Wireless Local Area Networking For Device Monitoring

by

Colin Goldsmith

Supervised By

Professor Wendi Heinzelman

A thesis
submitted in partial fulfillment
of the
Requirements for the
Degree of Masters of Science
in
Electrical and Computer Engineering

University of Rochester
Rochester, New York

2004

Curriculum Vitae

The author was born in Rochester, New York on September 25th, 1981. He attended the University of Rochester from 1999 to 2003, and graduated with a Bachelor of Science in Electrical and Computer Engineering concentrated on VLSI. He then continued his studies at the University of Rochester in the 3-2 Master's program in Electrical and Computer Engineering, concentrating on communications. With the guidance of Professor Wendi Heinzelman, he has researched and developed a wireless local area networking system for device monitoring.

Acknowledgements

I would like to thank Professor Wendi Heinzelman for all her guidance throughout my schooling at the University of Rochester. She has been an integral part in my development as a student through her classes and projects executed under her supervision. In addition, I would like to thank Professors Guarav Sharma, Martin Margala, Jack Mottley, Mark Bocko, and the rest of the Electrical and Computer Engineering faculty and staff at the University Of Rochester for there teaching and support.

I would also like to thank my colleague, Owen Zacharias, in the development of this project for his hard work and friendship. Also I would like to thank Micheal Wieckowski and my other classmates at the University of Rochester for all the experiences we have shared.

Finally, I would like to thank my parents, brother, and fiancé, Arathi Rajendran, for all there support throughout my life and collegiate career.

Abstract

In this thesis, a wireless local area networking technique is developed, which is intended for use in a device monitoring system. A full review of the current wireless local communications protocols 802.11, 802.11a, 802.11b, 802.11g, HomeRF, Bluetooth, and Ultrawideband is presented. A detailed comparison of these techniques is performed with 802.11b, being chosen as the most suitable protocol for the device monitoring system. Finally, a prototype of the wireless local area network for device monitoring is designed with code developed using the Java programming language.

Table of Contents

List of Figures

List of Tables

Chapter 1
Introduction

Wireless local area networking (WLAN) protocols are quickly becoming a standard solution for connecting many different types of devices together. The current local wireless protocols are 802.11, 802.11a, 802.11b, 802.11g, Bluetooth, HomeRF, and Ultrawideband. These protocols, developed within the last seven years, are making it easier to develop a local area network since the need for wires has been removed - a device no longer has to be fixed to a single location by a wire. The device can be moved at any time, and new devices can be introduced to a network with ease.

The supporting company has developed an infrastructure called the Device-Centric services (DCS) that provides a set of device monitoring applications including automated meter reads, product break-notifications, and maintenance support. This infrastructure currently contains a wired network connecting the supporting company's devices into the backbone of their customer's network, where data is transmitted over the Internet into a company database. This current implementation is not compatible with all of the current devices and it requires that the data be transmitted along the customer's network backbone. Utilizing the qualities of a wireless network, these issues can be resolved.

In this thesis, a WLAN will be used for a device monitoring application. The endless possibilities of wireless technologies shall be used to monitor the variables involved in printers, fax machines, scanners, and other devices. Utilizing a WLAN, a device can be polled for data without interfering with the network backbone, the device does not have to be

tethered to a single location and it can be accessed in a remote location that cannot be connected to a wired network.

Wireless technology allows the capability of creating a network that operates separately from the customer's underlying wired network - the device monitoring application can be developed to use its own separate network. A similar system for wireless wide area networking for device monitoring is being developed in parallel with the development of this local area networking solution [21]. When these two systems are integrated together, the device monitoring application will be capable of monitoring devices from a remote location, i.e. from the corporation database server.

1.1 Contributions

This thesis offers a wide range of contributions to the wireless communications research field. It began with a complete review of the common WLAN protocols. From this research, a comprehensive comparison of these protocols was performed with a choice of which protocol fits into the DCS system the "best". Once this protocol has been selected hardware architecture was developed to implement the protocol into the DCS system, with software developed to operate on top of the devise that runs the WLAN protocol. This development leaves the supporting company with a complete solution for converting the DCS system from a wired system to a wireless system. Finally, the thesis presents hardware architecture for integration of this WLAN solution with the wireless wide area networking solution for the creation of a fully wireless device monitoring solution [21].

1.2 Organization

This thesis is organized as follows. Section 2, introduces all the basic communications topics discussed in this thesis. Section 3, describes how the local area network will be organized and the requirements of the device monitoring application being developed. Section 4, reviews the potential wireless protocols to be utilized for the system, and section 5, covers a complete comparison of the protocols and the choice of the most suitable protocol for the device monitoring application. Section 6, describes the hardware implementation of the protocol and other hardware concerns. A detailed explanation of the software developed to implement this protocol is presented in section 7. Finally, section 8 presents the future implement of this system, integrating it with the wide area network application and conclusions.

Chapter 2
Background

In this chapter, the terms and there abbreviations that are used throughout the thesis are described.

2.1 Capacity

Capacity is the maximum data rate that can be achieved by a transmission over a communications medium.

2.2 Pulse Amplitude Modulation (PAM)

PAM is a modulation technique that transmits a symbol by assigning specific amplitude to the transmitted signal for each symbol of a digital signal. This technique is similar to amplitude modulation (AM) in an analog system. In the digital system, a limited number of different amplitudes are mapped to a set of bits. A PAM signal can be defined by a single sinusoidal basis function that is multiplied by specific amplitudes defined by the bits to be transmitted.

2.3 Pulse Position Modulation (PPM) [17]

PPM is a modulation technique similar to PAM except that the magnitude is not adjusted to identify a different symbol. Instead, the symbol is defined by the position in time that a pulse occurs. PPM is commonly used in optical systems where data is typically transmitted as on or off. Therefore, to create a PPM signal the transmission period is broken up into a set of on and off segments. As the on segment is shifted within the set of off segments, the value signifies a different symbol. Refer to Table 2.1 for further detail. This modulation technique

is immune to noise unless a strong interference signal is sent during a transmission. In PPM it is difficult to increase the number of bits per symbol or number of different symbols because the data rate is greatly reduced by keeping the same on or off segment length. If the segment length is decreased to increase the data rate, this will require more complex hardware to transmit shorter on segments.

Data Bits	4-PPM Symbols
01	0001
11	0010
10	0100
00	1000

Table 2.1 4-PPM Symbols

2.4 Frequency Shift Keying (FSK)

FSK is a digital modulation technique that is similar to frequency modulation (FM) in analog devices. The major difference is that FSK only uses a limited number of frequencies. Each digital symbol, for example 101 for 8-FSK, is mapped to a specified frequency. The receiving device must know what symbol each frequency translates to. A major advantage of FSK is that each frequency signal assigned to a symbol is orthogonal to all other FSK signals, which reduces the effects of noise. This orthogonality comes with a cost, as FSK is bandwidth inefficient.

2.5 Orthogonal Frequency Division Multiplexing (OFDM) [17]

OFDM is a modulation technique that breaks the available bandwidth into many smaller bandwidths with carrier frequencies that are close together and orthogonal to one another. This bandwidth is shared by a single set of data that is transmitted in parallel. This allows for

the data on each carrier to have a lower bit rate while increasing the overall bit rate as compared to a system that does not transmit data in parallel.

2.6 Phase Shift Keying (PSK)

PSK is a modulation technique that is similar to phase modulation in analog communication systems. In digital modulation there is a finite set of phases that maps to a specific bit symbol. For example, in binary phase shift keying (BPSK), a bit value of 1 could map to a zero phase positive cosine signal and a bit value of 1 could translate to a zero phase negative cosine wave or a cosine wave, that is 180^{o} out of phase. This means that BPSK has two symbols.

2.7 Quadrature Phase Shift Keying (QPSK)

QPSK is a modulation technique that expands BPSK to four different symbols or two bits per symbol. This is able to send more data in the same bandwidth as BPSK due to the larger number of bits per symbol.

2.8 Differential Phase Shift Keying (DPSK)

DPSK is a modulation technique that balances the in-phase and quadrature modulators. The transmitter modulates two signals with different phase components. When received, the signal is decoded by finding the phase difference between the consecutive signals. This signaling scheme is slightly more reliable than PSK alone because it is often assumed that two consecutive signals will be affected by relatively the same noise, so the phase difference between the signals will remain unchanged.

2.9 Differential QPSK (DQPSK)

DQPSK limits DPSK by only transmitting signals that are 90^{o} out of phase. This limits the number of symbols that can be transmitted in Mary-DQPSK to four symbols or two bits per symbol.

2.10 Differential Binary PSK (DBPSK)

DBPSK limits DPSK further by only transmitting symbols that are 180^{o} out of phase. The number of available symbols is thus limited to two.

2.11 Media Access Control (MAC)

MAC is used to enable a group of devices to operate in a finite frequency range during a finite amount of time. There are many factors involved in developing a high performance MAC. These factors include sharing the medium fairly, maintaining high throughput, transferring data reliably, etc. Many different MAC protocols have been developed to attempt to optimize these different parameters.

2.12 Time Division Multiple Access (TDMA)

In a TDMA MAC protocol devices are assigned a time slot where they can have full access to the transmission medium. This means that all connected devices can transmit at the maximum data rate using the full bandwidth in the specified time slot. The set of time slots repeats after all the connected devices have had an opportunity to transmit data. The TDMA MAC protocol has a significant amount of overhead because only one device can transmit at a time. As a result, if a device does not have any data to transmit in its time slot the channel goes unused.

2.13 Direct Sequence Spread Spectrum (DSSS)

DSSS is a modulation technique designed to transmit data that is spread over a wide bandwidth. In DSSS a signal's modulated bandwidth is several times wider than the messages bandwidth. This signal bandwidth spreading is achieved by multiplying the message signal by a pseudorandom sequence, which is a wide bandwidth signal. This spreads the message signal over a very wide bandwidth - refer to Figure 2.1 for further detail. When the DSSS data reaches the receiver the receiver must multiply the signal by the same pseudorandom sequence used to spread the data. This shows that DSSS has a positive side effect in that it has a built in security mechanism, since the data can only be received by a device that knows the pseudorandom sequence. The use of the pseudorandom sequence and correlation with a codeword give DSSS the property that it rejects narrowband interference.

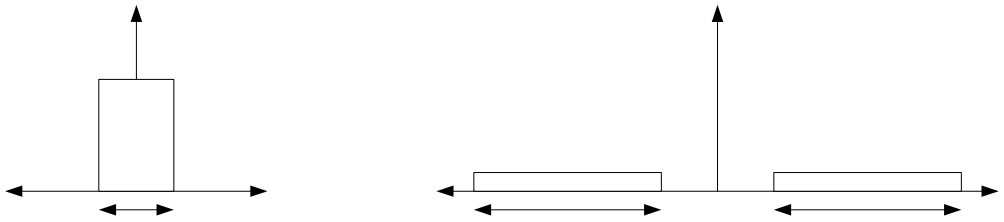

Figure 2.1 DSSS Modulation Diagram

2.14 Frequency Hop Spread Spectrum (FHSS)

FHSS is a modulation technique designed to transmit reliable and secure data utilizing a specified bandwidth. In FHSS the available bandwidth is broken up into a set of smaller bandwidths or channels. Each device hops from channel to channel at a specified frequency, see Figure 2.2 for details. A channel hopping pattern is defined by a pseudorandom sequence

that each device in a connection must be synchronized to for reliable data transmission. Narrowband interferes have a minimal affect on the modulated signal because each signal transmits at a specific frequency for only a short period of time.

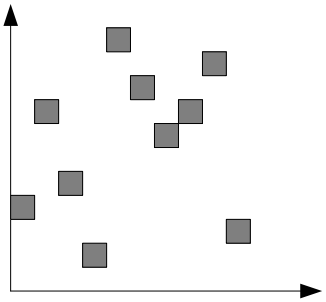

Figure 2.2 FHSS Modulation Diagram

2.15 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

There are many different types of CSMA/CA MAC protocols that have been developed but for this thesis, only the general idea behind a CSMA/CA MAC will be discussed. A CSMA/CA MAC has three common problems to deal with: the hidden node problem, the exposed node problem, and the capture problem, as shown in Figure 2.3. There are two common techniques utilized by CSMA/CA MAC protocols to solve these problems. These two techniques are out-of-band signaling and controlled handshaking. In out-of-band signaling, the receiving device transmits a signal, often on a separate channel, to notify all devices that could interfere with the data being received that a transmission is occurring. This technique removes the hidden node problem and capture effect but it increases the number of exposed nodes. When using the controlled handshaking technique devices

transmit data to notify other devices in the network that they are within range of the transmitting device, receiving device, or both. The packets received by other devices include an estimation of transmission time. This technique comes with a large amount of overhead but reduces the effects of all three channel access issues. It is clear that when developing a CSMA/CA MAC protocol, there are many tradeoffs between overhead, reliability, and performance.

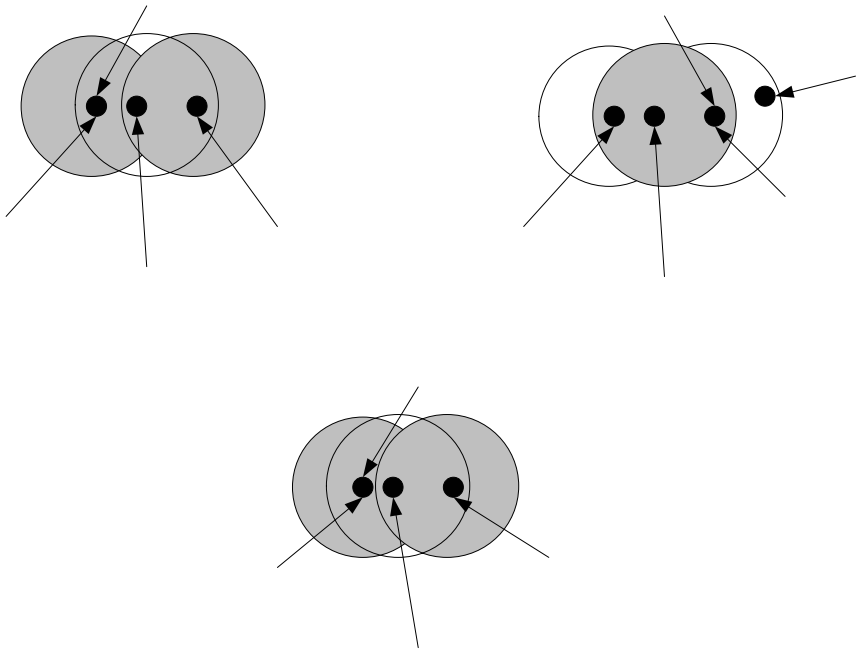

Figure 2.3 CSMA/CA Issues [6]

2.16 Complimentary Code Keying (CCK) [17]

CCK is a digital modulation technique derived from OFDM and DSSS. CCK expands the OFDM protocol using in-phase and quadrature techniques with complex symbols. The advantage of using CCK is that it allows for multi-channel operation. CCK uses eight complex chips that can choose one of four phases with a 64-bit pseudorandom spreading

sequence. This pseudorandom sequence is used in a similar fashion as DSSS. Before the modulation of the signal, one of 64 complex QPSK vectors is chosen for the symbol. It is clear that CCK is a complicated modulation technique that offers a high degree of inherent security. Also, it uses the bandwidth available for modulation efficiently, which allows for higher data rates than DSSS.

2.17 Convolutional Codes [18]

A convolutional code is a coding scheme in which a continuous sequence of information bits is mapped to a continuous sequence of output bits [17]. This output code is generated when the data stream is passed through a finite state shift register that contains N k-bit stages and m linear algebraic coding generators, see Figure 2.4. The data is input into the registers k bits at a time, where the bits are combined to generate an output data sequence n bits long. The code rate of a convolutional code is k/n. The inputs to the linear algebraic coding generators are defined by generator polynomials. Generator polynomials are a set of n vectors defining if a corresponding shift register phase is connected or not. Utilizing convolutional codes before modulating a signal increases performance by reducing the number of errors. The increase in performance comes with an increase in bandwidth because the length of an input binary stream is increased. This requires that the data rate of transmission is increased to achieve the same overall data rate as modulation without any coding.

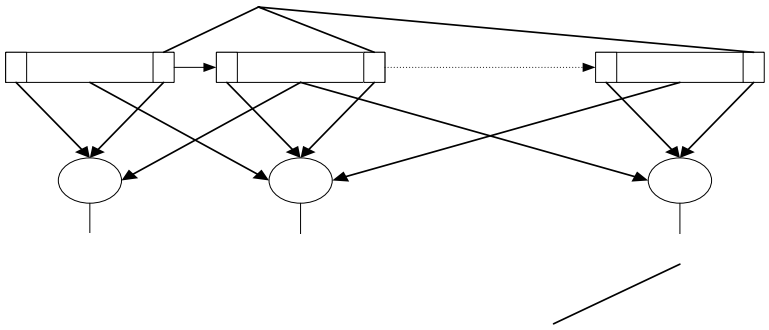

Figure 2.4 Generic Convolutional Coding Scheme

2.18 Packet Binary Convolutional Coding (PBCC) [17]

PBCC is a coding scheme that uses a 64-bit binary convolutional code with a coding rate of ½. A PBCC scheme also uses a 16-bit pattern, used to produce a 256-bit cover sequence. This cover sequence selects the QPSK symbol used for data transmission.

Chapter 3
Proposed Solution and Wireless Factors of Concern

Currently the DCS system operates using a wired network to monitor devices in locations throughout the country. It is desired to remove the need for connecting devices to the wired network because of the inefficiency of the current system. This inefficiency occurs, since the system requires access to customer's backbone networks and not all the devices to be monitored are capable of connecting to a wired network. The goal of the solution being developed is to remedy these issues. This is done through the development of a fully wireless solution. This thesis is concerned with the development of a WLAN for device monitoring solution. When integrated with the wireless wide area network for device monitoring, being developed in parallel, the final system will be fully wireless system with all devices connected with no need for interference with customer's network backbone, developed in Section 8.1 [21].

A protocol has been developed to create a reliable and efficient wireless connection between a host and a target device. Since there may be multiple devices in a specific area, a WLAN must be created so the host has access to data from many devices whenever desired. The WLAN is created by using an existing wireless protocol that has already been developed to make the design and implementation of the solution efficient and timely. A decision was be made between 802.11, 802.11a, 802.11b, 802.11g, Bluetooth, HomeRF, and Ultrawideband. The choice between these protocols was made based on their capabilities to handle the many criteria needed for the device monitoring system. The criteria for this system include network topology, capacity, range, data rates, scalability, power, cost,

reliability, security, and availability. An example of the network topology is shown in Figure 3.1.

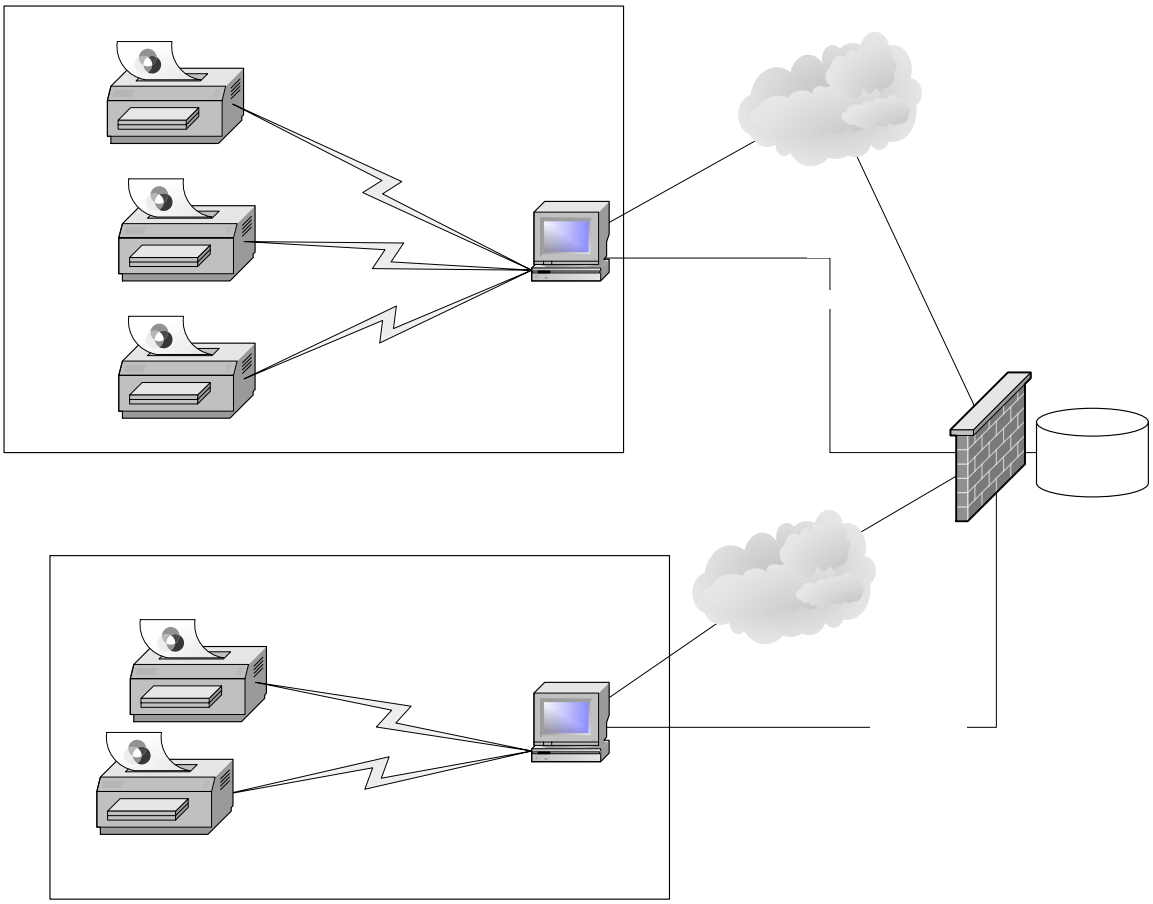

Figure 3.1 Proposed Device Monitoring Application

Figure 3.1 shows two LANs at a site where there are five devices to be managed. The device services application described in this thesis is only concerned with efficiently creating a set of local area networks that can connect all devices to a local area network host. A discussion of how the data is transmitted over a wired or wireless WAN to the company database will be discussed in Chapter 8. An element of the LAN to WAN connection that

will be considered is how well the WLAN data formats interface with the WANs formats. Looking at connecting a single LAN, this device monitoring application will have to be able to connect a group of devices to a single host device, in Figure 3.1 the host is a workstation. It is not required that the devices can communicate directly to one another. If this capability is available then the possibility of using an ad-hoc type of network could be used to connect more devices on a single WLAN. This leads to the consideration of the capacity of the device services application.

A major concern of the WLAN system is the number of WLANs deployed at a location. It is desired that the number of WLANs at a location is minimize to reduce complexity in the connection of the WLAN to the WAN system. This will reduce the cost of the system because the WAN system has the potential for a high cost. Minimizing the number of WLANs is directly related to the capacity and transmission range of the protocol. The data being transferred on the network is expected to be low so the capacity will not have a strong affect in the initial device monitoring application. On the other hand, the range is of great concern since the devices at a location are expected to be separated by large distances. This means that the larger the range of the chosen protocol, the more devices it will be able to handle with a single WLAN host. Also, the capacity of the system is influenced by the data rates of the protocol. The data rates are not a foremost concern initially given that expected data on the network are low and speed is of minimal concern.

Scalability is a concern for the future use of the device services application. The previous three factors, capacity, range, and data rates, are major factors to be considered for the scalability of the system. For future expansions, the device services application must be

capable of transmitting more data if it is desired. It also must be seamless to add a device in the range of a host that can connect to a current host device without being required to add a new host to handle the new device. These possible expansions to the system must be accommodated by the WLAN protocol that is chosen for the implementation of the system.

As mentioned previously, an important factor is the cost of using a protocol. The operating expense that will influence the cost of the WLAN is the power required. The cost of the power to operate these devices is going to be to be very low and not a major concern. Thus, the first effort for reducing the cost is to reduce the number of WLANs required to connect a group of devices, as mentioned previously, due to the fact that the WAN solution has the potential to be expensive. When considering the WLAN's cost alone, the only true cost is the implementation cost. This cost includes the cost of each host and each device on the network.

The users of the device services application require reliable data delivers so the wireless protocol chosen must be reliable. This includes noise immunity and immunity to interferers. The wireless community is getting larger so there are more devices that want to use the license-free bands. Therefore, there are many interfering devices that the chosen protocol must not be affected by.

A similar concern is security of the wireless transmissions. The data is going to be transmitted on a license free band, as explained in Chapter 4, which any external device can attempt to monitor. The data must be transmitted in such a way that an eavesdropping device cannot interpret the data being transmitted. Therefore, the protocol chosen must have security capabilities available.

Finally the availability in industry of devices or chipsets developed to implement the desired protocol must be considered. Since the device services application is being developed using an existing protocol, there is no need to develop a new chipset to operate a device using the chosen protocol. Using existing chipsets will be more cost and time efficient. This will require comparing what hardware has been developed to operate the devices and the capabilities of these developed devices.

Chapter 4
Review of Candidate Protocols

4.1 Bluetooth

The development of the Bluetooth wireless protocol began in 1998 when a group of companies joined to form a special interest group intended to develop a wireless interface to connect device developed by many manufactures. The decision was made to use the 2.4 GHz Industrial-Scientific-Medical band because it is a worldwide license-free band that any system can use. Using this band allows the Bluetooth protocol the potential to become a standard around the world for interfacing devices together wirelessly.

The 2.4 GHz band is a commonly used band because it is license-free; therefore, a communications protocol had to be developed that would allow the devices using Bluetooth to transfer data reliably over their wireless network. To guarantee a high level of reliability over the wireless medium, the communications technique FHSS was chosen for use. FHSS increases reliability by breaking up the wide band spectrum used for transmissions into many narrowband channels. During a connection, the devices switch from channel to channel in a pseudorandom fashion. Since the device is transmitting over many different narrowband channels the effects of narrowband interfere is reduced. If there is interference at a certain frequency, packets will only be dropped when the transmission occurs at this frequency. Every other packet transmitted will be received. FHSS requires accurate timing when switching between channels and it requires that the pseudorandom sequence is known by all devices connected on a channel. A major advantage of FHSS for the Bluetooth protocol is that it is lower power and lower cost than other communications techniques. In addition to

interference from non-Bluetooth transmissions, Bluetooth must also avoid interference from other nodes connected using Bluetooth.

The wireless channel access is maintained by creating an ad hoc connection, called a piconet. A piconet consists of two or more devices creating a wireless connection. When a connection is created, one device is chosen to be the master. Once the master has been selected, the slaves synchronize their native clocks to the master unit is clock based on the master's identification and native clock, which is sent to the slaves. Devices can join the piconet until there are a maximum of seven slaves connected to the piconet. Once the connection has been created, the piconet can begin transmitting data between devices. Access to the channel on the piconet is controlled by the master using a polling technique. When the master is prepared to receive data from a slave device, it sends a poll to the device. The device can now transmit packets of varying sizes to the master. The slave can transmit packets that are single-slot, 3-slot, and 5-slot packets. Once the slave has transmitted data in its slot, it must wait until it is polled again to transmit data. In addition to controlling access to the channel, the master also controls routing of packets. The master receives packets from the slaves and has an opportunity to transmit packets to slaves when it polls a device. When polling a slave, the master can transmit packets to the slave in a similar fashion as the slave's transmission to the master. When a packet is sent between two devices, an automatic repeat request (ARQ) technique is used to verify that the packet has been received. This describes how the Bluetooth protocol can be useful in a home or small office setting. Often a network must expand beyond eight devices, which can be accomplished through a network topology called a scatternet.

Many piconets can be connected together to form a scatternet. A scatternet allows a Bluetooth network to expand beyond the limits of eight devices per piconet. A scatternet also allows a Bluetooth network to more efficiently use the data rates that are available to the entire network. In a single piconet there is a channel capacity of 1 Mbps. The total capacity available to a Bluetooth network is 79 MHz. A scatternet is able to use more of the available capacity by using different pseudorandom sequences in different piconets. A scatternet is created by a device being declared to be the bridge between two piconets. A bridge device operates as the link between two piconets, passing data between piconets and transmitting its own data when needed. A bridge device shares its time between two piconets by using time division duplexing. A bridge device can be a slave in multiple piconets or a master in one piconet and a slave in another. Figure 4.1 shows for an example of a scatternet consisting of two piconets. A scatternet can also be useful to increase the coverage of a Bluetooth network. It only requires that a node from one piconet is within the range of a node in another piconet to create a scatternet.

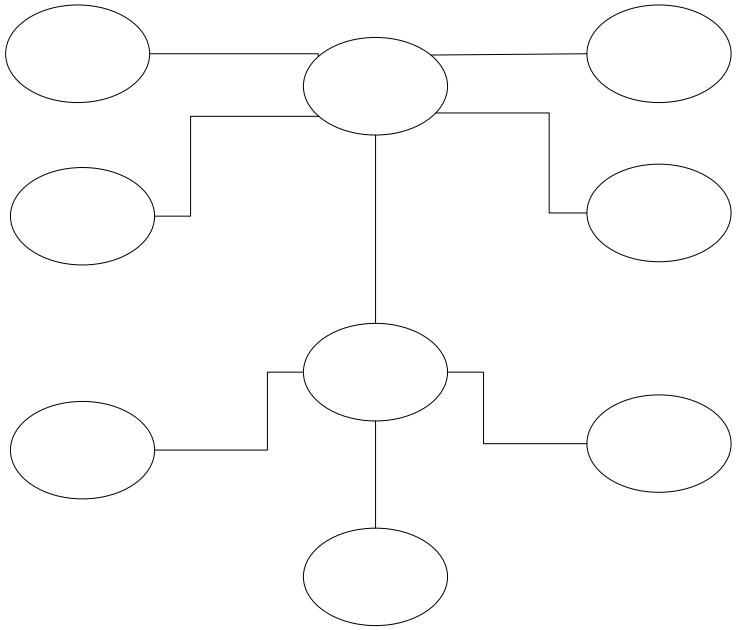

Figure 4.1 Example Bluetooth Network

Bluetooth has a range of less than 10 meters. The range is increased when a scatternet is used because each unit only has to be within 10 meters of one other unit. The range can also be increased if the data is transmitted in a high power mode which offers transmissions up to 100 meters. Bluetooth also offers a cipher algorithm for security. This is most useful in the high power mode because when data is being transmitted further there is a greater possibility of an unwanted device receiving the network's data. FHSS increases the security because devices that are not connected to the network do not know the pseudorandom hopping sequence. Bluetooth is a well designed protocol that has many positive qualities to offer including: low cost, low power, security, polling style channel access, and security.

4.2 HomeRF

In early 1997, several companies formed the Home RF working group to begin the development of a standard designed specifically for wireless voice and data networking in the home. The development of this working group was motivated by the widespread use of the internet and the development of affordable PCs that can be used in most homes. This protocol allows PCs in the home to have greater mobility, providing a connection to the Internet, printers, and other devices anywhere in the home. With all this potential, many members of industry worked to develop the Shared Wireless Access Protocol-Cordless Access (SWAP-CA) specification.

The SWAP-CA specification was designed to operate in the 2.4 GHz Industrial-Scientific-Medical band. Similar to Bluetooth, the use of this band opens the Home RF protocol to potentially operate worldwide. Also similar to Bluetooth, Home RF utilizes the communications technique FHSS to minimize the effects of interferes in this part of the spectrum. The SWAP-CA protocol is explained in more detail in Section 4.2.1.

A network topology of the Home RF protocol consists of four types of nodes: Control Point, Voice Terminals, Data Nodes, and Voice and Data Nodes. The control point is the gateway to the public switched telephone network (PSTN) and the Internet. It is also responsible for power management of the network. A voice terminal communicates with the control point via voice only. A data node communicates with the control point and other data nodes. Finally, a voice and data node is a combination of the previous two nodes [10].

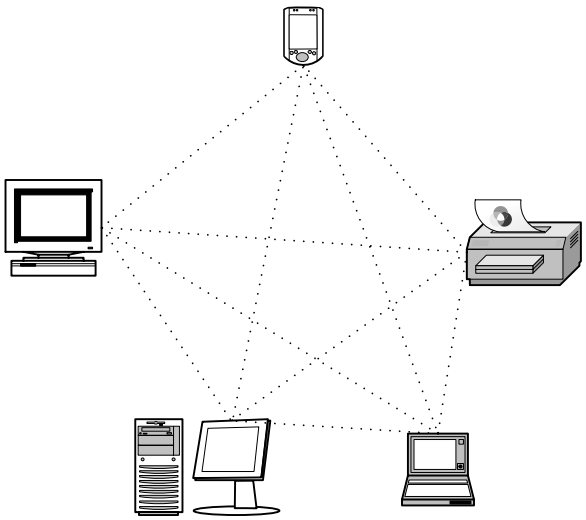

Figure 4.2 HomeRF Network

Once the devices in the network have been assigned their node types, they can be connected using two different network topologies: Managed Network and Peer-To-Peer Ad-Hoc Network. In the managed network topology the control point is in complete control of the network. This means that the control point is the gateway between devices in the network, a device to the PSTN, and a device to the Internet. This network topology can support real-time audio traffic and data traffic. In the peer-to-peer ad-hoc network topology, all devices have to control access to the network and routing independently, see Figure 4.2. This network topology only supports data transfer [11].

Using the above network topologies, there is not a specific maximum number of nodes that can be connected to a single network. The number of connected nodes is limited only by the capacity of the network. The network developer has to balance the number of nodes and the achievable per-node capacity. The maximum data rates of the network are .8 and 1.6 Mbps for a node. The size of the network is also limited by the transmit range of the

devices, which is a maximum of 50 meters. This means that any device must be within 50 meters of another device in the network to maintain a connection. Other specifications of a Home RF network are that share-key encryption is used to define the hop pattern and maintain security. Also, a 24-bit network identifier is used to prevent two Home RF networks from communicating. Home RF was developed as a low-cost protocol so that it could be used in many homes around the world. Home RF also includes many other positive qualities including: low-power, good range, security, two types of network topologies, and the capability of connecting many nodes.

4.2.1 SWAP-CA [10]

To manage the Home RF protocol, a media access control (MAC) specification had to be developed to handle both voice and data communications. This specification was developed in the form of the SWAP-CA specification. This specification is defined to manage data communications using a CSMA/CA service, derived from the IEEE 802.11 protocol, and to manage voice communications utilizing a TDMA service. Since both CSMA/CA and TDMA are used, a channel scheduling protocol must be developed to allow this data to transmit.

During a single hop period, a superframe, which includes two contention-free periods and a contention period, is used for data transmissions. In the contention-free periods, TDMA is used for voice traffic and during the contention period, CSMA/CA is used for data transmissions. The period of a superframe is equivalent to the hop period of 20 ms. The above channel scheduling protocol is used only for a managed network when voice transmission can occur. In a peer-to-peer ad-hoc network, the entire superframe only

involves the contention period. With a channel scheduling protocol in place, the channel access protocol of the MAC must be defined for the contention-free and contention periods.

In the contention-free period, the control point of the network has complete control of when each node has access to the channel. The two contention-free periods are divided into pairs of TDMA slots equal to the number of nodes connected to the network. The first TDMA slot is the downlink slot, in which the control point can communicate with the node, and the second slot is the uplink slot, in which the node can communicate to the control point. The digital messages transmitted during these periods use the 2-FSK digital modulation technique.

The contention period of the MAC is broken up into a set of contention windows, where a node attempts to access the channel. Before a node attempts to access the channel in one of the contention windows, the node randomly selects a backoff value. This backoff value is decremented by one for each contention window where the channel is free. Once the backoff value has become zero, the node can attempt to access the channel. If there is a collision, the steps must be repeated to attempt another transmission

4.3 802.11 [17]

The first WLAN standard was adopted in 1997 by the IEEE. This standard was the 802.11 standard. The 802.11 standard was developed to operate using the same interfaces as wired LANs. To accomplish this, the IEEE 802.11 standard adopted the IEEE 802.2 logical link control (LLC) sub-layer. Using an interface that is exactly the same as a wired LAN's interface, any protocol operating above the LLC sub-layer does not need to be aware that a WLAN is being used for the network connection. Therefore, 802.11 operates using the

Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocols. Utilizing this widely used protocol has allowed the 802.11 standard to be integrated into the networking community effortlessly. Enhancing the ease of use of the 802.11 protocol is that it was designed to operate in the 2.4 GHz Industrial-Scientific-Medical band. The 802.11 protocol defines a medium access control (MAC) layer, a MAC management and services layer, and three physical layers.

The 802.11 MAC protocol utilizes a frame exchange protocol to increase reliability on the noisy and crowded 2.4 GHz band. This frame exchange protocol minimally consists of two frames which are the request to send (RTS) and the clear to send (CTS) packets. These two packet types are used with a CSMA/CA access mechanism. When there is a collision of the RTS packet, the 802.11 MAC starts a backoff timer before attempting to send another RTS. There are also a maximum number of times that the 802.11 MAC can attempt to send the RTS signal. The 802.11 protocol offers two different channel access mechanisms: distributed coordination function (DCF) and centrally controlled access mechanism (CCAM).

When the 802.11 MAC is operating in the DCF mode, after the RTS and CTS have been transmitted, the MAC waits for a specified period of time, monitoring the channel. If the channel remains inactive for this period of time, the device begins transmitting data. When the target device has received the data, it responds with an acknowledgement notifying the transmitting device that the data was received. If the transmitting device does not receive the acknowledgement, it enters in to a backoff period and retransmits the data. Again there is

a maximum retry count for the number of attempts to transmit data. This type of access mechanism is commonly known as an ad-hoc network.

When the MAC operates in the CCAM mode, the channel access is controlled through a polling technique, similar to Bluetooth. In this mode there is a central device, called the access point (AP). The AP periodically polls the connected devices on the network for data. The AP also operates as a router to route data to and from devices on the network. This network mode utilizes a contention free period, where the AP has complete control of the channel access and a contention period, where the devices can attempt to access the channel in the same manor as the DCF mode. After the contention period, the AP regains control of the channel through a beacon signal and begins the contention free period.

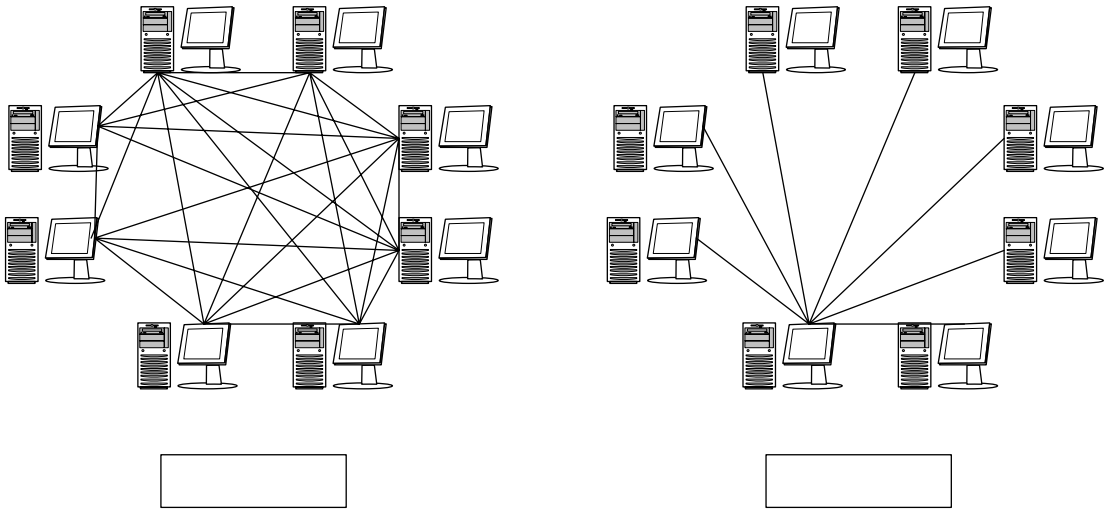

Figure 4.3 802.11 Network Topologies

The previously explained 802.11 MAC protocol deals with channel access of other 802.11 devices, but since the 802.11 protocol operates in the 2.4 GHz ISM band there are many other devices trying to access the channel. Therefore, the 802.11 standard must define a MAC management protocol. First an 802.11 device must have a mechanism to decide

whether the signal being received is coming from another 802.11 device. This is done through device authentication. There are two types of authentication: open system authentication, which does not use anything more then an authentication that the communication device is an 802.11 device, and shared-key encryption, which requires that the communicating devices both know the encryption algorithm. If the devices can communicate, a device sends an association request to the AP and the AP grants the connection to the WLAN. Once there is a connection to the specific WLAN, the devices must synchronize themselves to increase the reliability of the channel access. In the CCAM mode the AP sends out a beacon periodically to synchronize the WLAN devices. In the DCF mode the initial node sends out a beacon command and as each node connects, if it has never received a beacon, the device attempts to send its own beacon. The final function of the MAC management protocol is to control the power modes. A device is capable of entering into a power saving state where the receiver and transmitter are turned off. The only way that a device is put back into a regular power mode is if a beacon is sent in DCF mode or the AP commands the device to in CCAM mode.

Finally, the lowest layer of the protocol stack must be designed. The 802.11 standard operates three different physical layers: DSSS, FHSS and infrared (IR). The DSSS layer uses DBSK and DQPSK modulation techniques, which are specified in the packet header. The data is scrambled with a 7-bit polynomial to transmit secure data. This data can be descrambled by the receiving device after the 7-bit polynomial has been exchanged by the devices. The FHSS layer utilizes a Gaussian FSK (GFSK) modulation technique to transmit data. A 127-bit sequence is used to randomize the data for secure data transmissions. This

127-bit sequence and the hopping sequence must be known by the transmitting and receiving devices for accurate transmission. The IR physical layer is used for indoor transmissions since the IR spectrum cannot transmit through solid walls. The IR layer employs a PPM modulation technique but does not use any security features because of the limited transmission range. Each of the physical layers exploits a code redundancy check (CRC) sequence to increase reliability of transmitted data.

These previously explain physical layers offer data rates of 1 or 2 Mbps depending on the modulation technique being used. The FHSS and DSSS physical layers can transmit data up to 50 meters. The 802.11 protocol offers many positive qualities including: low-power, good range, good data rates, security, two types of network topologies, TCP/IP compatibility, and there is no absolute maximum number of nodes that can be connected to the network. Since the development of the 802.11 WLAN standards, there have been three different advances in the use of the physical layers. The advances include 802.11a, 802.11b, and 802.11g. These extensions of the original 802.11 standard operate using the same MAC protocols and the same interface layer. Therefore, the advantages of an interface equivalent to a LAN and the highly capable MAC are maintained. The three advancements of the 802.11 protocol are explained in the following subsections.

4.3.1 802.11a

Shortly after the development of the 802.11 standard, the IEEE 802 Executive Committee approved the development of two 802.11 protocols to offer higher data rates. The first of these standards, although it was the second to become a standard, was the 802.11a protocol. As mentioned previously this standard was developed to offer higher data rates in the

physical layer while keeping all other layers of the 802.11 protocol unchanged. The first major difference between 802.11 and 802.11a is that the 802.11a IEEE standard operates in the 5 GHz license-free band. The advantage of using this frequency band is that fewer devices operate using this frequency band. Therefore, there is going to be much less interference. A disadvantage of operating at a higher frequency is that the signal does not travel through walls and other obstructions as well. This limits the 802.11a standard to being efficient at connecting devices in a single room or outdoors.

The 802.11a standard achieves high data rates by using an OFDM physical layer. The OFDM physical layer separates the frequency band being used into 52 separate sub-carriers. The sub-carriers are modulated using BPSK or QPSK. Again, a 127-bit generator sequence is used to randomize the data transmitted. This physical layer handles data rates in the range of 6 – 54 Mbps, while using DSSS and FHSS for the 1 and 2 Mbps data rate as in the 802.11 standard. The 802.11a protocol can also achieve a range of 100 meters.

4.3.2 802.11b

The second standard, which was released first, is the 802.11b standard. The 802.11b standard has more similarities to the 802.11 standard by maintaining the same MAC and interface along with using the same frequency band, 2.4 GHz ISM band. Therefore, the same concerns of handling a busy frequency band come into play, but the indoor capabilities of the 802.11 standard are also maintained.

For the 802.11b standard, higher data rates were obtained by using a high rate DSSS (HR/DSSS) technique. This technique is similar to the DSSS used by 802.11, but the data rates have been increased to also transmit data at 5.5 and 11 Mbps. The higher data rates are

achieved by operating with an enhanced modulation technique. The higher data rates use CCK modulation and PBCC. As in the 802.11 standard, a 7-bit data scrambling polynomial is used. The 802.11b standard maintains backward compatibility with the 802.11 protocol by operating with the same physical layer as the 802.11 standard. The 802.11b standard also offers a shorter header to reduce the amount of overhead that occurs during a transmission. As in 802.11a, 802.11b offers a transmission range of 100 meters.

4.3.3 802.11g

In 2001, new modulation techniques were allowed by the FCC. Making these modulation techniques available allowed the IEEE to extend the 802.11b standard. The 802.11g standard was release in 2002 by the IEEE, defining new data rates up to 54 Mbps. Again, there was no change to the MAC and interface layers of the 802.11 standard with the frequency band remaining in the 2.4 GHz ISM band.

The 802.11g standard operates at data rates up to 54 Mbps using the same DSSS and FHSS techniques as in the 802.11 and 802.11b standards. This maintains backwards compatibility with these two standards. To achieve higher data rates, an OFDM technique is used as in the 802.11a standard. The OFDM technique is exactly the same as the 802.11a OFDM technique except that it operates in the 2.4 GHz band instead of the 5 GHz band. As in the other 802.11 extensions, 802.11g offers a transmission range of 100 meters.

4.4 Ultrawideband [12]

During the development of wireless communications protocols there has been a desire to develop a protocol that could handle all communication types in the home, office, and public hot spots. This would include audio, video, and data communications. The previously

discussed protocols have the potential to handle audio to some extent, but none of the protocols have high enough data rates to handle video data efficiently. Enter in ultrawideband. This protocol was recently permitted to be used by the FCC in 2002. This protocol has been developed with the intention of connecting every device in a home or office wirelessly. It is proposed to handle data rates up to 500 Mbps, which is high enough to handle high quality video. In 2003, a task group was developed to select the best protocol to become the ultrawideband standard. Currently the decision of the most appropriate protocol has not been chosen. There are two potential approaches that could be used to transfer data at these high data rates. The proposals which utilize the following approaches have been submitted to the IEEE attempting.

The first approach is to transmit narrow baseband pulses that occupy a very large spectrum. Using this approach, simple and inexpensive hardware can be developed to operate the protocol. This is because the hardware would not be required to demodulate a signal. The hardware could receive a digital signal and begin processing. The second approach is to divide a large spectrum into several smaller bandwidths, referred to as "multibanding." To cover a narrower spectrum a broader pulse would be transmitted to cover the allotted spectrum. This type of protocol would require more complicated hardware to modulate and demodulate the pulses but has more immunity to noise. A common pulse modulation technique being considered is binary phase-shift keying. An example of an ultrawideband proposal was developed by Texas Instruments called the "Multi-band OFDM Physical Layer Proposal [2]."

This proposal was presented in 2003 as a potential building block for the development of the IEEE ultrawideband standard. This proposal attempts to utilize OFDM to break up the available bandwidth into several smaller bandwidths. The proposed bandwidth is 528 MHz. OFDM is a modulation technique that has been used in many other wireless protocols including 802.11. Therefore, it is a modulation technique that wireless developers have been using for many years and should be easy to handle. OFDM is a protocol that is inherently robust to multi-path systems, which gives the protocol the capability of handling multi-path systems. The proposal offers data rates from 55 Mbps to 480 Mbps. One of the most attractive elements of the protocol is that it is proposed to have potential to work with an 802.11 MAC. This is attractive, of course, because the 802.11 MAC is a proven protocol that is efficient and can be used well in practice. Since this protocol separates the bandwidth into several smaller bandwidths, the hardware is going to be a bit more difficult than using one large bandwidth, but it is still expected to be capable of being produced cheaply. As explained above, this solution has better immunity to noise and interference and should be more efficient. Due to the low transmit power requirement of the FCC this protocol will consume low power during transmission and reception of signals. The proposed time to market is 2005.

A very large spectrum must come with some limitations on transmit power to avoid interfering with other wireless devices. "An ultrawideband signal is one whose -10 dB bandwidth exceeds 20% of its center frequency or 500 MHz, whichever is smaller.[11]" Also there are limitations on the maximum transmit power over all frequencies in the spectrum. This can be observed in Figure 4.4.

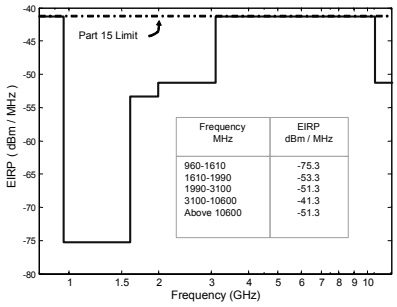

Figure 4.4 FCC Allowed Transmission Power Over the Frequency Spectrum [12]

The capabilities of ultrawideband are not endless. Ultrawideband can achieve data rates in the range of 100 – 500 Mbps, but these data rates can only be achieved with transmission ranges of 2 -10 meters. This is because of the strict limitations on the transmission power. It is shown in Figure 4.5 that ultrawideband can achieve a capacity many times higher than other wireless protocols when the transmission range is less than 12 meters. Once the transmission range is above 12 meters, other wireless protocols begin to have higher capacities.

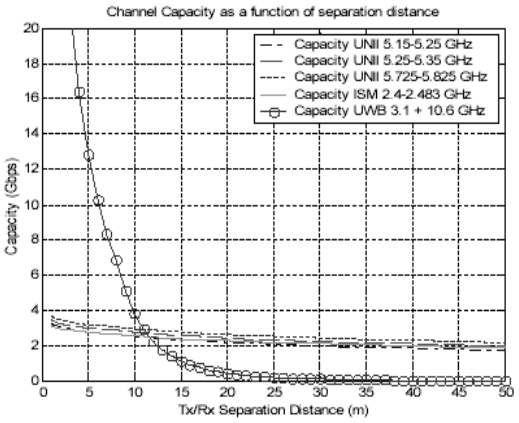

Figure 4.5 Capacity vs. Transmit Range for Different Wireless Protocols [12]

Chapter 5
Comparison and Decision

Table 5.1 and Table 5.2 list the relevant features of the Bluetooth, HomeRF, 802.11, 802.11a, 802.11b, and 802.11g protocols. Data from this table was used to make the final decision about which protocol best suits the needs of the device services application.

As mentioned in Chapter 3, there are many factors that must be taken into account when making a decision about the best protocol to use. Each factor is going to be considered in the subsequent sections, where the advantages and disadvantages of each protocol will be compared. Once the advantages and disadvantages have been compared, the factors must be weighed to make the final decision. The factors will be weighed in the discussions in Section 5.2.

5.1 Comparisons

5.1.1 Network Topology

Each of the protocols discussed previously has a slightly different type of network topology available. Bluetooth is a protocol that strictly uses a polling technique where the master polls up to seven slave devices. Bluetooth also allows a larger number of nodes to be connected together through the use of a scatternet. All 802.11 protocols and HomeRF use a similar type of network topology. They offer the most flexibility out of the protocols, where the network can be configured to use either a network where the host or master has complete control of the network or an ad-hoc type of network. The ultrawideband protocol has not been finalized, so there is no defined network topology.

Looking at network topology, the 802.11 and HomeRF protocols are the most attractive because they offer the most flexibility to be connected in almost any type of topology. These protocols also do not have a limitation on the number of devices that can be connected. A Bluetooth network is limited to just eight nodes, one master and seven slaves, when there is a single master, but because of the scatternet capability Bluetooth is capable of connecting many devices. This type of topology is not as efficient as the 802.11 and HomeRF topologies, but it is capable of meeting the requirements of the device services application.

The interface protocol used by the protocols must also be considered because connecting to a WAN is a desired feature. The 802.11 devices utilize TCP/IP, which is exactly the same as the routing protocol used by a WAN. The HomeRF protocol utilizes SWAP/CA, which is easily compatible with TCP/IP. Also, Bluetooth does not use TCP/IP but as there are devices developed to act as a WLAN cable, Bluetooth is capable of interfacing with TCP/IP. Clearly, the 802.11 protocol offers the easiest interface between the WLAN and the WAN.

5.1.2 Capacity

The capacity determines the maximum amount of data that a WLAN can have transmitted over the channel, which will limit the amount of data that can be transmitted on the network. Bluetooth has the lowest capacity and it has bottlenecks that are created at bridge nodes to further reduce the capacity. The 802.11 and HomeRF protocols have approximately the same capacity since their data rates are similar. 802.11a, 802.11b and 802.11g improve upon the capacity of the 802.11 protocol. The capacity of each of these protocols is expected to be more than sufficient for the network being developed.

Ultrawideband can handle the largest amount of data and is limited by a specified number of devices that can be connected on the network. The device monitoring application does not require much data to be transmitted on the network so all these protocols can handle the expected amount of data on the network.

5.1.3 Range

This is the first factor where the disadvantages of some of the protocols can really be observed. Bluetooth has the capability of transmitting up to 100 meters in a high power mode, but during regular operation it transmits up to 10 meters. HomeRF can transmit data up to 50 meters. 802.11 can transmit data up to 50 meters while its extension protocols can transmit up to 100 meters. However, when transmissions are indoors, 802.11a has a disadvantage by operating in the 5 GHz band, where wireless signals will have more difficulty traveling through walls. This greatly limits the range of 802.11a devices indoors to a single room of a size up to 100 meters. Ultrawideband can transmit data from 2-10 meters with a significant reduction in data rate at higher ranges. Clearly, the best transmission ranges are with Bluetooth in high power mode and the 802.11 protocol extensions.

5.1.4 Data Rates

In terms of data rates, it is clear that the ultrawideband protocol offers the highest data rates, up to 500 Mbps. These data rates are well beyond the data rates desired for the device services application because the ultrawideband protocol was developed to have the capability of transmitting all types of data traffic, including video and voice. The device services application is only going to transmit data and currently it is going to be a limited amount of data. 802.11a and 802.11g offer data rates up to 54 Mbps, which is

also well above the needs of the device monitoring application. 802.11b has data rates up to 11 Mbps while 802.11 has data rates up to 2 Mbps. Finally, HomeRF has data rates up to 1.8 Mbps and Bluetooth has data rates of approximately .721 Mbps. Bluetooth has the lowest data rates but they should still be high enough to handle all the data transmitted for the device services application.

5.1.5 Scalability

Scalability is a factor that looks at the future capabilities of the protocol in terms of capacity, range, and data rates. All the protocols have high enough data rates to be capable of handling a greater deal of data than the initial design of the device services application. Ultrawideband is the most limited in terms of its scalability for the device services application. It has a sufficient data rate to expand to handle a very large amount of data, but the short transmission range of the devices will not be sufficient to add devices to a WLAN in the device services application. The devices are most likely going to be far apart, so ultrawideband is not going to have the ability to scale well to a number of devices. HomeRF is slightly limited by its data rates and range, but it will be able to scale well in the device monitoring application. However, it will hit the limits of scaling faster than the 802.11 expansion protocols. The original 802.11 will have a similar limitation on scaling. Bluetooth is also a protocol that is limited for scaling. It has the capabilities of a higher transmit range than HomeRF and 802.11, but it is limited by its network topology and data rates. Bluetooth has the lowest data rates and a network topology that is difficult to manage. The use of scatternets creates bottlenecks on the network. This is because all data has to transmit from scatternet to scatternet through a bridge device. Once there are too many devices attempting to communicate to the host

device, the data will not be transmitted efficiently enough to the host because of these bridge nodes. The protocols that are going to work best for scaling are 802.11a, 802.11b, and 802.11g, with 802.11a and 802.11g scaling equally well and better than 802.11b because of the higher data rates that 802.11a and 802.11g provide. Another note is that the 802.11g protocol is backward compatible with 802.11b. Therefore, when the maximum amount of scaling that 802.11b can provide is nearly achieved, 802.11g devices can be integrated into the system for increased scalability.

5.1.6 Power

For the device services application, power is not of great concern. All the different protocols are developed to attempt to use as little power as possible. Therefore, in terms of the power required, there is not a significant difference between any of the protocols.

5.1.7 Cost

The cost of the 802.11, HomeRF, and ultrawideband protocols is not available do to no availability in industry. This will be explained later. The remaining protocols have similar costs that are relatively low. Off-the-shelf Bluetooth devices are approximately $30 per device. 802.11b has APs for approximately $50 with adapters for approximately $20 [24]. When comparing 802.11b and Bluetooth there is essentially no difference because when all the devices for an identical network are purchased, the costs almost even out. 802.11b would be slightly less because it only requires one access point for a network with all other devices connected with an adapter. The devices for the 802.11a and 802.11g protocols are slightly more expensive with 802.11g devices about twice as expensive as 802.11b devices and 802.11a devices three to four times more expensive. This cost analysis is, for off-the-shelf only off the shelf devices. The devices developed

for the device monitoring application will be developed using only purchased chipsets with custom circuit boards built around them to reduce cost further. The cost of chip sets are not available, except for a Bluetooth chip set was found to be available for around $4 [26]. The cost of off-the-shelf devices is a rough comparison that should be nearly accurate for this analysis.

5.1.8 Reliability

Since the ultrawideband protocol has not been developed, the factors that play into reliability are unknown. All of the other protocols have capabilities to attempt to transmit data as reliably as possible. None of the protocols is be completely immune to noise and interferes, but they all utilize error detection and correction techniques to avoid any dropped data. Bluetooth is capable of handling interferes because of the use of FHSS, as explained in Section 4.1. It also employs a polling-style MAC to avoid collisions between other devices on the same network. HomeRF also utilizes FHSS for interference immunity and uses a CSMA/CA style MAC to reduce collisions between connected devices on the network. The 802.11 protocols use FHSS and DSSS to avoid interferes on the frequency band and they use a CSMA/CA style MAC. 802.11a has an added advantage that it operates in the 5GHz band, which is less crowded so there are fewer interferes.

5.1.9 Security

All of the protocols discussed offer a security feature, except for ultrawideband which has not been defined. Each of the protocols has inherent security by using FHSS or DSSS, and they all also offer an encryption technique for greater security.

5.1.10 Availability

When a system is to be developed using existing devices, availability becomes a great concern. First, the ultrawideband protocol has yet be developed, with the expectation that the first devices will be available off-the-shelf in two or three years. This makes it very difficult to develop a system utilizing ultrawideband until devices have been developed. On the other hand, the HomeRF protocol was never received well by industry and currently there are not any devices developed utilizing HomeRF. The analysis of the Bluetooth protocols availability is more complicated. There are many off-the-shelf Bluetooth devices available but currently these devices do not implement all the features of the protocol. The off-the-shelf devices have been developed to connect devices that are typically developed to be used in a single office space. This would require connecting the workstation, printer, scanner, and other devices in an office. This style of connection only requires a piconet because there will not be any more than eight devices connected together and typically these devices would be within 10 meter range of each other. Therefore, the devices that are available off the shelf cannot handle scatternets and do not implement the high power mode defined by the standard. The 802.11 extension devices have been developed by many companies and are currently available off-the-shelf. The original 802.11 protocol currently does not have any devices available off-the-shelf because the newer protocols have been developed and taken its place. Most of the 802.11a, 802.11b, or 802.11g devices implement the infrastructure network topology and a subset of the devices implement ad-hoc networks. The 802.11b protocol is the most mature of the protocols and has the most devices available. 802.11a and 802.11g have around the same number of devices developed. There are also devices that implement a subset of the 802.11 protocols on the same device. This would offer the flexibility of

choosing a standard AP with the adapter device utilizing the specific protocol that suits the location where it is being used.

5.2 Discussion

Observing the advantages and disadvantages of each of the protocols, a few of the factors take the greatest weight in the decision. These factors are availability, network topology, range, and scalability. This is not saying that the other factors considered are not important but these factors demonstrate the greatest differences between the different protocols. For many of these factors, the protocols can all operate equally well. All the protocols have been developed for their own specific needs and they are capable of filling these needs well. When using previously developed products, industry has already made some of the decisions.

Availability quickly became an issue when looking for hardware available using the HomeRF protocol. The HomeRF protocol sounds good on paper because it is easily compatible with TCP/IP and has a network topology that is suitable for the device monitoring application. These two elements of the protocol are ideal for the device monitoring application, but during an Internet search there were no available devices utilizing HomeRF. When looking for available networking systems, there are numerous companies that have developed devices for Bluetooth, 802.11a, 802.11b, and 802.11g networks. Finally as mentioned previously ultrawideband is not expected to be available for two or three more years.

Bluetooth, 802.11a, 802.11b, and 802.11g protocols have off-the-shelf products available to be implemented in a wireless local area network. These products come in the form of PCI cards, PCMCIA cards, USB connected devices, and others. They also

typically consist of a computer that is connected to a host device, with the network nodes connecting to the backbone network through this host. The fundamental difference between the network implementations of the two protocols is that the 802.11 extension protocols are used to connect many devices, usually other computers, within a home or office to the network backbone. On the other hand, Bluetooth is used to connect devices, such as printers, mice, keyboards, scanners, and others, within a room to a host computer. Bluetooth is capable of operating similar to 802.11, but the products that have been developed have not been meant for this use. Both of these networks are designed to use nearly the same elements to connect to the network. This fundamental difference does not clearly differentiate the 802.11 extension protocols or Bluetooth as the better solution for the device services application.

When looking more closely at the protocols, there are two elements that begin to separate the two protocols, namely, transmit range and the scalability. Observing the protocol definitions, the differences are minimal. In the Bluetooth protocol definitions there is an option to increase the transmit power, which will allow for a 100 meter transmit range. Also, Bluetooth is able to handle a larger number of nodes by creating a scatternet. Similarly the 802.11 extension protocols are specified to have approximately a 100 meter transmit range with an unspecified maximum number of nodes. The 802.11 protocols have a slightly easier network topology to manage.

As explained is Section 5.1.10 the Bluetooth devices available do not implement high power mode and scatternets. With these limited specifications, Bluetooth is not going to have a long enough range to connect many devices together. Since the expectations are that devices are going to be separated by large distances, the available

Bluetooth devices are not going to be able to be connected efficiently. Therefore, one of the 802.11 extension protocols must be chosen for the final implementation.

The device services application is expected to be implemented inside of a building, so 802.11a is not going to be capable of fulfilling the requirements well. The choice has now been reduced to 802.11b or 802.11g. In terms of scalability, 802.11g has the most potential and is the new evolving technology in industry. 802.11b is cheaper and more readily available on the current market. Currently, the device services applications is not anticipated to transmit a large amount of data, so 802.11b has a high enough data rate for the initial implementation with the capability of scaling well. Therefore, to reduce risk and cost, since 802.11g is a new technology, 802.11b is the protocol selected to start the development of the system. The major advantage of this choice is that 802.11g is backward compatible with 802.11b. Thus, if in the future the amount of data being transmitted on the network exceeds the capabilities of 802.11b, 802.11g devices can be developed and integrated seamlessly into the WLAN.

Characteristic	802.11	802.11a	802.11b	802.11g
Operational Spectrum	2.4 - 2.4835 GHz	5.15 - 5.35 GHz, 5.725 - 5.825 GHz	2.4 - 2.4835 GHz	2.4 - 2.4835 GHz
Bandwidth	83.5 Mhz	300 Mhz	83.5 Mhz	83.5 Mhz
Modulation Type	1, 2 Mbps DSSS, 1, 2 Mbps FHSS	6, 9 Mbps BPSK, 12, 18 Mbps QPSK, 24, 26 Mbps 16-QAM, 48, 54 Mbps 64-QAM	1 Mbps DBPSK, 2 Mbps DBPSK, 5.5, 11 Mbps DQPSK/CCK	OFDM/CCK, OFDM, DQPSK/CCK, DQPSK, DBPSK
Channel Access	CSMA/CA with RTS/CTS	OFDM	CSMA/CA with RTS/CTS	CSMA/CA with RTS/CTS and OFDM
Data Rates	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 22, 24, 33, 36, 54 Mbps
Data Traffic	TCP/IP	TCP/IP	TCP/IP	TCP/IP
Range	50 m	100 m	100 m	100 m
Error Robustness	CRC/ARQ Type II	CRC/ARQ Type II	CRC/ARQ Type II	CRC/ARQ Type II
Security	YES	YES	YES	YES
Communications Topology	Peer-to-Peer, MS-to-BS	Peer-to-Peer, MS-to-BS	Peer-to-Peer, MS-to-BS	Peer-to-Peer, MS-to-BS
Vender Stability	N/A	Very Good	Very Good	Very Good
Device Scalability	Low	Very Good	Very Good	Very Good
Data Scalability	OK	Very Good	Good	Very Good
Transmit Power	NA	NA	NA	NA
Energy Conservation	Directory Based	Directory Based	Directory Based	Directory Based
Capital Cost	N/A	Access Point: ≥$190 Adapter: ≥$66 Chipset: N/A	Access Point: ≥$50 Adapter: ≥$20 Chipset: N/A	Access Point: ≥$80 Adapter: ~$36 Chipset: N/A
Operational Cost	None	None	None	None

Table 5.1 Protocol Comparison Table 1

Characteristic	Bluetooth	HomeRF	Ultrawideband
Operational Spectrum	2.402 - 2.480 GHz	2.404 - 2.478 GHz	Full Spectrum
Bandwidth	78 MHz	74 MHz	Physically Limited
Modulation Type	FHSS (1600 Hops/sec), GFSK	FHSS (50 Hops/sec), 2-FSK, 4-FSK	Pulse Modulation Technique
Channel Access	Master-Slave Polling	CSMA/CA and TDMA	N/A
Data Rates	.721 Mbps Peak	.8, 1.8 Mbps	100 – 500 Mbps
Data Traffic	PPP	TCP/IP	N/A
Range	Regular – 10 m High Power – 100 m	50 m	2-10 m
Error Robustness	1/3 rate FEC, 2/3 rate FEC, ARQ Type 1	CRC/ARQ Type I	N/A
Security	YES	YES	N/A
Communications Topology	Peer-to-Peer, Master-to-Slave	Peer-to-Peer, MS-to-BS	N/A
Vender Stability	Very Good	N/A	N/A
Device Scalability	Currently Very Low	Good	Very Low
Data Scalability	Low	OK	Very Good
Transmit Power	NA	100 mW	200-300 mW
Energy Conservation	Yes	Directory Based	N/A
Capital Cost	Adapter: ~$30 Chipset: Under $4 in Bulk	N/A	N/A
Operational Cost	None	N/A	N/A

Table 5.2 Protocol Comparison Table 2

Chapter 6
Hardware Design

6.1 System Design and Communications

It was mentioned in the previous chapter that many different devices have been designed utilizing 802.11b. 802.11b systems are typically designed for use in an environment where a group of computers in a home or office must be networked together on a WLAN. Therefore, as mentioned previously, the 802.11b protocol is designed to use TCP/IP for routing of its communications. The TCP/IP protocol is used in all wired networks for network routing. As a result, designing a system using 802.11b does not require any conversions from TCP/IP to another routing protocol when interfacing between a wired network and a wireless network. A diagram of the high level design using TCP/IP is shown in Figure 6.1.

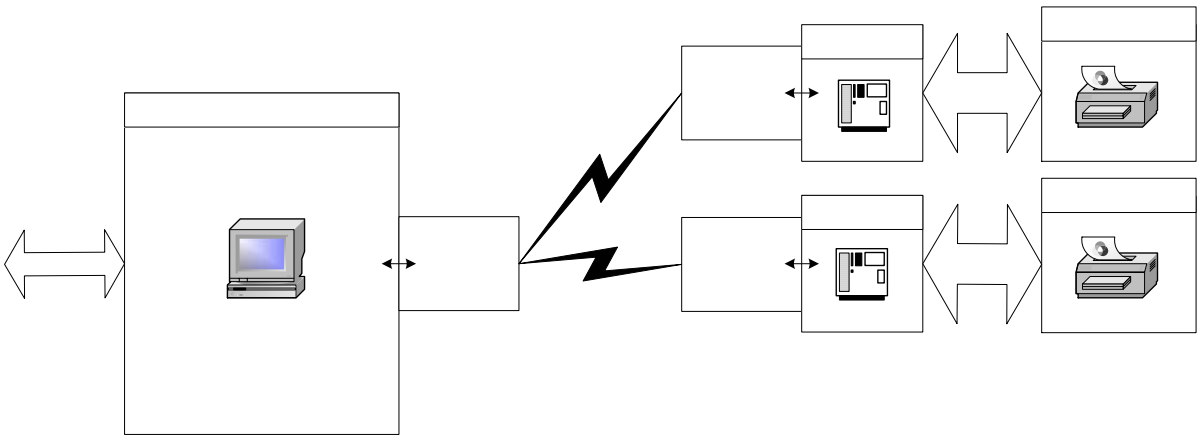

Figure 6.1 High Level Hardware Design

Note: The naming convention utilized is not the typically name of devices on an 802.11b network. The Access Point is contained within the Client Device and the Server Device contains the Adapter Device.

The above design shows a single communications network, where the wireless access point controls the activity of the wireless network. For the device services system, the 802.11b device would be configured to use the infrastructure topology, if available, where the access point has complete control of the data activity on the network. The wireless network adapters will be attached to the devices through a server device. This server device must be capable of handling the polling of data from the client device and transmitting the data to the wireless access point when desired. The interface between the server and target devices is being handled by a separate group with the supporting company, so this design is only going to be concerned with the interface between the server device and the client device. For the transfer of data from the server device to the host computer, a polling style technique will be used. This polling technique is similar to the polling design of the Bluetooth protocol.

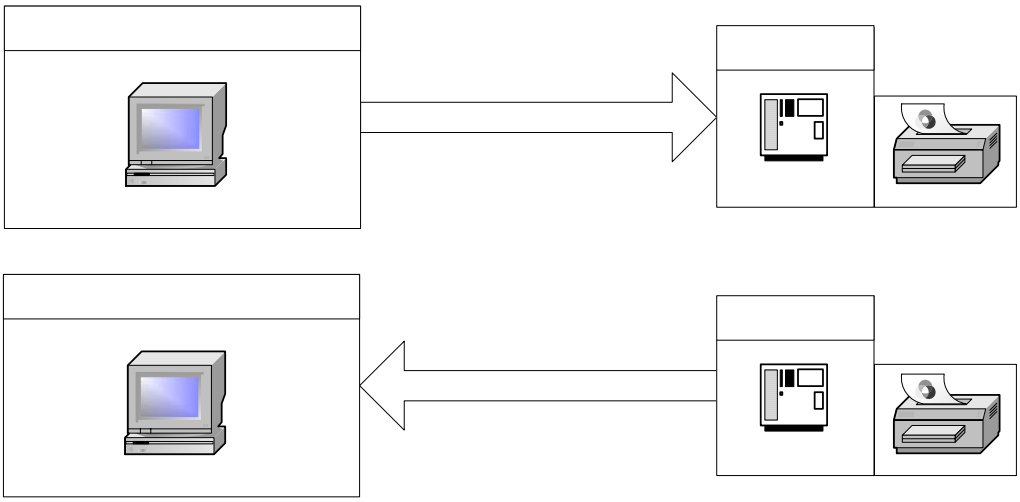

Figure 6.2 Device Services Data Transfer System

Figure 6.2 shows the data transfer technique that is going to be used for the device monitoring system. The underlining 802.11b devices will control the channel access and

convert the data for wireless transmissions as defined in the 802.11b protocol standard. This system needs to be designed so that there is no need for user intervention at the server end of the system. Therefore, the control of the system must occur at the client device, utilizing user intervention when data is desired or the use of a scheduling procedure to initiate the poll. The data transmission interface between the server device and the target device was not defined for the overall system.

6.2 System Layout in a Building

To make the device services system efficient, as explain in Chapter 3, the network WLAN needs to be placed in such a way that the client devices are used as efficiently as possible. This will require knowledge of the position of the devices. When host computers are introduced to a location, they will have to be placed as efficiently as possible. This means that in a single location the fewest number of client devices must be placed to be capable of accommodating all the server devices with the fewest number of WLANs created. When the client devices are placed at a location, it is going to appear to be similar to a cellular system. Indoors, a device operating with the 802.11b protocol is able to achieve approximately 50 meters because of the extra interference introduced by walls and other devices that operate on the same frequency band. For this reason, it cannot be expected that a single 802.11b device connected to a client device will not be capable of connecting to every device in a location or even a floor of a large building.

Figure 6.3 shows an example of two networks connecting all the devices on a signal floor. Notice that the placement of the client devices is in between a number of devices. Keeping the client devices in the middle of a set of devices maximizes the range that is

available from the client device. In this example target devices one through five are connected to client device 1 and target devices six through nine are connected to client device 2. There is one device that overlaps between the two networks. This will require that the two networks operate on different channels. This requires that the networks operate using a different pseudorandom sequence. Device 5 was chosen to connect to client device 1 instead of client device 2 because it was closer to client device 1 for this example. In practice, this connection would have to be tested to decide which client device offers the strongest signal to device 5.

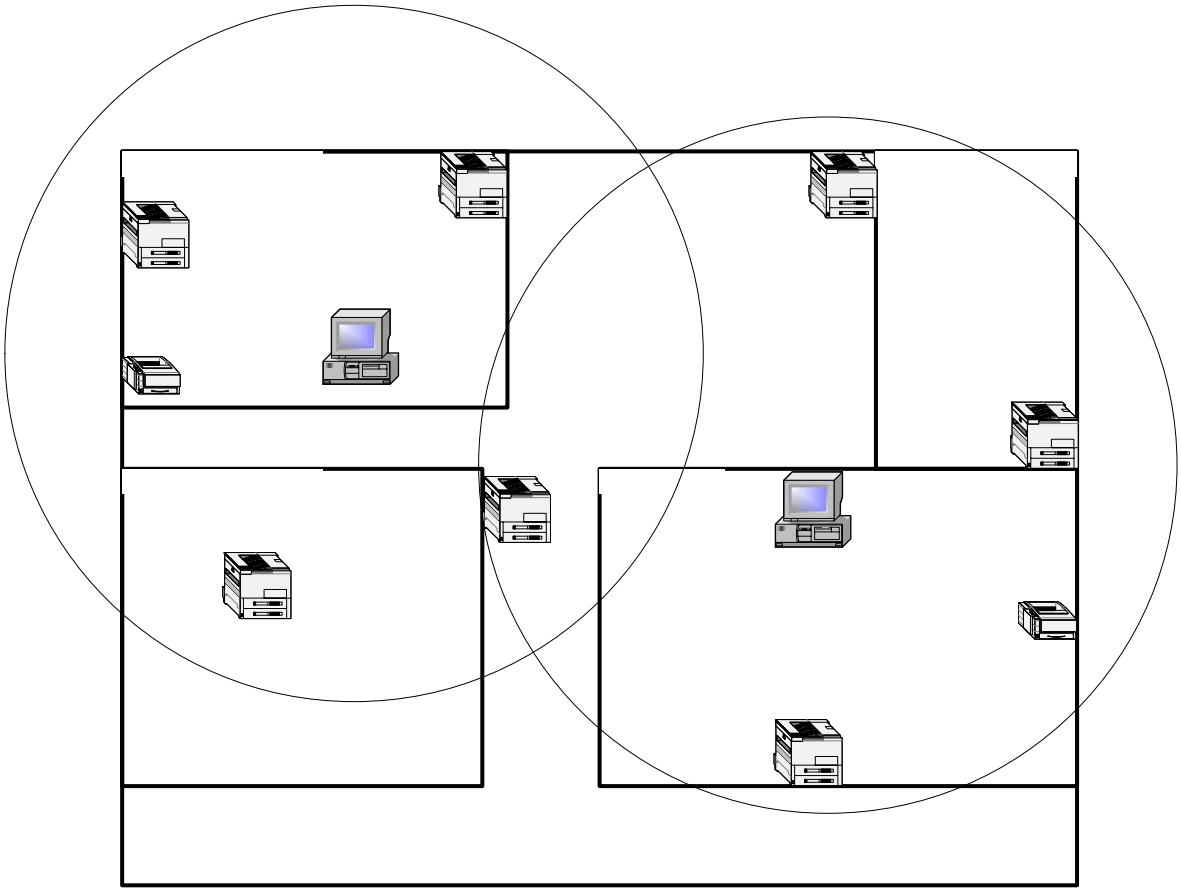

Figure 6.3 Placement of Host Computers

Note: A server device will have to be connected to all devices to create the device monitoring system.

This example shows the dependence of the placement of the client device on the locations of the target devices. If a target device was placed out of the range of the current client devices, a new client device would have had to be added if the two client devices could not accommodate all the devices at the location. This demonstrates the issues involved when attempting to scale the device monitoring system. Hence, when the device monitoring system is deployed at a location, the client devices must be placed well to reduce any issues involved when a new device is added or a current device is moved. There is also the potential for an issue to occur when the amount of data that needs to be transmitted on the network exceeds the capacity of the 802.11b protocol. It is assumed that this issue is unlikely to occur because the data requirements of the system are well within the specifications of the 802.11b protocol.

In this example the client device that has been used is a server or desktop computer. This is not required when using an 802.11b device. The host device could be a laptop computer, PDA, or some other device that can maintain a TCP/IP connection and can store the data received. To make the client devices mobile, a person is going to be required to control the system. Therefore, to keep the system completely independent of user intervention, a server or desktop computer is going to continue to be the device used as the client device.

Chapter 7
Software Development

The software was developed with the intention of implementing it into the parallel project, [21], to satisfy the requests of our supporting company. This software is easily adjusted to work with the wireless local area networking device monitoring application. There are no major differences between the operations of the wireless wide area network and the wireless local area network because they both operate utilizing TCP/IP. The names used for the classes also translate directly to the names used in the hardware design, developed in Chapter 6. The code developed is available in Appendix A.

The software was developed using the Java programming language in the Eclipse development environment. The Java programming language is commonly used for Internet programming and other networking applications. Therefore, the communications were done with the commonly used Java socket connection to transmit data over TCP/IP. The software is not dependant on the hardware, since the communications is done utilizing a protocol known by the native hardware device. The hardware operates the MAC and physical layers of the protocol when implemented in the WLAN application. The only requirement is that the hardware be configured properly upon installation of the drivers.

The software has been developed to implement the communications steps shown in Figure 7.1. This figure shows the steps that must be followed to create a connection between the client, server, and target devices. These connection steps allow the client and server devices to create a connection that can be maintained indefinitely. Once a connection has been created, the client device can poll the server for data as requested by the user. The

client device provides a method for the connection to be terminated, which is initiated by user intervention.

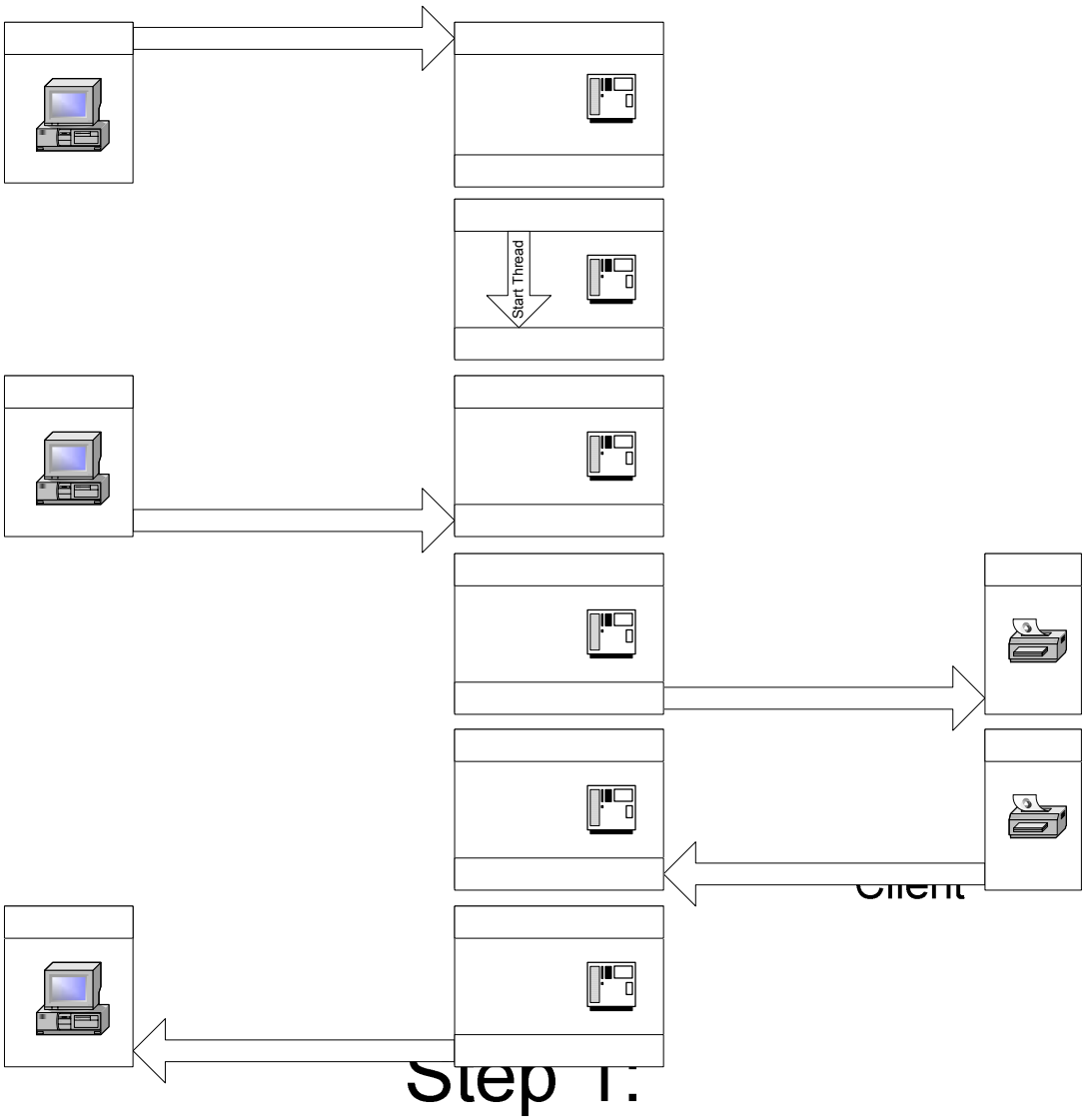

Figure 7.1 Software Polling Interface

Figure 7.1, shows the communications steps that occur between classes during the creation of a connection and subsequently the polling of the device for data. The name on the top of each element is the title of the class that contains the code executing the steps and the name below is the device that the code is operating on. Steps one and two are executed

when creating the socket connection between client and server devices. The thread handler class runs on the server device and receives commands from the client device. Steps three through six are the steps run to poll the target device for data. These steps can be repeated as many times as desired while the connection between the client device and server device is maintained. As stated previously, the connection between the server and target device is unknown and not a concern for this work. Therefore, steps four and five are specific to the simulation of the application being run with a simulated target device. This target device simulation was run in a class, called DeviceSim, which runs on the server device. When the full system is developed, the server communications with the target device must be adjusted to accommodate the communications interface. To clarify the classes developed and their interactions with each other, see Figure 7.2.

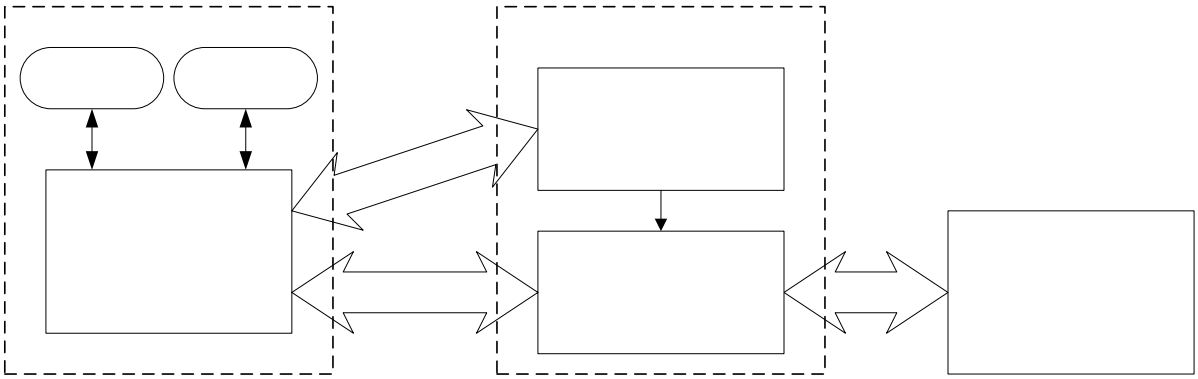

Figure 7.2 Software Interface

This diagram shows the interface between the classes developed in the device monitoring application. They are explained in more detail in the following sections.

7.1 Client Device

As shown in Figure 7.2, the client device consists of graphical user interface (GUI) support code, a console class, and a client class. The GUI support code and console class software is the collection of code that interfaces the software to the user. The GUI is supplied for the user to view the values received from the device and to allow the user control of commands. The GUI can be viewed in Figure 7.3, Figure 7.4, and Figure 7.5.

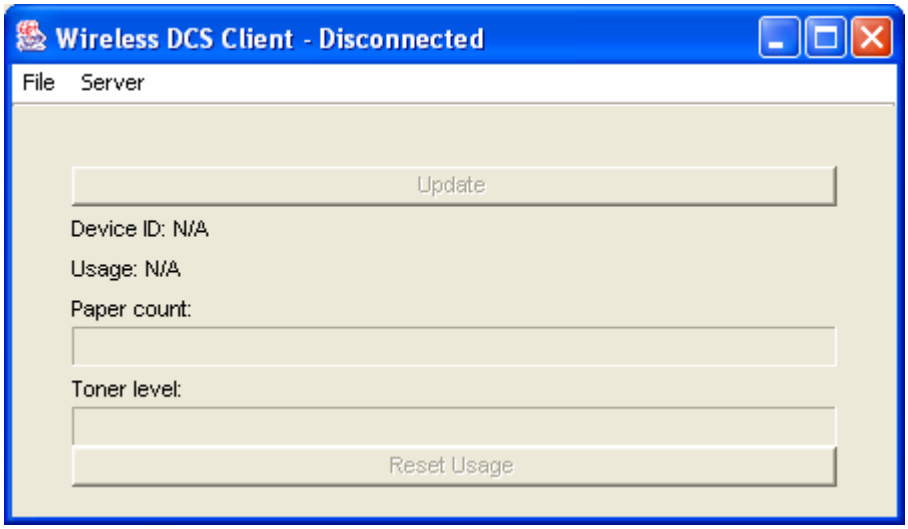

Figure 7.3 Main GUI

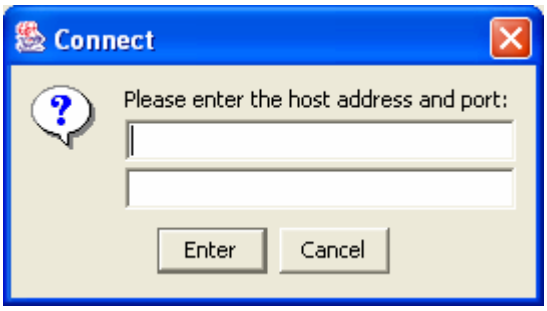

Figure 7.4 Connection GUI

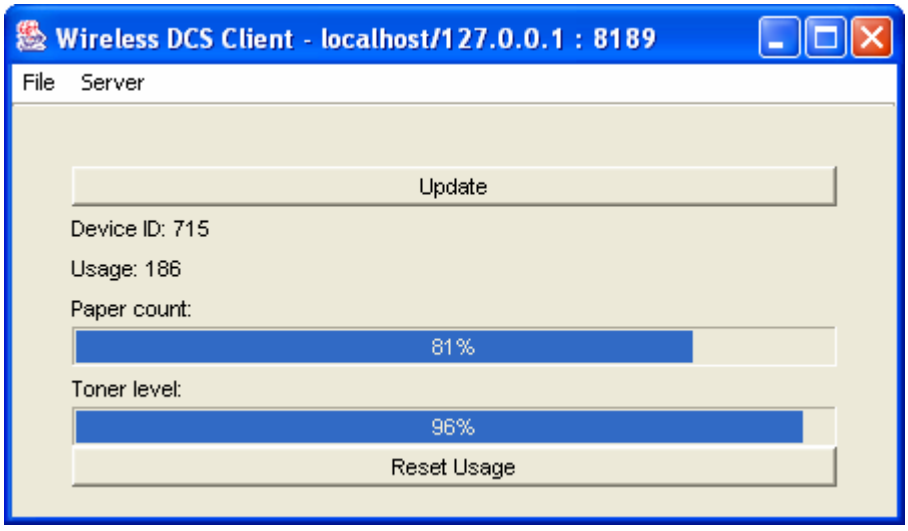

Figure 7.5 Main GUI During an Active Connection

Figure 7.3 shows the main GUI that is initially displayed when the code is initiated. Figure 7.4 shows the GUI panel where the address and port of the server device are entered. This panel is displayed when Server→Connect is selected on the main GUI. The IP address of the server is entered in the top line and the port is entered in the bottom line. Once a connection has been created, the values received from the target device are displayed, along with Update and Reset Usage buttons. The Update button will instruct the client device to poll the target device for all the data contained in the target device. This follows steps three through six from Figure 7.1 for each value that is available. The Reset Usage will set the usage value on the target device to zero.

The console input is used to run the same set of commands that are utilized in the GUI but in a text environment. The available commands to get data from the target device are: t for toner level, p for paper count, u for usage, and i for device ID. These commands initiate a poll of the target device for the data value that will be displayed in the text interface. The commands for other operations are: r for reset usage, h for help, q for quit, and

s for shutdown server. The reset usage command works as the button explained above. The help command displays all available commands. The quit command exits the console and the shutdown server command drops the connection to the server and stops its operation.

The final class of the client device is the client class. This class controls the connection to the server and the polling of the target device. It receives commands from the GUI or console interface and transmits them over a socket connection. Then it receives the returned data, which is passed to the GUI or console for display.

7.2 Server Device

The server device is the interface between the target device and the client device. It accepts commands through the socket connection interface and passes them to the target device. When the target device responds, the data is then sent back through a socket connection to the client device. The operation of the server device is illustrated in Figure 7.6.

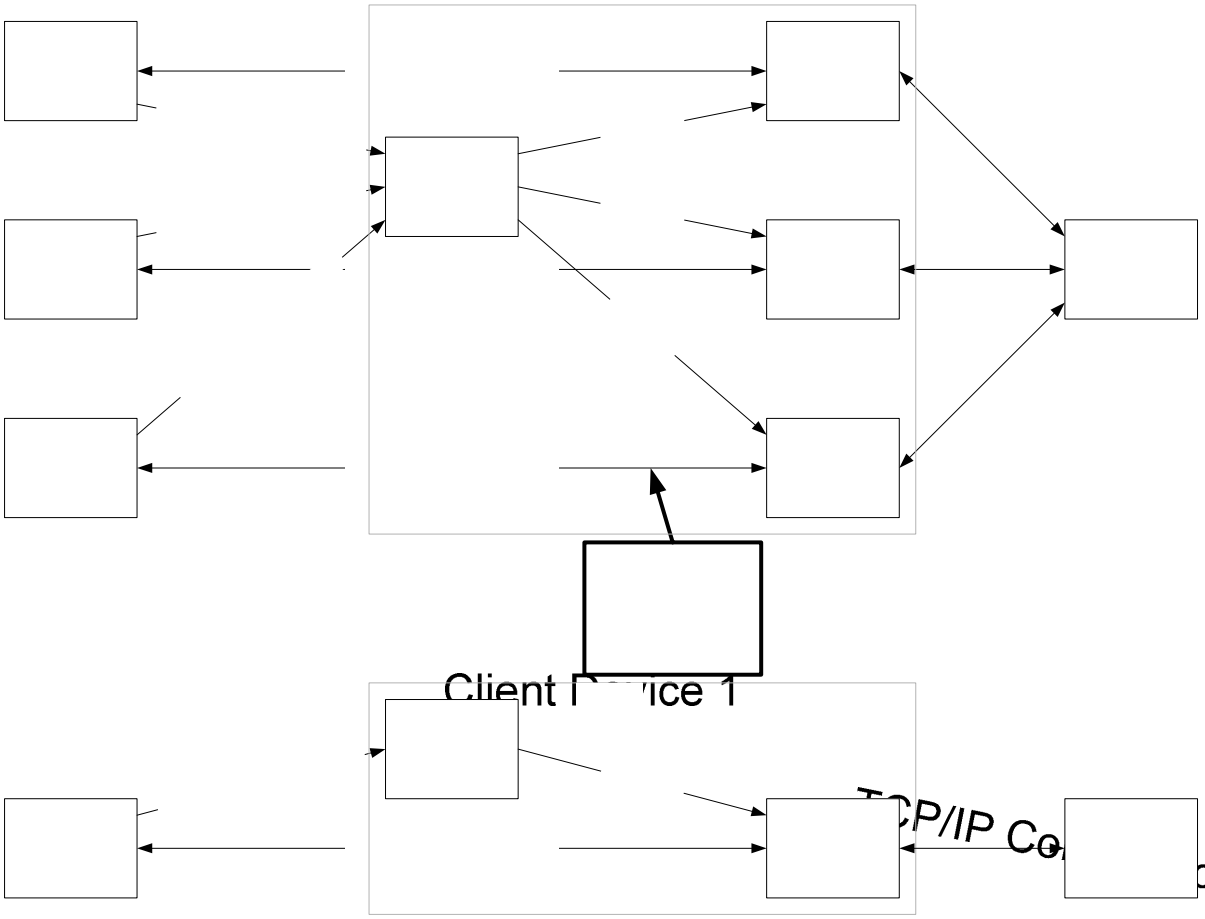

Figure 7.6 Server Device Operation

This figure shows the two classes utilized by the server device. The server class manages requests for connections from client devices and then it spawns a thread, called the Request Handler. The Request Handler handles commands received from the client device. When a command is received, the request handler issues a command to the target device, or SimDevice in Figure 7.6. The target device then returns the requested data or executes the desired command. Once a response is received from the target device, the data is returned to the client device over the client to server socket connection.

The code is capable of handling only one target device connected to a server device. On the other hand, the code is capable of having multiple client devices connected to a server device. This is why multiple threads are required for the server device. The server class must receive a connection request from a client device, which induces the request handler thread for handling the interface between the three devices.

Chapter 8

Future Work and Conclusions

8.1 Integrate WAN and LAN Networking for Device Monitoring

The final step involved in the full development of the device services application is integrating the LAN solution developed in this paper and the WAN solution that has been developed in parallel [21]. Refer to Figure 8.1 for a diagram of the integrated system. This figure shows the connections that will be used to develop the entire device monitoring system from the client device in a remote location to the local target device.

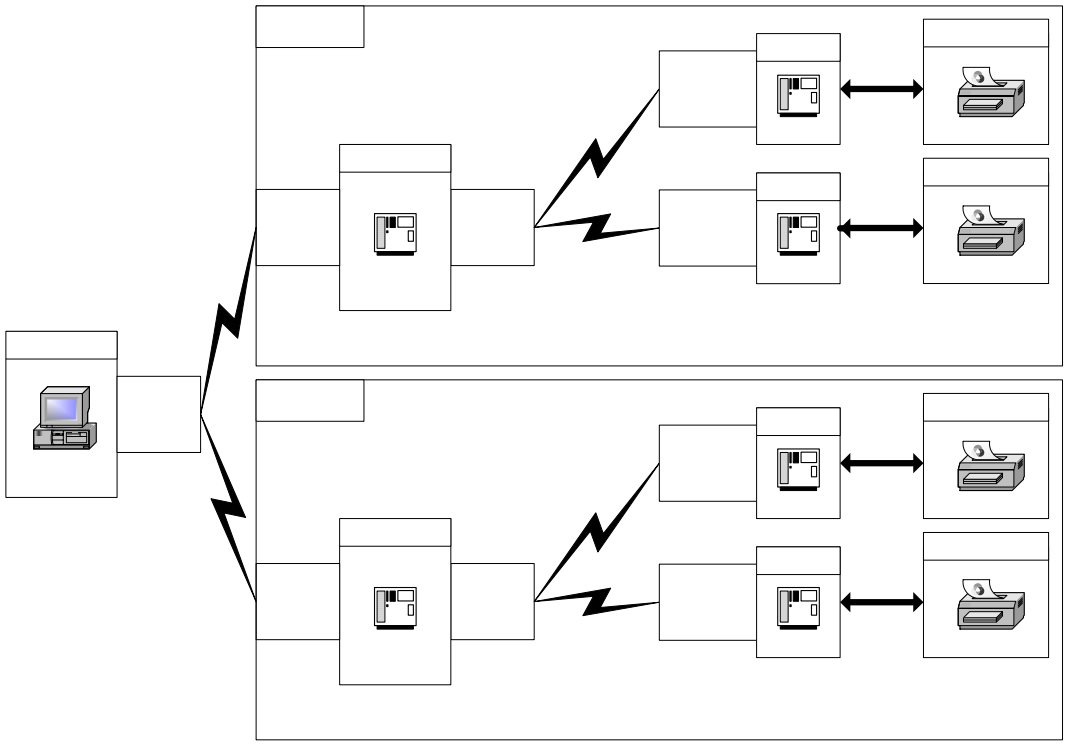

Figure 8.1 WAN and LAN Integration

Figure 8.1 shows that there will have to be the addition of a WAN-LAN interface device into the system. This device is required to route TCP/IP data received from the WAN to the LAN communications mediums and visa versa. The software running on the WAN-LAN interface device is going to be similar to the server device software developed in Section 7.2. It will accept a poll from the WAN, initiating the device to create a socket connection with the server device. There is no manipulation of the data required because both networks utilize TCP/IP routing. The device will then pass the data received to the server device to finish the polling sequence with the target device. The data is then returned from the server device to the WAN-LAN interface device, which passes the data back to the client device. It is clear that the integration is not going to require any changes to the systems developed. New steps will have to be added to the software-polling interface for the entire data path.

The WAN-LAN interface device will be a device that can run the software developed. It must also be capable of containing the cellular modem and the 802.11b wireless access point, along with the drivers required for interfacing the devices between the software developed, running on the operating system, and the hardware devices used. To be capable of running the developed software, the WAN-LAN interface device must have an operating system that operates the code, typically a workstation. An on-location view of the integrated device monitoring system can be seen in Figure 8.2.

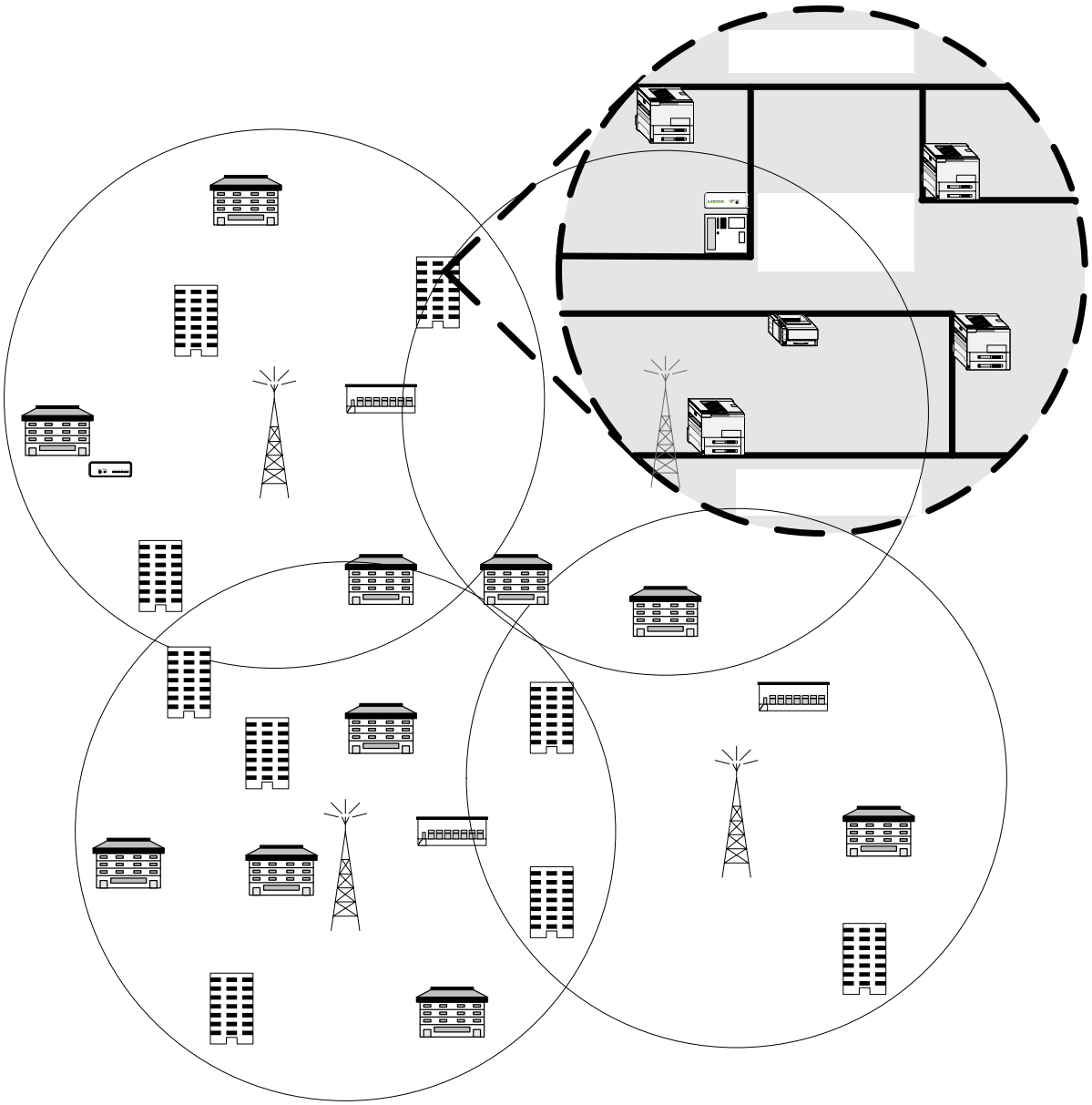

Figure 8.2 Integrated Networks for Device Monitoring

Note: The WLAN Access Point is contained within the WAN-LAN Interface Device

Figure 8.2 shows that the system has been expanded to a cellular system connected to a WLAN system. The location dependencies are expanded to be affected by the location of the building and the location of the devices. The cellular backbone is used to connect the

WAN-LAN interface devices to the client device, with the WLAN protocol used to connect the WAN-LAN interface to the server and target devices. It is clear that the wireless WAN is similar to the WLAN, with the devices from the WLAN being equivalent to buildings in the WAN application.

8.2 Conclusions

A wireless local area networking system has been developed for the use in a device monitoring application. The IEEE 802.11b protocol was determined to be the best fit WLAN protocol to utilize in the application based on its cost, range, data rates, and networking topology. The 802.11b protocol makes data networking straightforward because of its use of the TCP/IP protocol. Thus, the network is easily interfaced with wired LANs and the wireless WAN. The 802.11b protocol was then utilized to design a hardware configuration to be used in the device monitoring application. 802.11b has a large transmission range and good data rates, so it integrates well onto a location where it can handle many devices to minimize the WAN costs.

Software was then developed for the parallel WAN for the device monitoring site application. This code can be integrated into the WLAN application in a straightforward manner. The software then implements a polling interface between the client, server, and target devices. This software is shown to be flexible to accommodate many different situations. The software will require future development when integrating the WAN and LAN applications together and when adding the actual interface between the server device and target device.

8.3 Contributions

A fully wireless solution for implementation into the DCS system has been developed in this thesis. This thesis concentrates on the WLAN solution and also offers hardware architecture for integrating with the wireless wide area network solution [21]. This thesis offers a complete review of popular WLAN protocols, including 802.11, 802.11a, 802.11b, 802.11g, Blutooth, HomeRF, and Ultrawideband. A complete comparison of the capabilities of the WLAN protocols in the DCS system is executed with 802.11b chosen as the most appropriate protocol for the DCS system. Then hardware architecture is designed for the DCS system coving hardware issues involved in the implementation of the system are discussed. Finally, software is developed and tested for managing the communication of this system that runs on top of the WLAN solution. The resulting system offers the supporting company with a fully wireless communications solution for implementation into the DCS system.

Appendix A
Prototype Code

The source code contained within is organized using the following package structure:

- EDU
  - ROCHESTER
    - ECE
      - DCSClient
        - Client.java
        - Console.java
        - GUI
          - ConnectDialog.java
          - Gui.java
      - DCSServer
        - DeviceSim.java
        - RequestHandler.java
        - Server.java
      - Tools
        - ConsoleInput.java

Note: all Java code was developed using JDK 1.4.2_01

Bibliography

[1] "54 Mbps IEEE 802.11 Wireless LAN at 2.4GHz," Intel Corporation, November, 2002.

[2] Batra, A. et. al., "Project:IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)," <http://grouper.ieee.org/groups/802/15/>

[3] Batra, A., et. al., "Physical Layer Submission to 802.15 Task Group 3a: Time-Frequency Interleaved Orthogonal Frequency Division Multiplexing," Texas Instruments, Inc., Dallas, Texas, 2003.

[4] Chen, James C., "Meassured Performance of 5-GHz 802.11a Wireless LAN Systems." Atheros Communications. Sunnyvale, CA. <www.atheros.com>.

[5] Haartsen, Jaap C., Sven Mattisson. "Bluetooth—A New Low-Power Radio Interface Providing Short-Ranged Connectivity." Proceedings of the IEEE October 2000: 1651-1661.

[6] Heinzelman, W., Lecture Presentations from ECE 437, Wireless Communications, Electrical and Computer Engineering, University Of Rochester, 2003.

[7] "High-Speed Wireless LAN Option 802.11a and 802.11g." Wireless LAN Association. San Jose, CA. < www.wlana.org>.

[8] "IEEE 802.11a White Paper." <http://www.vocal.com/data_sheets/ieee802.11a.html>

[9] "IEEE 802.11b White Paper." <http://www.vocal.com/data_sheets/ieee802.11b.html>

[10] Lansford, J., "HomeRF™/SWAP: A Wireless Voice and Data System for the Home," Intel Communications Architecture Labs, Hillsboro, Oregon, 2000.

[11] Lansford, J., Paramvir B., "The Design and Implementation of HomeRF: A Radio Frequency Wireless Networking Standard for the Connected Home." Proceedings of the IEEE October 2000: 1662-1676.

[12] Leeper, D.G., " Ultrawideband – The Next Step in Short-Range Wireless," Intel Corporation, Chandler, Arizona.

[13] Lough, L. Danial, et. al. "A Short Tutorial on Wireless LANs and IEEE 802.11." The Bradley Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University. Blacksburg, Virginia. <http://www.computer.org/students/looking/summer97/ieee802.htm>.

[14] Kraemer, R., "Bluetooth Based Wireless Internet Applications for Indoor Hot Spots: Experience of a Successful Experiment During CeBIT 2001," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Volume 41 , Issue 3, February 2003, pp. 303 – 312.

[15] Matiae, D., "OFDM as a Possible Modulation Technique for Multimedia Applications in the Range of mm Waves," 1998, <www.ubicom.tudelft.nl/MMC/Docs/introOFDM.pdf>

[16] Negus, K. J., Stephens, A. P., and Lansford, J., "HomeRF: Wireless Networking for the Connected Home," 2000, < pompone.cs.ucsb.edu/~wenye/majorexam/ Communication/Negus00.pdf>

[17] O'Hara, B. and Petrick, A., IEEE 802.11 Handbook: A Designer's Companion, Standards Information Network, IEEE Press, New York, New York, 1999.

[18] Rappaport, T. S., Wireless Communications: Principles and Practices, Second Edition, Prentice Hall PTR, Upper Saddle River, New Jersey, 2002.

[19] Salonidas, T., Bhagwat, P., Tassiulas, L., and LaMaire, R., "Distributed Topology Construction of Bluetooth Personal Area Networks," University of Maryland at College Park, < www.ieee-infocom.org/2001/paper/785.pdf>

[20] "Wireless-B Access Point User Guide," Linksys, < http://www.linksys.com>

[21] Zacharias, O., "Wireless Wide Area Networking for Device Monitoring," University of Rochester, Rochester, New York, 2004.

[22] <http://focus.ti.com/docs/apps/catalog/overview/overview.jhtml?templateId=1101&path= templatedata/cm/level1/data/wire_ovw>

[23] < http://java.sun.com>

[24] <http://www.eclipse.com>

[25] <http://www.newegg.com>

[26] <http://focus.ti.com/docs/apps/catalog/overview/overview.jhtml?templateId=1101&path= templatedata/cm/level1/data/wire_ovw>