# Wireless Connectivity

### Content

Abstract

### **Introduction**

**Operation**

### **Wireless Application Design**

**Caching**

**Prefetching**

**Data reduction**

**Mobile WWW Browsers**

**Active documents**

**Dynamic URLs**

### **Data over Cellular links**

Radio-based wireless connectivity

IEEE 802.11 protocol

#### **Interworking Units for wireless connectivity**

### **Internet Mobile Host Protocol**

**IP Tunneling**

### Abstract

Traditional networking technologies offer tremendous capabilities from an office or home via the Web. But, limitations to networking through the use of wired-based systems exist because you cannot utilize these network services unless you are physically connected to the system. As mobile computing becomes more prevalent, systems and applications must deal with scarcity of resources such as bandwidth. Mobile devices and wireless workstations should handle some of the work that has been traditionally carried-out by the network through techniques such as document partitioning. Dynamic documents can also be used to cache and prefetch documents while the network connection is not being utilized fully.

Meanwhile, the need for higher speed wireless connections is growing with multimedia rich contents on the World Wide Web (WWW). The IEEE 802.11 protocol and the Medium Access Control part of the protocol (DFWMAC) will allow wireless networks to operate at high data rates (1 to 20 Mbps). Furthermore, the 802.11 only effects the bottom two layers of the OSI's seven layered architecture; hence, through an access point (Router), wireless packets are routed to the Web.

### ****Introduction****

Wireless LANs will provide the first layer of connectivity between mobile users and the global information infrastructure. Wireless devices such as Personal Digital Assistants (PDAs) and Notebooks will be an extension of the Web. The user should not know nor care whether the information travels over a wire or a radio frequency. Depending on the power of the transmitters and the sensitivity of the receivers, wireless devices may become the first truly universal form of virtual LAN. By mixing the wireless Networks with other wireless communication technologies such as cellular and satellite, the user can have full connectivity at all times and more importantly everywhere on the globe.

Wireless connectivity to the web can also be achieved through the use of existing cellular telephone links. Using Spread Spectrum Technologies (SST) such as time-division multiple access (TDMA), code-division multiple access (CDMA) and extended time-division multiple access (ETDMA) has allowed the cellular links to carry more information and as a result better suited for data transmission. Although the overhead in cellular data transmission is somewhat high, but data reduction techniques, and caching is used to reduce network latency.

With the Introduction of PDA, people began to see the natural progression of Wireless technology into these devices. However, the current state of these devices has obvious limitations. Computational power, storage, communication bandwidth, display size and power consumption are just a few of these limitations. Nevertheless, presently such devices are running Web browser, mail clients and etc.Presently there is a variety of pen based computer systems like palmtops, notebooks and different versions of what John Sculley, Apple's vice president in 1992 introduced as a PDA.

Personal communication is the primary motivation for wireless connectivity, but in addition, wireless users need access to on-line information in real time. There are three reasons why users need to be connected to the Web. First, it is often difficult, if not impossible, to determine the data of interest ahead of time and download it to the hand-held device. Second, even then, space limitations may prevent caching of all data. Finally, some data changes dynamically with time such as weather forecast, or stock market activities. (Watson, 1994)

The current application environment is ill-suited for the wireless Web, the wired web squanders bandwidth through unusable information on the client's side. In the wired world these inefficiencies amount to only milliseconds, but as the bandwidth is reduced over wireless links, milliseconds can add up to seconds and perhaps time-outs by the underlying protocols such as TCP/IP. As a result various groups have proposed new HyperText Mark-up Language (HTML) or new protocols such as HTTP+. But these avenues of solutions are rigid and the need for standardization is greater than a temporary increase in throughput for a particular scheme.

### ****Operation****

Similar to any transmission system, a wireless system needs a transmitter, a receiver and a transmission medium. In a wireless system, the transmission medium is air rather than the cables used by conventional wired systems. The use of air as a transmission medium utilizes two major spectra: infrared and radio frequency.

The key difference between the use of infrared and radio frequency is the support of roaming. Infrared is a line-of-sight technology. There has to be a direct line of sight or at least a surface to bounce the waves from the transmitter to the receiver. On the other hand, radio frequency systems can penetrate through objects such as walls and doors in most office buildings; hence their popularity in present wireless systems. FCC rules allow only small sections of the electromagnetic spectrum (figure below) to be used for wireless data networks; thus techniques are needed to avoid interference from other devices that share the space or perhaps multiple stations using the same frequency.

A technique developed by the military in the 1970s to help secure transmissions offers a way around this problem. This technique is called Spread Spectrum Technology (SST). It involves spreading transmissions across a range of frequencies, rather than transmitting on one frequency all the time.

One approach known as Frequency-Hopping Spread Spectrum (FHSS) involves dividing a range of the radio spectrum into individual channels, each on a specific frequency. A transmitter can hop from one channel to the next and if the receiver is aware of the hopping pattern of the transmitter, it can follow the pattern and receive the information. The second method of spread spectrum is Direct Sequence Spread Spectrum (DSSS). The source data to be transmitted is first exclusive ORed with a pseudorandom binary sequence. The bits making up the sequence are random but the same sequence is made much larger than the source data rate. When this data is modulated and transmitted it occupies a wider frequency band than the original source data bandwidth. This would make the signal appear as noise to any other devices using the same frequency spectrum. All the members of this wireless system know the binary sequence being used .(Halsall, 1996) Thus, all receivers first search for the known preamble sequence, once it has been recognized, the receivers start to interpret the bit stream.

FCC rules for DSSS transmission requires 10 or more redundant data bits to be added to each signal. This limits the maximum throughput of DSSS transmitters to approximately 2 Mbps when using the 902-MHz band, and approximately 8 Mbps in the 2.4-GHz band.

### ****Wireless Application Design****

Designing a web application for a wireless node is different from designing a web application for a workstation. Bandwidth is a precious resource in the wireless domain and it must be utilized in the most efficient fashion. Research focuses on streamlining applications to make the best use of the available bandwidth. These options include using dynamic documents which use the resources of the mobile node itself to generate parts of a document or partitioning the application between a client and the server.

Dynamic documents can address the variable resources requirement of mobile computers accessing the Web. Dynamic documents are programs executed by programs such as Web browsers in order to generate the actual information displayed to the user. Execution of a dynamic document cause the client to perform any number of actions in order to generate a final presentation to the user. Dynamic documents are flexible enough to address many mobile computing resource constraints. Documents can be customized at the client depending on available resources. (Kaashoek, 1994)

Application partitioning can also be used over a wireless link for more effective use of the wireless link. Much like a client/sever system, applications and their functionality can be divided into different parts. the boundaries between how much of the application should be run on the client side vs. the server side can be determined dynamically and based upon the availability of the bandwidth. The data and their functions are packaged into hyperobjects. The purpose of hyperobjects is to expose a certain level of application structure and semantics to the system in a uniform and manageable way. The system will use this hyperobject structure, along with observations of access patterns to make informed decisions. (Watson, 1995)

Partitioning documents are combined with several other well-known techniques to increase the effectiveness of wireless clients such as browsers.

**Caching**

Applications specify the caching attributes of an object or a number of objects. The default is to optimistically replicate objects on the mobile device. Explicit synchronization can be used to make the cache consistent with the wired network if the wireless link is up. (Watson, 1995)

**Prefetching**

As a document is loaded and displayed on a mobile device, the links in a hiarchial fashion are used to prefetch the relevant documents and cached. In a hyperobject application the system will use its knowledge of the relevancy and the position of various objects in order to anticipate and prefetch other objects. Prefetching can only be done if the system resources allow it. For example, as a user is viewing the first page of a document, the relevant objects for that document are being prefetched into the cache, given the wireless link is up and functioning. Prefetching hides the latency of the link, and it will also filter the burstiness by spreading the traffic over a longer time.

**Data reduction**

Data reduction can be dynamically decided by the user for various high bandwidth applications such as video transmissions. A video stream delivers certain number of frames per constant unit of time. As the number of frames are reduced, it adversely affects the quality of the video, but the bandwidth needed is also reduced; hence, the user can dynamically find a balance between what the available resources and the desired video quality. The same principal can be applied to the sound, and also any real-time stream of data over the wireless link.

**Mobile WWW Browsers**

Web infrastructure as it exists today can not easily accommodate mobile clients, because of the fact that almost all information resides statically in HTML documents. The dynamic information that the Web supports is returned to the client without incorporating any user context, or is incorporated explicitly using forms-based interfaces that require user input on the client. Extensions to the Web have been created to include:

* A network server that maintains mobile computing contexts within a client-specific domain.
* An asynchronous callback mechanism to notify Web clients when a user's dynamic computing environment changes.
* A syntax for referencing dynamic information in URLs and documents. (Voelker)

**Active documents**

Active documents are HTML documents that allow the Web client to automatically react to changes in mobile computing environment. If the information in an active document that the client is displaying becomes invalid, then the client can be notified of that change so that more relevant information can be displayed. Variables such as location can be updated as the mobile user roams from one cell area to the next. Active documents are written just like any other HTML file with only a minor addition. A subscribe command is embedded in an HTML comment line. By having the subscribe command embedded in a comment line, backward compatibility can be preserved, thus allowing regular Web browsers to view the documents. (Voelker)

**Dynamic URLs**

Ordinarily URLs are links to set static documents on the Web. Dynamic URLs will reference a user to a different document based upon other variables, such as the location variable. Dynamic URLs exist in active documents in order to receive the variables from the client. When a user selects a dynamic URL in a document, the client browser is responsible for resolving all references to dynamic variables within the URL. When all variable references have been resolved, the result is a standard URL that the client then sends to the server. (Voelker)

### ****Data over Cellular links****

The analog cellular telephone system uses FM (Frequency Modulation) radio waves to transmit voice grade signals. To accommodate mobility, this cellular system switches radio connection from one cell to another as the mobile user moves from one cell to another (roaming). Every cell within the network has a transmission tower that links mobile callers to a Mobile Telephone Switching Office (MTSO). The MTSO, which is owned and operated by the cellular carrier in each area provides a connection to the public switched telephone network. The public telephone networks acts also as gateways to the Internet.

Most modems that operate over wireline telephone services will also interface and interoperate with cellular phones; however, modem software optimized to work with cellular phones minimizes battery usage. There are problems with modem communication over cellular links. The first problems occurring were the hand-off problems or roaming. As a mobile user moves from one service area to the next, a hand-off occurs from one service area to the next. The hand-off would disrupt the call for 100 to 200 ms. This is just enough to disrupt the carrier detect (CD) cycle; hence, the modem assumes that one of the callers has disconnected, and it hangs up. This problem can be overcome similar to fax modems over cellular links. The modem will delay 400 ms before hanging up, giving the hand-off enough time to take place. Some data might be affected, but error detection, and error correction procedures (CRCs) will detect and correct the data bits that have been corrupted. But, all these techniques lower the effective throughput of our communication system and the effective throughputs achieved with cellular modems hover around 19200 bits/s. (Bates, Gregory, 1995)

To establish a dedicated wireless data network for mobile users, a consortium of companies in the United States developed the Cellular Digital Packet Data (CDPD) standard. CDPD overlays the conventional analog cellular telephone system, using a channel hopping technique (previous section) to transmit data in short bursts during idle times in cellular channels. CDPD operates full duplex, meaning simultaneous transmission in both directions in the 800 and 900 MHz frequency bands. The main advantage of the analog cellular system is widespread coverage. Since CDPD piggybacks on this system, it will also provide nearly worldwide coverage. The main advantage with CDPD is that, it uses digital signals, making it possible to enhance the transmission of data. With digital signaling, it is possible to encrypt the data stream and provide easier error control. CDPD is a robust protocol that is connectionless and corrects errors at the receiver side without asking the source to retransmit the errored packet.

Other digital techniques presently being tested and utilized by the carrier companies are:

* Time-division multiple access (TDMA)
* Extended time-division multiple access (ETDMA)
* Code-division multiple access (CDMA)
* Narrowband advanced mobile phone service (N-AMPS)

In the case of ETDMA the bandwidth can be increased by a factor of 15, making it much more acceptable for today's application needs.

### Radio-based wireless connectivity

The most widely sold wireless LAN products use radio waves as a medium between computers and the WEB or each other. An advantage of radio waves over other forms of wireless connectivity such as infrared and microwaves is that they propagate through walls and other obstructions with little attenuation. Even though several walls might separate the user from the server or an access point to the Web, users can maintain connections to the network, thus supporting true mobility. The disadvantage for radio frequencies is that governments manage the region and not all the spectrum can be used everywhere; hence, techniques such as FHSS and DSSS (as described ) must be used.

There are three regions of the E-M spectrum utilized by these waves:

* 902-928 MHz
* 2.4-2.484 GHz
* 5.725-5.850 GHz

Presently Metricom is operating a two way radio based multi-user data communications system is San Francisco called Ricochet. The architecture is shown below:

The concept is to use wireless access points and network radio relays approximately one half mile apart to facilitate connectivity between users. The radios operate in the license-free 902-928 portion of the radio spectrum using FHSS. The underlying network protocol is TCP/IP, allowing it to interact with the Internet seamlessly.

An important goal for wireless communications has been to make the application layer transparent to the underlying protocol (TCP/IP) in order to have more acceptability by the Web users. To understand the kind of standards developed for wireless networks, it helps to see the affected layers in an OSI (Open System Interconnect) model. The bottom two layers are the ones of interest to us. At the very bottom is the Physical layer. This layer defines the electrical characteristics of the actual connection between network nodes. For wired networks, it covers topics like voltage levels and type of cabling. But for wireless networks, it addresses areas such as frequencies used and modulation techniques, including spread-spectrum technologies.

The next layer up is the Data Link Layer. It deals with how the network is shared between nodes. The Data Link Layer defines rules such as who can talk on the network, how long they can occupy network resources. This layer can be further divided into two separate layers (shown below).

* The Medium Access Control (MAC) layer.
* The Logical Link Control (LLC) layer.

The first five layers of the OSI model remains unchanged; hence, TCP and IP can be implemented in their respective layers.

### IEEE 802.11 protocol

The wireless network interface manages the use of air through the operation of a communications protocol. For synchronization, wireless networks employ a carrier sense protocol similar to the common Ethernet standard. This protocol enables a group of wireless computers to share the same frequency and space.

The lack of standards has been a significant issue with wireless networking. In response to this problem, the Institute for Electrical and Electronic Engineers (IEEE) has been involved in the development of wireless LAN standards for the last seven years. This effort is nearly complete, and the final standard (IEEE 802.11) will be ready by May of 1997.

As with other 802 standards such as Ethernet and token ring, the primary service of the 802.11 standard is to deliver MSDUs (MAC Service Data Units) between LLC (Logical Link Control) connections to the network. In other words, the 802.11 standard will define a method of transferring data frames between network adapters without wires. In addition, the 802.11 standard will include:

* Support of asynchronous and time-bounded delivery service
* Continuity of service within extended areas
* Accommodation of transmission rates between 1 and 20 Mbps
* Support of most market applications
* Multicast service
* Network management services, Registration and authentication services

The IEEE 802.11 standard supports operation in two separate modes, a distributed coordination (DCF) and a centralized point-coordination mode (PCF). The IEEE 802.11 MAC is called DFWMAC (Distributed Foundation Wireless MAC), and the access mechanism is based upon the principal of CSMA/CA (Collision Sense Medium Access with Collision Avoidance), which is another adaptation of CSMA/CD used by Ethernet networks.

Under CSMA/CD, when a station has data to send, it first listens to determine whether any other station on the network is occupying the medium. If the channel is busy, the station will wait until it becomes idle before transmitting data. Since it is possible for two stations to listen at the same time and discover an idle channel, it is also possible that two stations could then transmit at the same time. When this occurs a collision will take place, and then a jamming signal is sent throughout the network in order to notify all stations of the collision. The stations will then wait for a random period of time before re-transmitting their respective frames.

CSMA/CA is a modified version of the CSMA/CD access system. Under the CSMA/CA technique, as before stations are listening to the medium at all times. A station that is ready to transmit a frame will sense the medium, if the medium is busy, it will wait for an additional predetermined time period of DIFS (DCF Interframe Space) length and then, based upon a random calculation, picks a time slot within a contention window to transmit its frame. If there were no other transmissions before this time slot has arrived, it will start transmitting its frame. On the other hand if there were transmissions by other stations during this back-off time period, the station will freeze its counter and will pick-up the count where it left off after the other station has completed its frame transmission. The collisions can now occur only when two or more stations select the same time slot to transmit. These stations will have to reenter the contention procedure to select new time slots to transmit the collided frames. The figure below illustrates DFWMAC access scheme.

#### ****Interworking Units for wireless connectivity****

Just as in wired networks, the interworking unit (IWU) provides the protocol manipulation to connect networks with different protocols together. The IWUs act as access points between wireless stations and the Web. They address issues such as:

* Correct delivery of data to its destination.
* Congestion control.
* Differences in maximum PDU sizes.

To connect a wireless network that is using the 802.11 protocol to the Internet, IWUs are needed at access points. Access points are nodes that allow traffic flow in and out of the Wireless network. Alternatively, IWUs (IP Routers) control the traffic in and out of the Internet; thus routing wireless packets into and out of the Internet as shown below:

The 802.11 protocol can support data rates of 20 Mbps, thus making it an attractive wireless protocol for Internet connectivity. Companies such as Proxim that have been involved with the development of 802.11, are migrating rapidly to the new standard.

### ****Internet Mobile Host Protocol****

An important part of wireless connectivity is mobility. Mobile computers must be able to move between adjacent cells or across multiple network domains without disturbing the application level process. Mobile users and mobile protocols must not make any changes to the existing TCP/IP Internet protocol to insure connectivity and usability of the Internet as it exists today.

A mobile host is the Internet Mobile Host Protocol (IMHP) entity that roams through the Internet. Each mobile host has a home agent on its home network. Each home agent maintains a list known as a home list. The home list is a list of mobile hosts that the home network will serve and it also maintains the location of each mobile host as the network becomes aware of their locations. As mobile hosts roam from one network to the next, they have to register with foreign agents on new subnets as they try to connect to that network. Foreign agents are much like a home agent except they interact with visiting home agents from other networks. Each foreign agent maintains a list known as the visitor list, which identifies the mobile hosts that are currently registered with it. The combination of the foreign agents address for a particular home agent (care-of-address) along with its home address is known as a binding. A binding defines where to send packets for a particular home agent at any given time. (Perkins, Myles, and Johnson, 1994)

The registration protocol which is part of the IMHP management protocol notifies all the concerned parties of the new mobile host's location. Those include the previous foreign agents and the host's home agent. It is the responsibility of the IMHP management protocol to keep a forwarding pointer from the previous foreign agents until all information about the new location has been updated with the new network and the home network. Time stamps are used to keep visitor lists current and to delete the home agents that have left the network. Figure below shows the registration process for a home agent through a foreign agent and the notification process.

Any node may function as a cache agent by caching the bindings of one or more mobile hosts. All of these cache agents are under the umbrella of the IMHP management protocol which is running on all IMHP agents as long as they are not on their home networks. The IMHP management protocol manages the cache agents in a distributed fashion. This will allow packets to travel to their destinations without having to be routed to a home networks first. Cache agents actively attempt to reconform bindings in their location caches using the IMHP management protocol, and also periodically notifications are send out by the protocol to update caches when agents move in and out of networks.

**IP Tunneling**

IMHP entities direct and send packets to a mobile host's current location using a tunneling technique. Tunneling in IMHP management protocol takes the form of encapsulation. The protocol will add 8 bytes to each packet sent to a mobile host if the sender has a location cache entry for the destination mobile host, otherwise it adds 12 bytes to each packet. The tunneling header is inserted into the packet immediately following the existing IP header. In the IP header, the protocol number is set to indicate the IMHP encapsulation tunneling protocol, and the destination address is set to the mobile host's care-of-address, and finally the source address is set to the IP address of the encapsulating agent. (Perkins, Myles, and Johnson, 1994)

This tunneling procedure will inssure packet delivery throughout the Internet as it exists today, since the intermediate routers will see a normal IP packet. It is only the IMHP network that can recognize the packets by seeing the protocol number and deliver them to their final destination.