CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

Part I

Introduction

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

1 History of Wireless Networks

1.1 Introduction

The wireless arena has been experiencing exponential growth in the past decade. We have seen great advances in network infrastructures, rapid growth of cellular network users, the growing availability of wireless applications, and the emergence of omnipresent wireless devices such as portable or handheld computers, personal digital assistants (PDAs), and cellular phones, all becoming more powerful in their applications. The mobile devices are becoming smaller, cheaper, more convenient, and more powerful. They can also run more applications on the network services. For example, mobile users can rely on their cellular phones to check e-mail and browse the Internet. They can do so from airports, railway stations, cafes, and other public locations. Tourists can use the global positioning system (GPS) terminals installed in cars to view driving maps and locate attractions. All these factors are fueling the explosive growth of the cellular communication market. As of 2006, the number of cellular network users approached two billion worldwide. Market reports from independent sources show that worldwide cellular users have been doubling every 1.5 years.

In addition to that of the traditional cellular networks, an exponential growth of the wireless access point (AP), which is a device that connects wireless communication devices together to create a wireless network, is also being experienced. The AP is usually connected to a wired network and can relay data between devices on each side. Many APs can be connected together to create a larger network, which is a so-called *ad hoc network*. Low-cost, easily installed APs grew rapidly in popularity in the late 1990s and early 2000s. According to a new research study from Pyramid Research, WiFi users will outnumber cellular users by 2007. This trend will put increasing pressure on wireless operators to bundle both types of access. Currently, most of the connections among wireless devices occur over fixed-infrastructure-based service providers or private networks. Although the research and development efforts devoted to traditional wireless networks are still considerable, the interest of the scientific and industrial community of telecommunications has recently shifted to more challenging ad hoc wireless networks, in which a group of (potentially mobile) units equipped with radio transceivers can communicate without any fixed infrastructure. We will soon see a convergence of seamless networks that will keep everyone connected from their home to their office and all points in between. In addition, with the breakdown of traditional communications

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

infrastructures during the recent Hurricane Katrina catastrophe, the need for reliable connectivity in order for emergency responders to talk to each other is even greater.

1.2 Different Wireless Networks

A number of different wireless networks exist and can be categorized in various ways depending on the criteria chosen for their classification, such as network architecture and communication coverage area.

Based on Network Architecture

Wireless networks can be divided into two broad categories based on how the network is constructed, i.e., the underlying network architecture.

1. **Infrastructure-based networks:** An infrastructure-based network is a network that has a preconstructed infrastructure that is made of a fixed network structure (typically, wired network nodes and gateways). Network services are delivered via these preconstructed infrastructures. For example, cellular networks are infrastructure-based networks, which are built from public-switched telephone network (PSTN) backbone switches, mobile switching centers (MSCs), base stations, and mobile hosts. Each node of the network has its specific responsibility in routing the data, and the connection establishment follows a strict signaling sequence among the nodes. Another example of infrastructure-based networks are wireless local-area networks (WLANs).
2. **Infrastructureless networks:** An infrastructureless network is a network that is formed dynamically through the cooperation of an arbitrary set of independent wireless devices. There is no prearrangement of the specific roles for each node. Typically, each node is assumed to be able to forward the data packets for any other node if it is asked to do so. Each node can independently make its own decision based on the network situation. Examples of infrastructureless wireless networks include mobile ad hoc networks and wireless sensor networks.

Another classification criterion for wireless networks is based on the communication coverage area of the networks.

Based on Communication Coverage Area

As with wired networks, wireless networks can be categorized into different types of networks based on the distances over which the data are transmitted.

1. **Wireless wide-area networks (WWANs):** WWANs are infrastructure-based networks that rely on networking infrastructures to enable mobile users to establish wireless connections over remote networks. These connections often could be over a very large geographic areas (across cities or even countries) through the use of multiple antenna sites or satellite systems maintained by wireless service providers. Examples of WWANs include cellular networks and satellite networks.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

2. **Wireless metropolitan-area networks (WMANs):** WMANs are also infrastructure-based networks that enable users to establish broadband wireless connections among multiple locations within a metropolitan area without the high cost of laying fiber or copper cabling lines. Both radio waves and infrared light can be used in WMANs to transmit data. The U.S. Institute of Electrical and Electronics Engineers (IEEE) set up a specific 802.16 Working Group on Broadband Wireless Access Standards that develops standards and recommended practices to support the development and the deployment of WMANs.
3. **Wireless local-area networks (WLANs):** WLANs enable users to establish wireless connections within a local area, typically within a corporate or campus building or in a public space such as an airport. The connections are typically within a 100-m range. WLANs can operate in an infrastructure-based mode or in an infrastructureless mode. In the infrastructure-based mode, wireless stations connect to wireless APs that serve as bridges between the stations and an existing network backbone. In the infrastructureless mode, several wireless stations within a limited area form a temporary network without using the wireless APs if they do not require access to outside network resources. Typical examples of WLAN implementations include 802.11 (also called WiFi) and Hiperlan2.
4. **Wireless personal-area networks (WPANs):** WPAN technologies enable users to establish ad hoc wireless communication among personal wireless devices such as PDAs, cellular phones, or laptops that are within a personal operating space. A WPAN operates in infrastructureless mode, and the connections are typically within a 10-m range. Two key WPAN technologies are Bluetooth and infrared light. Bluetooth is a cable-replacement technology that uses radio waves to transmit data to a distance of up to 10 m, whereas infrared can connect devices within a range of 1 m. WPAN implementations often have low complexity, lower power consumption, and are interoperable with 802.11 networks.

1.2.1 Wireless Cellular Networks

First-Generation Mobile Systems

The first generation of analog cellular systems included the Advanced Mobile Telephone System (AMPS), which was made available in 1983. It was first deployed in Chicago, with a service area of 2100 square miles. AMPS offered 832 channels, with a data rate of 10 kilobits per second (kbps). Although omnidirectional antennas were used in the earlier AMPS implementation, it was realized that using directional antennas would yield better cell reuse. In fact, the smallest reuse factor that would fulfill the 18-db signal-to-interference and noise ratio (SINR) by use of 120-deg directional antennas was found to be 7. Hence, a 7-cell reuse pattern was adopted for the AMPS. Transmissions from the base stations to mobiles occur over the forward channel by use of frequencies between 869 and 894 MHz. The reverse channel is used for transmissions from mobiles to the base station, with frequencies between 824 and 849 MHz.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

In Europe, the Total Access Communications System (TACS) was introduced with 1000 channels and a data rate of 8 kbps. AMPS and TACS use the frequency-modulation (FM) technique for radio transmission. Traffic is multiplexed onto a frequency-division multiple-access (FDMA) system. In Scandinavian countries, the Nordic Mobile Telephone is used.

Second-Generation Mobile Systems

Compared with first-generation systems, second-generation (2G) systems use digital multiple-access technology, such as time-division multiple access (TDMA) and code-division multiple access (CDMA). The Global System for Mobile Communications, or GSM, uses TDMA technology to support multiple users. Examples of 2G systems are the GSM, cordless telephone (CT2), personal-access communications systems (PACSs), and digital European cordless telephone (DECT4).

A new design was introduced into the MSC of 2G systems. In particular, the use of base station controllers (BSCs) lightens the load placed on the MSC found in first-generation systems. This design allows the interface between the MSC and the BSC to be standardized. Hence, considerable attention was devoted to interoperability and standardization in 2G systems so that a carrier could employ different manufacturers for the MSCs and BSCs. In addition to enhancements in MSC design, the mobile-assisted handoff mechanism was introduced. By sensing signals received from adjacent base stations, a mobile unit can trigger a handoff by performing explicit signaling with the network.

2G protocols use digital encoding and include the GSM, digital AMPs (D-AMPS) (TDMA), and CDMA (IS-95). 2G networks are in current use around the world. The protocols behind 2G networks support voice and some limited data communications, such as faxing and short messaging services (SMSs), and most 2G protocols offer different levels of encryption and security. Although first-generation systems support primarily voice traffic, 2G systems support voice, paging, data, and fax services.

2.5G Mobile Systems

The move into the 2.5G world began with the General Packet Radio Service (GPRS). GPRS is a radio technology for GSM networks that adds packet-switching protocols, a shorter setup time for Internet service provider (ISP) connections, and the possibility of charging by the amount of data sent rather than by connection time. Packet switching is a technique whereby the information (voice or data) to be sent is broken up into packets of, at most, a few kilobytes each, which are then routed by the network between different destinations based on addressing data within each packet. Use of network resources is optimized as the resources are needed only during the handling of each packet.

The next generation of data heading toward third-generation (3G) and personal multimedia environments builds on the GPRS and is known as the enhanced data rate for GSM evolution (EDGE). EDGE is also a significant contributor in 2.5G. It allows GSM operators to use existing GSM radio bands to offer wireless multimedia Internet-protocol-(IP-) based services and applications at theoretical maximum speeds of 384 kbps with

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

a bit rate of 48 kbps per time slot and up to 69.2 kbps per time slot in good radio conditions. EDGE will let operators function without a 3G license and compete with 3G networks offering similar data services. Implementing EDGE will be relatively painless and will require relatively small changes to network hardware and software because it uses the same TDMA frame structure, logic channel, and 200-kHz carrier bandwidth as today's GSM networks. As EDGE progresses to coexistence with 3G wideband CDMA (WCDMA), data rates of up to asynchronous-transfer-mode- (ATM-) like speeds of 2 Mbps could be available.

The GPRS will support flexible data transmission rates as well as a continuous connection to the network. The GPRS is the most significant step toward 3G.

Third-Generation Mobile Systems

3G mobile systems face several challenging technical issues, such as the provision of seamless services across both wired and wireless networks and universal mobility. In Europe, there are three evolving networks under investigation: Universal Mobile Telecommunications Systems (UMTSs), Mobile Broadband Systems (MBSs), and WLANs.

The use of hierarchical cell structures is proposed for IMT2000. The overlaying of cell structures allows different rates of mobility to be serviced and handled by different cells. Advanced multiple-access techniques are also being investigated, and two promising proposals have evolved, one based on WCDMA and another that uses a hybrid TDMA–CDMA–FDMA approach.

1.2.2 Wireless Access Points

A wireless AP is a device that connects wireless communication devices together to create a wireless network. The AP is usually connected to a wired network and can relay data between devices on each side. Many APs can be connected together to create a larger network that allows "roaming." In contrast, a network in which the client devices manage themselves is called an ad hoc network.

Low-cost, easily installed APs grew rapidly in popularity in the late 1990s and early 2000s. These devices offered a way to avoid tangled messes of cables associated with typical Ethernet networks of the day. Wireless networks also allowed users greater mobility, freeing individuals from the need to be stuck at a computer cabled to the wall. On the industrial and commercial side, wireless networking had a big impact on operations: Employees were often equipped with portable data terminals integrating bar-code scanners and wireless links, allowing them to update work-in-progress and inventory in real time.

One IEEE 802.11 AP can typically communicate with 30 client systems within a radius of 100 m. However, the communication range can vary a lot, depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, type of antenna, the current weather, operating radio frequency, and power output of the device. The range of APs can be extended through the use of repeaters and reflectors,

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

which can bounce or amplify radio signals that ordinarily could not be received. Some experiments have been carried out to allow wireless networking over distances of several kilometers.

A typical corporate use of an AP is to attach it to a wired network and then provide wireless client adapters for users who need them. Within the range of the AP, the wireless end-user has a full network connection with the benefit of mobility. In this instance, the AP is a gateway for clients to access the wired network. Another use is to bridge two wired networks for which cable is not appropriate; for example, a manufacturer can wirelessly connect a remote warehouse's wired network with a separate (though within line of sight) office's wired network.

An AP may also act as the network's arbitrator, negotiating when each nearby client device can transmit. However, in the vast majority of currently installed IEEE 802.11 networks, this is not the case, as a distributed pseudo-random algorithm is used instead.

Limitations

There are only a limited number of frequencies legally available for use by wireless networks. Usually, adjacent APs will use different frequencies to communicate with their clients in order to avoid interference between the two nearby systems. Wireless devices are able to "listen" for data traffic on other frequencies and can rapidly switch from one frequency to another to achieve better reception on a different AP. However, the limited number of frequencies becomes problematic in crowded downtown areas with tall buildings housing multiple APs because there can be enough overlap between the wireless networks to cause interference.

Wireless networking is far behind wired networking in terms of bandwidth and throughput. Whereas (as of 2007) typical wireless devices for the consumer market can reach speeds of 11 (IEEE 802.11b) or 54 megabits per second (Mbit/s) (IEEE 802.11a, IEEE 802.11g), wired hardware of similar cost reaches 1000 Mbit/s (Gigabit Ethernet). One impediment to increasing the speed of wireless communications is that WiFi uses a shared communications medium, so the actual usable data throughput of an AP is somewhat less than half the over-the-air rate. Thus, a typical 54-Mbit/s wireless connection actually carries TCP/IP (TCP stands for transmission control protocol) data at 20 to 25 Mbit/s. Because users of legacy wired networks are used to the faster speeds, people using wireless connections are anxious to see the wireless networks catch up.

Security

Another issue with wireless access in general is the need for security. Many early APs were not able to discern whether a particular user was authorized to access the network. Although this problem reflects issues that have long troubled many types of wired networks (it has been possible in the past for individuals to plug computers into randomly available Ethernet jacks and get access to the network), this was usually not a significant problem because many businesses had reasonably good physical security. However, the fact that radio signals bleed outside of buildings and across property lines means that physical security is not as much of a deterrent to war drivers.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

In response, several new security technologies have emerged. One of the simplest techniques involves only allowing access from certain medium-access control (MAC) addresses. However, MAC addresses can be easily spoofed, leading to the need for more advanced security measures. Many APs incorporate a wired equivalent privacy (WEP) encryption, but that also has been criticized by many security analysts as not good enough (the U.S. FBI demonstrated the ability to break WEP protection in 3 min). Newer (as of 2005) encryption standards available on wireless APs and client cards include WiFi protected access, WPA and WPA2 modes, both of which offer substantial improvements in security. The WiFi alliance has announced the inclusion of additional Extensible Authentication Protocol (EAP) types to its certification program for WPA- and WAP2-Enterprise. Also, a newer system for authentication, IEEE 802.1x, promises to enhance security on both wired and wireless networks. Wireless APs that incorporate technologies like these often also have routers built in, so they are somewhat more accurately described as wireless gateways.

1.2.3 Wireless Ad Hoc Networks

A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. The wireless nodes communicate over wireless links; thus, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, as the connectivity among the nodes may vary with time because of node departures, new node arrivals, and the change of environments. Hence, there is a need for efficient routing protocols to allow the nodes to communicate over multihop paths. Some of these features are characteristic of the type of packet radio networks that were studied extensively in the 1970s and 1980s. Recently, the wireless ad hoc networking research has received much attention from academia, industry, and government. Because these networks pose many complex issues, there are many open problems for research and opportunities for making significant contributions.

There are two major types of wireless ad hoc networks: mobile ad hoc networks and smart sensor networks.

Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) is a self-configuring wireless network composed of wireless devices. Figure 1.1 illustrates an example of an ad hoc network formed by eight laptop computers. In the figure, two computers are connected by a line if they can communicate directly with each other by using their wireless cards. In this case, we say they are within the transmission range of each other. The wireless devices are free to move randomly and organize themselves arbitrarily. Consequently, the network topology may change rapidly and unpredictably. A MANET network may operate in a

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

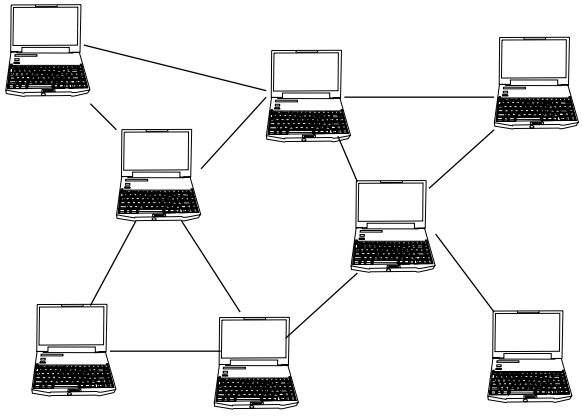

Figure 1.1 An ad Hoc network example.

stand-alone fashion or may be connected to the larger Internet. Because of their minimal configuration and quick deployment, ad hoc networks are often suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations, and so on.

The earliest MANETs were called "packet-radio" networks, first sponsored by the U.S. Defense Advanced Research Projects Agency (DARPA) in the early 1970s. It is interesting to note that some early packet-radio systems predated the Internet and, indeed, were part of the motivation of the original Internet protocol (IP) suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. The third wave of academic activity on wireless ad hoc networks started in the 1990s, especially with the wide usage of inexpensive 802.11 radio cards for personal computers.

The popular IEEE 802.11 ("WiFi") wireless protocol incorporates an ad hoc networking system when no wireless APs are present. In an IEEE 802.11 system, each node transmits and receives data but does not route anything between the network's systems. Notice that it is possible to design higher-level protocols to aggregate various IEEE 802.11 ad hoc networks into MANETs.

Because of the growing interests in establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks, there is a strong need for the rapid deployment of independent mobile users. Obviously, we cannot rely on a centralized and organized network structure for these application scenarios. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth-constrained wireless links, for which all network activity including discovering the topology and delivering messages must be executed by the nodes themselves.

The design of network protocols for these networks is a complex issue. A unique characteristic of wireless networks is that the radio signal sent out by a wireless terminal will be received by all the terminals within its transmission range and also possibly causes signal interference to some terminals that are not intended receivers. In other words, the

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86523-4 - Wireless Ad Hoc and Sensor Networks: Theory and Applications
Xiangyang Li
Excerpt
More information

communication channels are shared by the wireless terminals. Thus, one of the major problems facing wireless networks is the reduction of capacity because of interference caused by simultaneous transmissions. Using multiple channels and multiple radios can alleviate but not eliminate the interference. This raises the scalability issue of all wireless networks (MANETs, WSNs).

Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining feasible routing paths and delivering messages in a decentralized environment where network topology fluctuates over time is not an easy problem, and, to some extent, it is even not a well-defined problem. Although the shortest path (based on a given cost function) from a source to a destination in a static wired network is usually the optimal route, this idea is not easily extended to MANETs. A number of unique characteristics of wireless networks make the "simple" optimal unicast routing much harder. For example, various factors, such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. Notice that finding the path (or even multiple paths) with the largest throughput to connect a given pair of source and target nodes in a wireless network is already a nondeterministic-polynomial- (NP-) hard problem even if only the wireless interference (interpath interference and intrapath interference) is considered. Moreover, in many applications such as a military environment, preservation of security, achieving small latency, reliability, preventing intentional jamming, and recovery from failure are significant concerns. This will make the design of a good wireless protocol much harder. Additionally, in certain applications (especially military networks), we need to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible. A lapse in any of these requirements may degrade the performance and dependability of the network. Although there are so many challenges in designing secure and efficient wireless ad hoc networks, this book is not intended to (and, clearly, it is impossible to) solve all important and interesting problems here. Some of the algorithmic and graph theoretical issues that can form a foundation for further study of some of the problems not addressed here are covered.

Wireless Sensor Networks

Most sensors are electrical or electronic, although other types exist. A sensor is a type of transducer. Sensors are either direct indicating (e.g., a mercury thermometer or electrical meter) or are paired with an indicator [perhaps indirectly through an analog-to-digital (A/D) converter, a computer, and a display]. Sensors are heavily used, in addition to other applications, in medicine, industry, and robotics. With the technical progress, more and more sensors are manufactured with Micro-Electro-Mechanic-Systems (MEMS) technology. This often offers the potential of reaching a much higher sensitivity. A good sensor obeys the following rules:

1. The sensor should be sensitive to the measured property.
2. The sensor should be insensitive to any other property.
3. The sensor should not influence the measured property.

© Cambridge University Press www.cambridge.org