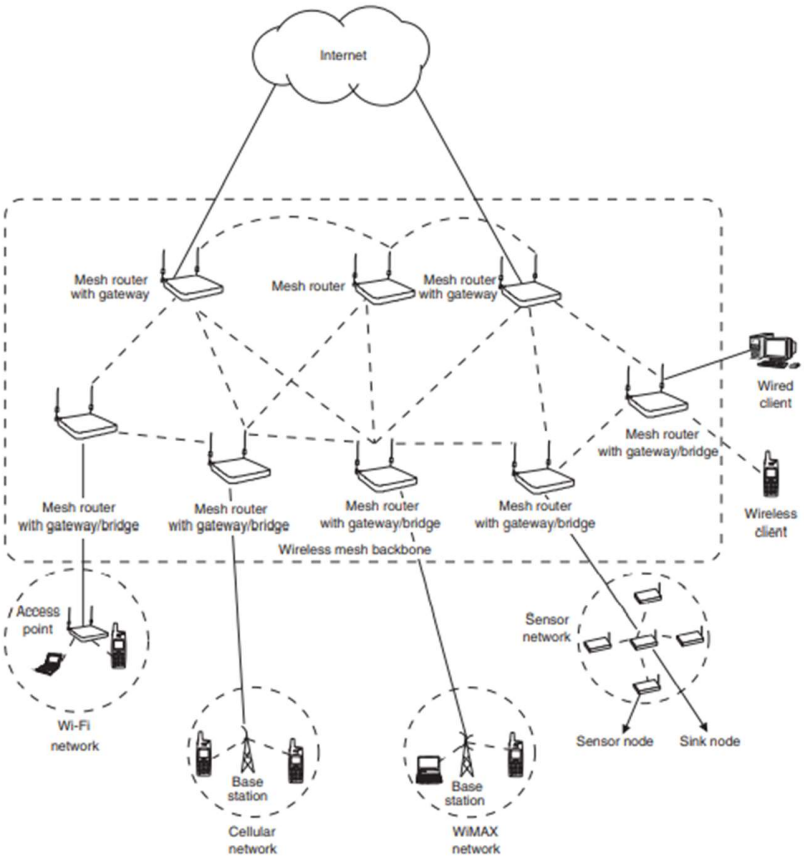

Figure 8.20 | Infrastructure/backbone WMNs.

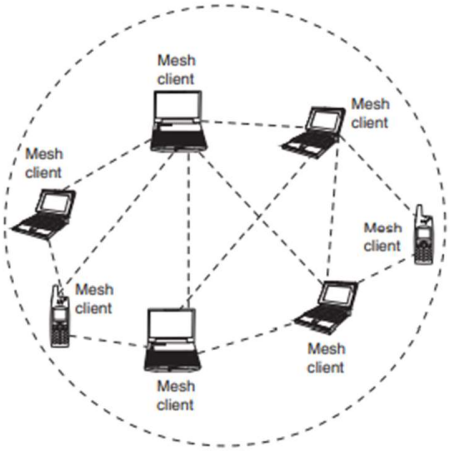

Figure 8.21 | Client WMNs.

3. Hybrid WMNs: This architecture is the combination of infrastructure and client meshing. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. Although the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi. WiMAX,

cellular, and sensor networks, the routing. capabilities of clients provide improved connectivity and coverage inside WMNS.

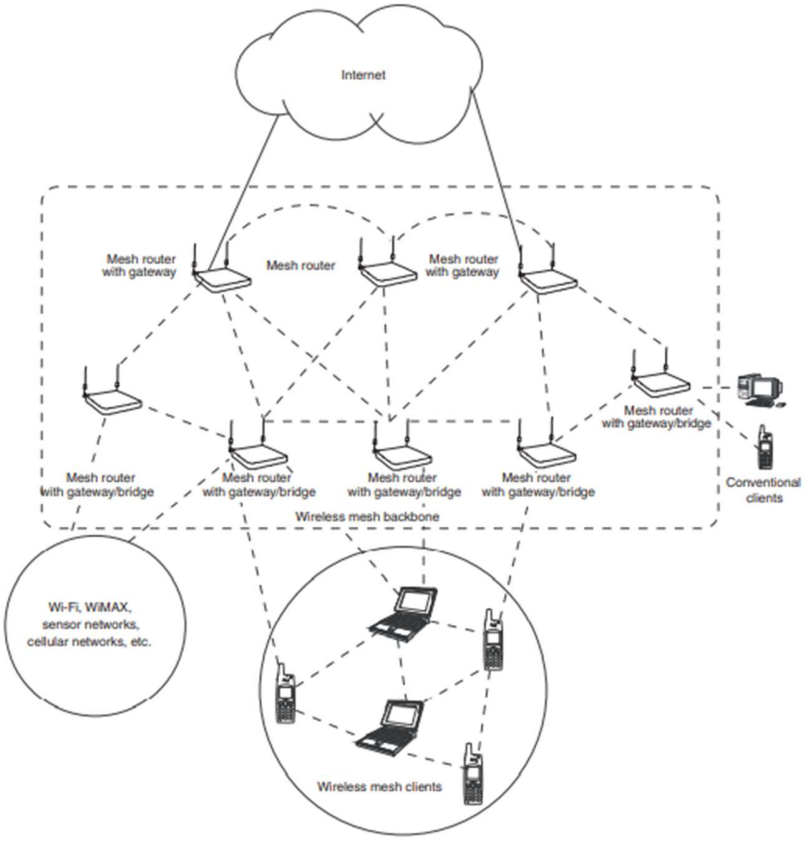

Figure 8.22 | Hybrid WMNs.

Routing Protocols

Multipath routing. The main objectives of using multipath routing are to perform better load balancing and to provide high fault tolerance. Multiple paths are selected between source and destination.

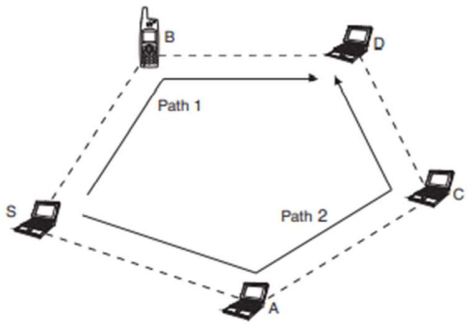

Figure 8.25 | Multipath routing scenario.

The process of multipath routing is as shown in Fig. 8.25. Here, from source 5 to destination D, two paths are available: S-B-D and S-A-C-D. Nodes A, B, and C are the intermediate nodes between source S and destination D. Initially, assume that the packets are routing by using the route S-B-D. But if this link is broken because of mobility or congestion, then the source node 5 will select the alternate path S-A-C-D without wasting much time to find the new route.

Multiradio routing. usually WMNs are characterized by stationary nodes which do not rely on batteries. In these environments, the focus of routing algorithms is on maximizing throughput rather than coping with mobility or minimizing energy

A multiradio link quality source routing (MR-LOSR) is a routing protocol for multiradio WMN. A new performance metric, called weighted cumulative expected transmission time (WCETT), is incorporated in the routing protocol. WCETT takes into account both link quality metric and the minimum hop count and achieves good trade-off between delay and throughput

A MR-LQSR routing protocols consists of four components

1:A component that discovers the neighbors of a node.

2. A component that assigns weights to the links that a node has with its neighbors.

3. A component to propagate this information to other nodes in the network.

4. A component that uses the link weights to find a good path for a given destination .

Hierarchical routing : In hierarchical routing, a certain self-organization scheme is employed to group network nodes into clusters. Each cluster has one or more cluster heads. Nodes in a cluster can be one or more hops away from the cluster head. As connectivity between clusters is needed, some nodes can communicate with more than one cluster and work as a gateway.

Technologies

Some of the standards and technologies for WMN are as follows:

1. IEEE 802.11 mesh networks: Currently, IEEE 802.11 wireless networks can achieve a peak rate of 11 Mbps (802.11b) and 54 Mbps (802.11a g)

2. IEEE 802.15 mesh networks: IEEE 802.15.3a standard is based on multiband OFDM alliance (MBOA) PHY layer that uses UWB to reach up to 480 Mbps. A competing proposal of a direct sequence-UWB (DS-UWB) claims support for up to 1.3 Gbps. Mesh networks have been predicted to be the killer application for UWB radio systems. The ZigBee network layer supports multiple network topologies of WMN including star, cluster tree, and mesh

3. IEEE 802.16 mesh networks. The original 802.16 standard operates in the 1066 GH_2 frequency band and requires line-of-sight towers. The 802.16a extension uses a lower frequency of 211 GHz, enabling non-line-of-sight connections. With 802.16a, carriers will be able to connect more customers to a single

and substantially reduce service costs. To allow consumers to connect to the Internet while moving at vehicular speeds, IEEE 802.16 standard called 802.16e is used.

Applications

1. Broadband home networking: In mesh networking, the access points are replaced by wireless mesh routers with mesh connectivity established among them. Therefore, the communication between these nodes becomes much more flexible and more robust to network faults and link failures. Communication within home networks can be realized through mesh networking without going back to the access hub all the time.

2. Community and neighborhood networking: "For community and neighborhood network ing, mesh networking allows many applications such as distributed file storage, distributed file access, and video streaming.

3. Enterprise networking: In mesh networking, access points are replaced by mesh routers and Ethernet wires can be eliminated. Multiple backhaul access modems can be shared by all utilization of enterprise networks. WMNS can grow easily as the size of enterprise expands.

4. Transportation systems: Convenient passenger information services, remote monitoring of in-vehicle security video, and driver communications can be supported with the help of WMNs. To enable such mesh networking for a transportation system, two key techniques are needed the high-speed mobile backhaul from a vehicle (car, bus, or train) to the Internet and the mobile mesh networks within the vehicle.

5. Security surveillance systems: As security is turning out to be a very high concern, security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc. To deploy such systems at locations as needed, WMNS are a much more viable solution than wired networks to connect all devices. As still images and videos are the major traffic flowing in the network, this application demands much higher network capacity than other applications.

Vehicular Ad Hoc Networks (VANETS)

Vehicular ad hoc networks (VANETS) are an envision of the intelligent transportation system (ITS). Vehicles communicate with each other in two ways: intervehicle communication and vehicle to roadside infrastructure communication. VANETS are based on short-range wireless communication between Unlike infrastructure-based networks such as cellular net works, these networks are constructed on the fly (self-organizing).

Unique Characteristics of VANETS

The fundamental characteristics that differentiate VANETS from other networks are as follows:

1. Geographically constrained topology: Roads limit the network topology to one dimen sion the road direction. Except for crossroads or overlay bridges, roads are generally located far apart. Even in urban areas, where they are located close to each other, there exist obstacles, such as buildings and advertisement walls, which prevent wireless signals from traveling between roads.

This implies that vehicles can be considered as points of the same line; a road can be approximated as a straight line or a small angled curve. This observation is quite important, because it affects the wireless technologies that can be considered. For example, as the packet relays are almost all in the same one-directional deployment region, the use of directional antennas could be of great advantage.

2. Partitioning and large-scale: The probability of end-to-end connectivity decreases with distance; this is true for one-dimensional network topologies. In contrast, connectivity is often explicitly assumed in research for traditional ad hoc networks, sometimes even for the evaluation of routing protocols. In addition, VANETS can extend in large areas, as far as the road is available. This artifact together with the one-dimensional deployment increases the above probability.

3. Self-organization: The nodes in the network must be capable to detect each other and transmit packets with or without the need of a base station.

4. Power consumption: (In traditional wireless networks, nodes are power-limited and their life depends on their batteries this is especially true for ad hoc networks. Vehicles, however, can provide continuous power to their computing and communication devices. As a result, routing protocols do not have to account for methodologies that try to prolong the battery life.

5. Node reliability: (vehicles may join and leave the network at any time and much more frequently than in other wireless networks. The arrival/departure rate of vehicles depends on their speed, the environment, as well as on the driver that needs to be connected to the network.

6: Channel capacity: The channels in VANETS over which the terminals communicate are subjected to noise, fading, interference, multipath propagation, path loss, and have less bandwidth. So high bit-error rates are common in VANETS, One end-to-end path can be shared by several sessions. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous. So smart algorithms are needed to overcome of fluctuating link capacity in networks.

7:Vehicle density: Multihop data delivery through VANETS is complicated by the fact that vehicular networks are highly mobile and sometimes sparse. The network density is related to the traffic density, which is affected by the location and time. Although it is very difficult to find an end-to-end connection for a sparsely connected network, the high mobility of vehicular networks introduces opportunities for mobile vehicles to connect with each other intermittently during moving.

Network Architecture

A typical VANETS architecture is as shown in Fig. 8.26. Vehicle-to-vehicle and vehicle-to road-side base station/gateway communication is possible for providing safety and other information services to vehicle users. Group of vehicles together may form a cluster to disseminate information among themselves as well as to other clusters and base stations.

In a VANET, each vehicle in the system is equipped with a computing device, a short-range wireless interface, and a global positioning system (GPS) receiver. GPS receiver provides loca tion, speed, current time, and direction of the vehicle. Manufacturers are already enhancing cars with sensors that help drivers to park and provide GPS compasses as standard equipment on luxury cars

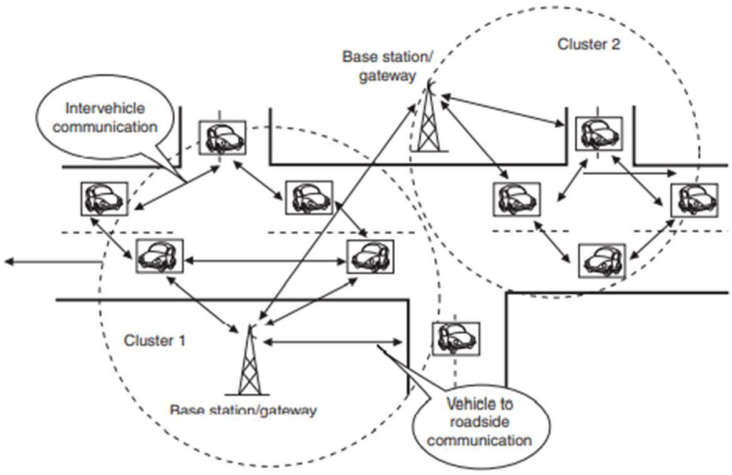

Figure 8.26 | VANET architecture.

Each vehicle stores information about itself and other vehicles in a local database. The records in this database are periodically broadcasted. A record consists of the vehicle identification, position in the form of latitude and longitude, current speed of the vehicle, direction, and timestamps corresponding to when this record was first created and when this record was received.

Protocols

Routing Protocols

As the topology of the network is constantly changing, the issue of routing packets between any pair of vehicles becomes a challenging task. So the protocols should be based on reactive routing instead of proactive routing

Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops in which the situation is more complex than the single hop communication.

Technologies

VANET may integrate networking technologies such as Wi-Fi (IEEE 802.11 b/g). WIMAX (IEEE 802.16), and Bluetooth (IEEE 802.15). Wi-Fi can be used for vehicle-to-vehicle as well as vehicle-to-base station communication. WIMAX can be used for forming wireless backbone connecting different base stations. Bluetooth can be used for intravehicle communication as well as communicating with nearest neighbors.

Applications

(Some of the important applications of VANETS are as follows:

1. Message and file delivery: This application focuses on enabling the delivery of messages and files in a vehicular network to the target receivers (group communication) with acceptable performance.

2 Internet connectivity: This application focuses on connecting the vehicles to the Internet using roadside infrastructure and intervehicle communications to facilitate browsing send/read e-mails, chatting, etc.

3:Communication-based longitudinal control: This application focuses on exploiting the "look-through capability of VANETS to help avoiding accidents. For example, a vehicle can check the status of upfront vehicles status (speed, brake applied, road blocks, etc).

4: Cooperative assistance systems: It focuses on coordinating vehicles at critical points such as blind crossings (a crossing without light control) and highway entries.

5. Safety services: Safety applications include emergency braking, accidents, passing assist ance, security distance warning, and coordination of cars entering a lane. Furthermore, sensors embedded in the car engine and elsewhere could be used for exchanging information,

6. Traffic monitoring and management services: In such types of services, all vehicles are part of a ubiquitous sensor system. Each vehicle monitors the locally observed traffic situation such as density and average speed using an on-board sensor and the results are transferred to other vehicles vía wireless data link through the network.