

1

Introduction

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs) has emerged recently [7, 8]. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front costs, easy network maintenance, robustness, and reliable service coverage.

Conventional nodes, e.g., desktops, laptops, PDAs, PocketPCs, phones, equipped with wireless network interface cards (NICs) can be connected directly to wireless mesh routers. Customers without wireless NICs can access WMNs by connecting to wireless mesh routers through, for example, Ethernet. Thus, WMNs will greatly help users to be always-on-line anywhere anytime. Moreover, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular systems, wireless sensor networks, wireless-fidelity (Wi-Fi) [264] systems, worldwide inter-operability for microwave access (WiMAX) [265], and WiMedia [266] networks. Consequently, through an integrated WMN, users of existing networks are provided with otherwise impossible services of these networks.

Wireless Mesh Networking is a promising wireless technology for numerous applications [189], e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. It is gaining significant attention as a possible way for cash-strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments. With the capability of self-organization and self-configuration, WMNs can be deployed incrementally, one node at a time, as needed. As more nodes are installed, up goes the reliability, and also the connectivity, that all subscribers will enjoy.

Deploying a WMN is not too difficult, because all the required components are already available in the form of ad hoc routing protocols, IEEE 802.11 MAC protocol, wired equivalent privacy (WEP) security, etc. Several companies have already realized the potential

of this technology and offer wireless mesh networking products. A few testbeds have been established in university research labs. However, to make a WMN be all it can be, considerable research efforts are still needed. For example, the available MAC and routing protocols applied to WMNs do not have enough scalability; e.g., throughput drops significantly as the number of nodes or hops increases. Existing security schemes may be effective for certain types of attack, but they lack a comprehensive mechanism to prevent attacks from different protocol layers. Similar problems exist in other networking protocols. Thus, existing communication protocols, ranging from application layer to transport, routing, MAC, and physical layers, need to be revisited and enhanced. In some circumstances, new protocols need to be invented.

Researchers have started to revisit the protocol design of existing wireless networks, especially of IEEE 802.11 networks, ad hoc networks, and wireless sensor networks, from the perspective of WMNs. Industrial standards groups are also actively working on new specifications for mesh networking. For example, IEEE 802.11 [113, 138], IEEE 802.15 [124, 147], and IEEE 802.16 [129, 211, 263] all have established subworking-groups to focus on new standards for WMNs.

1.1 Network Architecture

WMNs consist of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/repeater functions as in a conventional wireless router, a wireless mesh router contains additional routing functions to support mesh networking. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Compared to a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power through multihop communications. Optionally, the medium access control protocol in a mesh router is enhanced with a better scalability in a multihop mesh environment.

In spite of all these differences, mesh and conventional wireless routers are usually built based on a similar hardware platform. Mesh routers can be built based on dedicated computer systems, e.g., embedded systems, and look compact, as shown in Figure 1.1. They can also be built based on general-purpose computer systems, e.g., laptop/desktop PCs.

Mesh clients also have the necessary functions for mesh networking, and thus can also work as a router in WMN. However, gateway or bridge functions do not exist in these nodes. In addition, mesh clients usually have only one wireless interface. As a consequence, the hardware platform and the software for mesh clients can be much simpler than those for mesh routers. Mesh clients have a greater variety of devices compared to mesh routers. They can be a laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, BACnet (Building Automation and Control network) controller, and many other devices, as shown in Figure 1.2.

The architecture of WMNs can be classified into three main groups based on the functionality of the nodes.

- **Infrastructure/Backbone WMNs:**

The architecture is shown in Figure 1.3, where dashed and solid lines indicate wireless and wired links, respectively. This type of WMN includes mesh routers that form an infrastructure for clients that connect to them. The WMN infrastructure/backbone

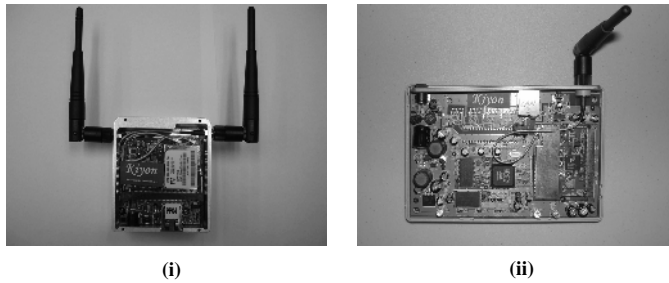


Figure 1.1 Examples of mesh routers based on different embedded systems: (i) PowerPC, (ii) ARM

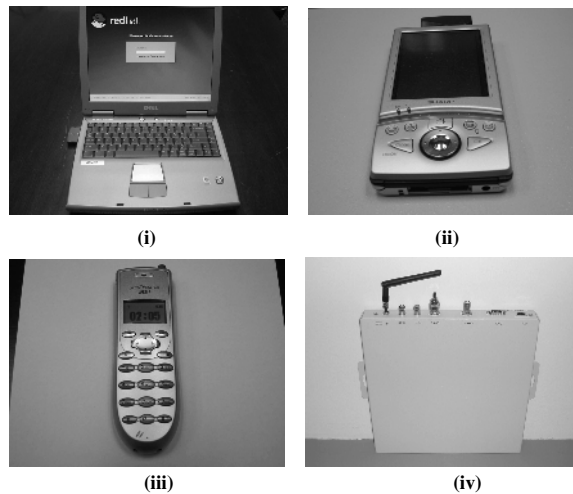


Figure 1.2 Examples of mesh clients: (i) laptop, (ii) PDA, (iii) Wi-Fi IP phone, (iv) Wi-Fi RFID reader

can be built using various types of radio technology, in addition to the heavily used IEEE 802.11 technology. 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 backbone for conventional clients and enables the integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers. Conventional clients with Ethernet interface can be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers. If different radio technologies are used, clients must communicate with the base stations that have Ethernet connections to mesh routers.

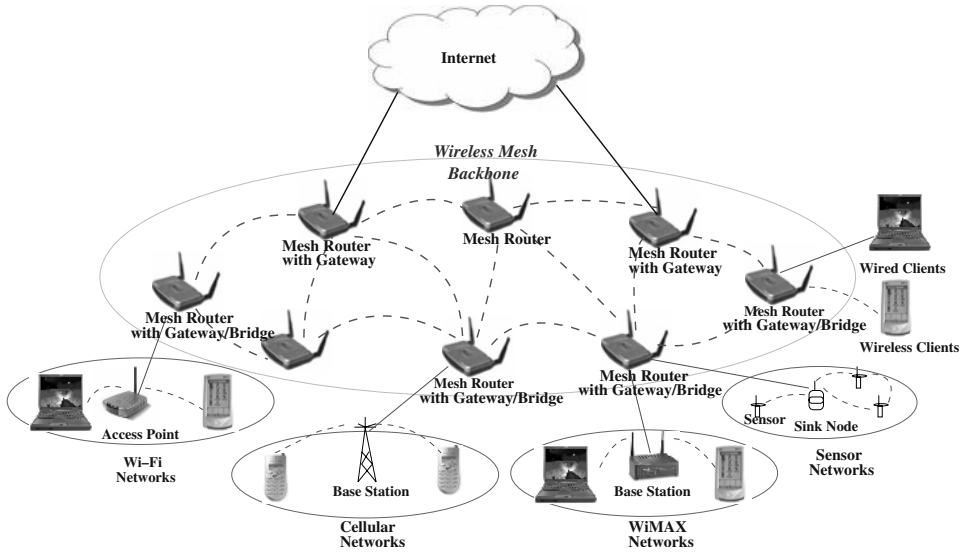


Figure 1.3 Infrastructure/backbone WMNs

Infrastructure/Backbone WMNs are the most commonly used type. For example, community and neighborhood networks can be built using *infrastructure meshing*. The mesh routers are placed on the roofs of houses in a neighborhood, and these can serve as access points for users in homes and along the roads. Typically, two types of radio are used in the routers, i.e., for backbone communication and for user communication. The mesh backbone communication can be established using long-range communication techniques including, for example, directional antennas.

- **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 this type of network. The basic architecture is shown in Figure 1.4. In *Client WMNs*, a packet destined to a node in the network hops through multiple nodes to reach the destination. *Client WMNs* are usually formed using one type of radio on devices. Moreover, the requirements on end-user devices is increased when compared to *infrastructure meshing*, since, in *Client WMNs*, the end users have to perform additional functions such as routing and self-configuration.
- **Hybrid WMNs:** This architecture is the combination of *infrastructure* and *client meshing* as shown in Figure 1.5. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While 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 the WMN. The hybrid architecture will be the most applicable case in our opinion.

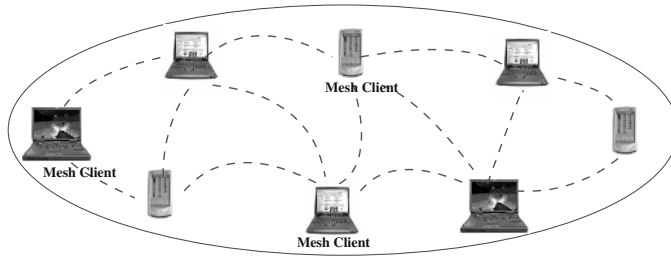


Figure 1.4 Client WMNs

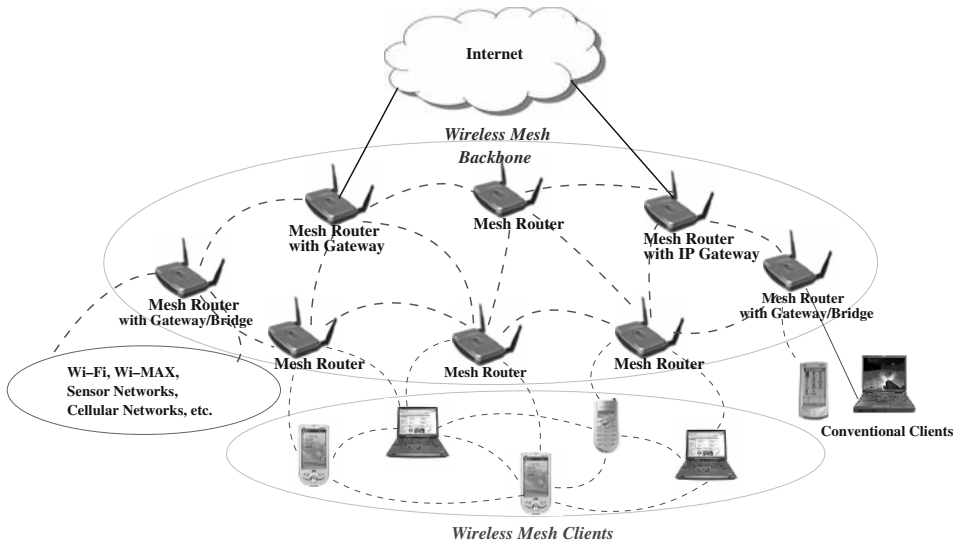


Figure 1.5 Hybrid WMNs

1.2 Characteristics

The characteristics of WMNs are explained in what follows.

- **Multihop wireless network:** One incentive to develop WMNs is to extend the coverage range of current wireless networks without sacrificing the channel capacity. Another major objective of WMNs is to provide nonline-of-sight (NLOS) connectivity among users without direct line-of-sight (LOS) links. To meet these requirements, mesh-style multihopping is indispensable [154], which facilitates higher throughput without sacrificing effective radio range via shorter link distances, less interference between nodes, and more efficient frequency reuse.
- **Support for ad hoc networking, and capability of self-forming, self-healing, and self-organization:** Ad hoc networking enhances network performance, such as flexible

network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity, i.e., multipoint-to-multipoint communications. Due to these features, WMNs have low upfront investment requirement, and the network can grow gradually as needed.

- **Mobility dependence on the type of mesh nodes:** Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes. Thus, the mobility in WMNs varies from node to node, which is different from ad hoc networks.
- **Multiple types of network access:** In WMNs, both backhaul access to the Internet and peer-to-peer (P2P) communications within WMNs are supported [139]. In addition, integration of WMNs with other wireless networks and providing services to end-users of these networks can be accomplished through WMNs. However, an ad hoc network does not require these capabilities.
- **Dependence of power-consumption constraints on the type of mesh nodes:** Mesh routers in WMNs usually do not have strict constraints on power consumption. However, mesh clients may require power efficient protocols. As an example, a mesh-capable sensor requires its communication protocols to be power efficient. Thus, the MAC or routing protocols optimized for mesh routers may not be appropriate for mesh clients, because power efficiency is the primary concern for wireless sensor networks [10, 11].
- **Compatibility and interoperability with existing wireless networks:** For example, WMNs built based on IEEE 802.11 technologies [133] must be compatible with IEEE 802.11 standards in the sense of supporting both mesh-capable and conventional Wi-Fi clients. Such WMNs also need to be interoperable with other wireless networks such as WiMAX, ZigBee [293], and cellular systems.

Based on their characteristics, WMNs are generally considered as a type of ad hoc network owing to the lack of wired infrastructure that exists in cellular or Wi-Fi networks through deployment of base stations or access points. While ad hoc networking techniques are required by WMNs, the additional capabilities necessitate more sophisticated algorithms and design principles for the realization of WMNs. More specifically, instead of being a type of ad hoc networking, WMNs aim to diversify the capabilities of ad hoc networks. Consequently, ad hoc networks can actually be considered as a *subset* of WMNs. To illustrate this point, the differences between WMNs and ad hoc networks are outlined below. In this comparison, the hybrid architecture is considered, since it comprises all the advantages of WMNs.

- **Wireless infrastructure/backbone:** As discussed before, WMNs consist of a wireless backbone with mesh routers. The wireless backbone provides wide coverage, connectivity, and robustness in the wireless domain. However, the connectivity of ad hoc networks depends on the individual contributions of end users which may not be reliable.
- **Integration:** WMNs support conventional clients that use the same radio technologies as a mesh router. This is accomplished through a host-routing function available in mesh routers. WMNs also enable integration of various existing networks such as Wi-Fi, the Internet, cellular and sensor networks through gateway/bridge functionalities

in the mesh routers. Consequently, users in one network are provided with services in other networks, through the use of the wireless infrastructure. The integrated wireless networks through WMNs resemble the Internet backbone, since the physical location of network nodes becomes less important than the capacity and network topology.

- **Dedicated routing and configuration:** In ad hoc networks, end-user devices also perform routing and configuration functionalities for all other nodes in the networks. However, WMNs contain mesh routers for these functionalities. Hence, the load on end-user devices is significantly decreased, which provides a lower energy consumption and high-end application capabilities to possibly mobile and energy-constrained end-users. Moreover, the end-user requirements are limited which decreases the cost of devices that can be used in WMNs.
- **Multiple radios:** As discussed before, mesh routers can be equipped with multiple radios to perform routing and access functionalities. This enables separation of two main types of traffic in the wireless domain. While routing and configuration traffic is performed between mesh routers, access to the network from end users can be carried on a different radio. This significantly improves the capacity of the network. On the other hand, these functionalities are performed in the same channel in ad hoc networks constraining the performance.
- **Mobility:** Since ad hoc networks provide routing using the end-user devices, the network topology and connectivity depend on the movement of users. This imposes additional challenges to routing protocols as well as network configuration and deployment. Since mesh routers provide the infrastructure in WMNs, the coverage of the WMN can be engineered easily. While providing continuous connectivity throughout the network, the mobility of end users is still supported, without compromising the performance of the network.
- **Compatibility:** WMNs contain many differences when compared to ad hoc networks. However, as discussed above, ad hoc networks can be considered as a subset of WMNs. More specifically, the existing techniques developed for ad hoc networks are already applicable to WMNs. As an example, through the use of mesh routers and routing-capable end users, multiple ad hoc networks can be supported in WMNs, but with further integration of these networks.

1.3 Application Scenarios

Research and development of WMNs is motivated by several applications which clearly demonstrate the promising market, but, at the same time, these applications cannot be supported directly by other wireless networks such as cellular systems, ad hoc networks, wireless sensor networks, standard IEEE 802.11, etc. In this section, we discuss these applications.

- *Broadband home networking:* Currently broadband home networking is realized through IEEE 802.11 WLANs. An obvious problem is the location of the access points. Without a site survey, a home (even a small one) usually has many dead zones without

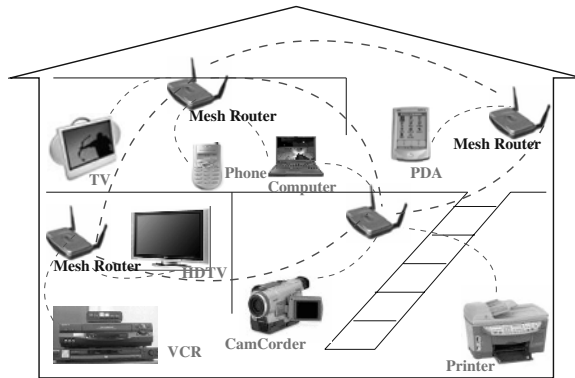


Figure 1.6 WMNs for broadband home networking

service coverage. Solutions based on site survey are expensive and not practical for home networking, while installation of multiple access points is also expensive and not convenient because of Ethernet wiring from access points to backhaul network access modem or hub. Moreover, communications between end nodes under two different access points have to go all the way back to the access hub. This is obviously not an efficient solution, especially for broadband networking. Mesh networking, as shown in Figure 1.6, can resolve all these issues in home networking. The access points must be 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. Dead zones can be eliminated by adding mesh routers, changing locations of mesh routers, or automatically adjusting power levels of mesh routers. Communication within home networks can be realized through mesh networking without going back to the access hub all the time. Thus, network congestion due to backhaul access can be avoided. In this application, wireless mesh routers have no constraints on power consumptions and mobility. Thus, protocols proposed for mobile ad hoc networks [59] and wireless sensor networks [10, 11] are too cumbersome to achieve satisfactory performance in this application. On the other hand, Wi-Fis are not capable of supporting ad hoc multihop networking. As a consequence, WMNs are well suited for broadband home networking.

- *Community and neighborhood networking:* In a community, the common architecture for network access is based on cable or digital subscriber line (DSL) connected to the Internet, and the last hop is wireless by connecting a wireless router to a cable or DSL modem. This type of network access has several drawbacks.
 - Even if the information must be shared within a community or neighborhood, all traffic must flow through the Internet. This significantly reduces network resource utilization.
 - A large percentage of areas in between houses is not covered by wireless services.

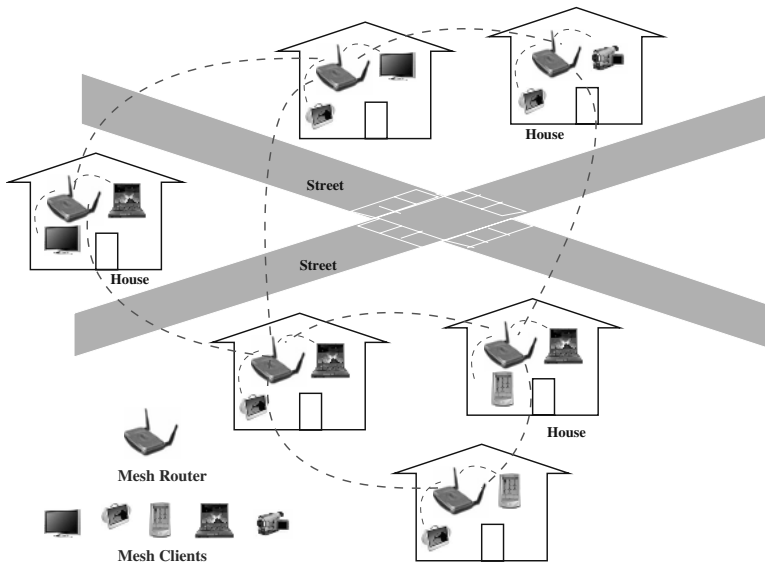


Figure 1.7 WMNs for community networking

- An expensive but high-bandwidth gateway between multiple homes or neighborhoods may not be shared, and wireless services must be set up individually. As a result, network service costs may increase.
- Only a single path may be available for one home to access the Internet or communicate with neighbors.

WMNs mitigate the above disadvantages through flexible mesh connectivities between homes, as shown in Figure 1.7. WMNs can also enable many applications such as distributed file storage, distributed file access, and video streaming.

- *Enterprise networking*: This can be a small network within an office or a medium-size network for all offices in an entire building, or a large-scale network among offices in multiple buildings. Currently standard IEEE 802.11 wireless networks are widely used in various offices. However, these wireless networks are still isolated islands. Connections among them have to be achieved through wired Ethernet connections, which is the key reason for the high cost of enterprise networks. In addition, adding more backhaul access modems only increases capacity locally, but it does not improve robustness to link failures, network congestion, and other problems of the entire enterprise network. If the access points are replaced by mesh routers, as shown in Figure 1.8, Ethernet wires can be eliminated. Multiple backhaul access modems can be shared by all nodes in the entire network, and thus improve the robustness and resource utilization of enterprise networks. WMNs can grow easily as the size of enterprise expands.

WMNs for enterprise networking are much more complicated than at home because more nodes and more complicated network topologies are involved. The service model

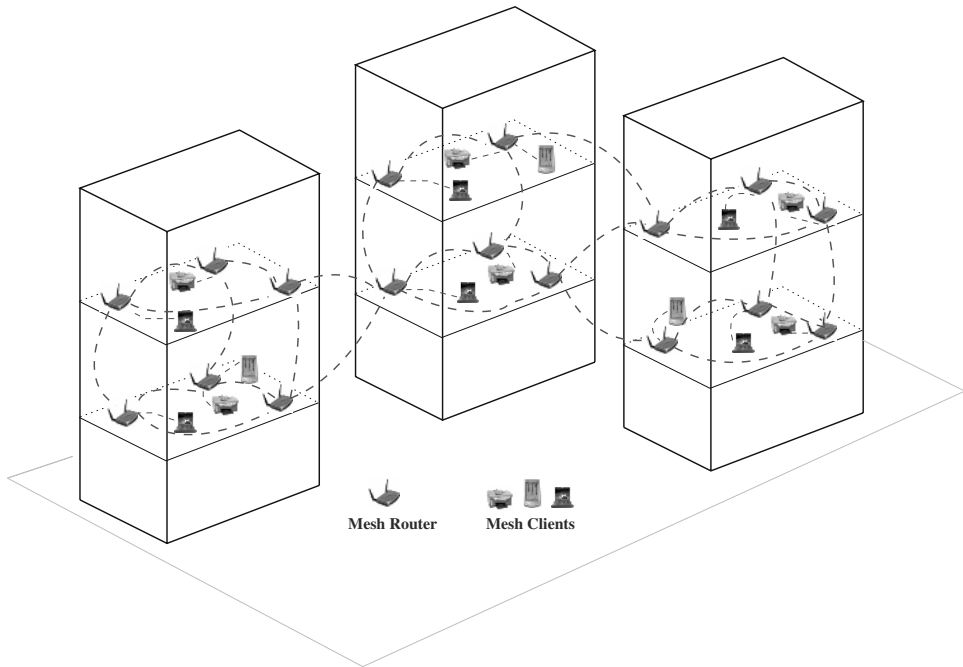


Figure 1.8 WMNs for enterprise networking

of enterprise networking can be applied to many other public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centers, sport centers, etc.

- *Metropolitan area networks (MAN):* WMNs in a metropolitan area have several advantages. The physical-layer transmission rate of a node in WMNs is much higher than that in any cellular systems. For example, an IEEE 802.11g node can transmit at a rate of 54 Mbps. Moreover, the communication between nodes in WMNs does not rely on a wired backbone. Compared to wired networks, e.g., cable or optical networks, wireless mesh MAN is an economic alternative to broadband networking, especially in underdeveloped regions. The wireless mesh MAN covers a potentially much larger area than home, enterprise, building, or community networks, as shown Figure 1.9. Thus, the requirement on the network scalability by wireless mesh MANs is much higher than that by other applications.
- *Transportation systems:* Instead of limiting IEEE 802.11 or 802.16 access to stations and stops, mesh networking technology can extend access into buses, ferries, and trains. Thus, convenient passenger information services, remote monitoring of in-vehicle security video, and driver communications can be supported. 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 mobile mesh networks within the vehicle, as shown in Figure 1.10.

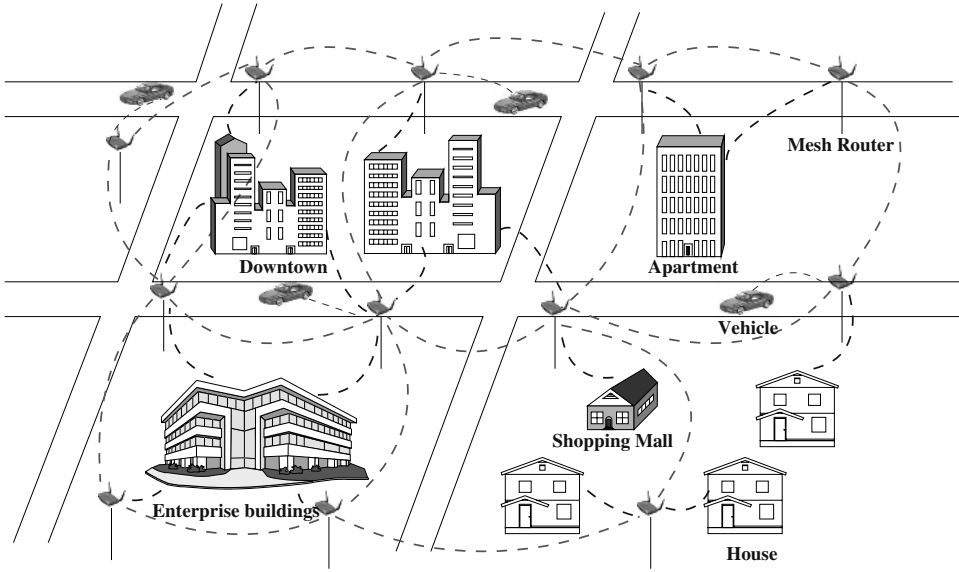


Figure 1.9 WMNs for metropolitan area networks

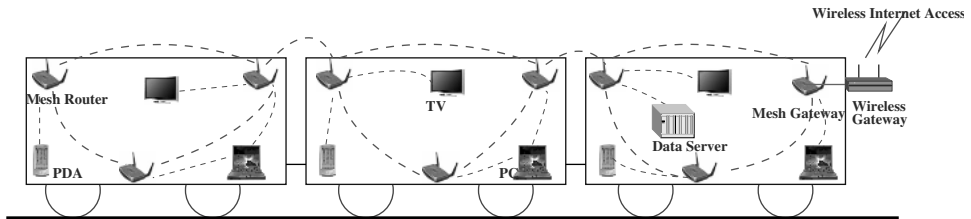


Figure 1.10 WMNs for transportation systems

- Building automation:* In a building, various electrical devices including power, light, elevator, air conditioner, etc., need to be controlled and monitored. Currently, this task is accomplished through standard wired networks, which is very expensive due to the complexity in deployment and maintenance of a wired network. Recently, Wi-Fi-based networks have been adopted to reduce the cost of such networks. However, this effort has not achieved satisfactory performance yet, because the deployment of Wi-Fi for this application is still rather expensive due to the wiring of Ethernet. If BACnet (Building Automation and Control networks) access points are replaced by mesh routers, as shown in Figure 1.11, the deployment cost will be significantly reduced. The deployment process is also much simpler due to the mesh connectivity among wireless routers.

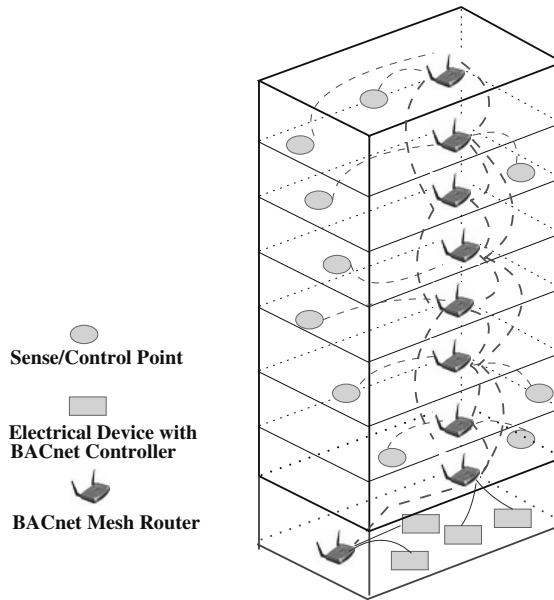


Figure 1.11 WMNs for building automation

- *Health and medical systems:* In a hospital or medical center, monitoring and diagnosis data need to be processed and transmitted from one room to another for various purposes. Data transmission is usually broadband, since high resolution medical images and various periodical monitoring information can easily produce a constant and large volume of data. Traditional wired networks can only provide limited network access to certain fixed medical devices. Wi-Fi-based networks must rely on the existence of Ethernet connections, which may cause high system cost and complexity but without the abilities to eliminate dead spots. However, these issues do not exist in WMNs.
- *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. In order to deploy such systems at locations as needed, WMNs are a much more viable solution than wired networks to connect all devices. Since still images and videos are the major traffic flowing in the network, this application demands much higher network capacity than other applications.

In addition to the above applications, WMNs can also be applied to *spontaneous (emergency/disaster) networking* and *P2P communications*. For example, wireless networks for an emergency response team and firefighters do not have in-advance knowledge of where the network should be deployed. By simply placing wireless mesh routers in desired locations, a WMN can be quickly established. For a group of people holding devices with wireless networking capability, e.g., laptops and PDAs, P2P communication anytime anywhere is an efficient solution for information sharing. WMNs are able to meet

this demand. These applications illustrate that WMNs are a superset of ad hoc networks, and thus, can accomplish all functions provided by ad hoc networking.

1.4 Critical Design Factors

Before a network is designed, deployed, and operated, factors that critically influence its performance need to be considered. For WMNs, the critical factors are summarized as follows.

- *Radio techniques.* Driven by the rapid progress of semiconductor, RF technologies, and communication theory, wireless radios have undergone a significant revolution. Currently many approaches have been proposed to increase capacity and flexibility of wireless systems. Typical examples include directional and smart antennas [219, 240], MIMO systems [245, 272], and multiradio/multichannel systems [4, 236]. To date, MIMO has become one of the key technologies for IEEE 802.11n [113], the high speed extension of Wi-Fi. Multiradio chipsets and their development platforms are available on the market.

To further improve the performance of a wireless radio and control by higher layer protocols, more advanced radio technologies such as reconfigurable radios, frequency agile/cognitive radios [158, 188], and even software radios [191] have been used in wireless communication.

Although these radio technologies are still in their infancy, they are expected to be the future platform for wireless networks owing to their capability of dynamically controlling the radios. These advanced wireless radio technologies all require a revolutionary design in higher layer protocols, especially in MAC and routing protocols. For example, when directional antennas are applied to IEEE 802.11 networks, a routing protocol needs to take into account the selection of directional antenna sectors. Directional antennas can reduce exposed nodes, but they also generate more hidden nodes. Thus, MAC protocols need to be redesigned to resolve this issue. As for MIMO systems, new MAC protocols are also necessary [245]. When software radios are considered, much more powerful MAC protocols, such as programmable MAC, are anticipated.

- *Scalability.* Multihop communication is common in WMNs. For multihop networking, it is well known that communication protocols suffer from scalability issues [108, 134], i.e., when the size of network increases, the network performance degrades significantly. Routing protocols may not be able to find a reliable routing path, transport protocols may lose connections, and MAC protocols may experience significant throughput reduction. As a typical example, the current IEEE 802.11 MAC protocol and its derivatives cannot achieve a reasonable throughput as the number of hops increases to four or higher (for 802.11b, the TCP throughput is lower than 1.0 Mbps). The reason for low scalability is that the end-to-end reliability sharply drops as the scale of the network increases. In WMNs, due to their ad hoc architecture, the centralized multiple access schemes such as Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) are difficult

to implement due to their complexities and a general requirement on timing synchronization for TDMA (and code management for CDMA). When a distributed multihop network is considered, accurate timing synchronization within the global network is difficult to achieve [108]. Thus, distributed multiple access schemes such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) are more favorable. However, CSMA/CA has very low frequency spatial-reuse efficiency [3], which significantly limits the scalability of CSMA/CA-based multihop networks. To improve the scalability of WMNs, designing a hybrid multiple access scheme with CSMA/CA and TDMA or CDMA is an interesting and challenging research issue.

- *Mesh connectivity.* Many advantages of WMNs originate from mesh connectivity which is a critical requirement on protocol design, especially for MAC and routing protocols. Network self-organization and topology control algorithms are generally needed. Topology-aware MAC and routing protocols can significantly improve the performance of WMNs.
- *Broadband and QoS.* Different from other ad hoc networks, most applications of WMNs are broadband services with various QoS requirements. Thus, in addition to the end-to-end transmission delay and fairness, more performance metrics such as delay jitter, aggregate and per-node throughput, and packet loss ratios, must be considered by communication protocols.
- *Compatibility and interoperability.* It is a desired feature for WMNs to support network access for both conventional and mesh clients. Thus, WMNs need to be backward compatible with conventional client nodes; otherwise, the motivation of deploying WMNs will be significantly compromised. Integration of WMNs with other wireless networks requires certain mesh routers to have the capability of interoperation among heterogeneous wireless networks.
- *Security.* Without a convincing security solution, WMNs will not be able to succeed due to the lack of incentives by customers to subscribe to reliable services. Although many security schemes have been proposed for wireless LANs, they are still not ready for WMNs. For instance, there is no centralized trusted authority to distribute a public key in a WMN owing to the distributed system architecture. The existing security schemes proposed for ad hoc networks can be adopted for WMNs, but several issues exist.
 - Most security solutions for ad hoc networks are still not mature enough to be practically implemented.
 - The network architecture of WMNs is different from a conventional ad hoc network, which causes differences in security mechanisms.

As a consequence, new security schemes ranging from encryption algorithms to security key distribution, secure MAC and routing protocols, intrusion detection, and security monitoring need to be developed.

- *Ease of use.* Protocols must be designed to enable the network to be as autonomic as possible, in the sense of automatic power management, self-organization, dynamic

topology control, robust to temporary link failure, and fast network-subscription/user-authentication procedure. In addition, network management tools need to be developed to efficiently maintain the operation, monitor the performance, and configure the parameters of WMNs. These tools together with the autonomic mechanisms in protocols enable rapid deployment of WMNs.

