Jan Suwart

Wireless Ad Hoc Networks: Limitations, Applications and Challenges

08 April 2008

Technische Universität at Braunschweig
Institute of Operating Systems and Computer Networks (IBR)

Project Thesis

Wireless Ad Hoc Networks:
Limitations, Applications and Challenges

by
Jan Suwart

Task formulation and supervision:
Prof. Dr.-Ing. Lars Wolf and M.S. Habib-ur Rehman

Braunschweig, 08 April 2008

Erklärung

Ich versichere, die vorliegende Arbeit selbstständig und nur unter Benutzung der angegebenen Hilfsmittel angefertigt zu haben.

Braunschweig, den 7. April 2008

Abstract

In the near future, there will be an increasing need to provide applications such as internet deployment for areas without infrastructure, wireless video streaming between moving objects, data exchange between office equipment etc. These applications can be solved with the help of wireless ad hoc networks that can be realized e.g., with Wi-Fi protocols. The question arises, what theoretical throughput different wireless standards can achieve, and how much the throughput will decrease when data has to be transferred over several hops.

This thesis provides an overview of wireless technologies which can be used in ad hoc scenarios. Their limitations are calculated using a formula created by us to determine the theoretical maximum throughput of the standards. The results show that in ad hoc mode the various Wi-Fi standards are limited to a fraction of their original throughput. Our findings are supported through additional testbed results. A scenario analysis shows that ad hoc networks could improve the performance of both small wireless home and office networks as well as large or mobile networks that require a high transmission range. These scenarios can be realized with the presented technologies. Even video transmissions can take place in ad hoc networks using techniques as resource allocation or multipath streaming. Recommendations are proposed, how the problem of mobile ad hoc scenarios can be solved on a limited scale with the help of delay-tolerant networks. The deployment of a low-cost internet access can be realized e.g., with mesh networks, and a communication between digital cameras, printers etc. can be realized with standards like Bluetooth.

Table of Contents

1. Introduction

Today wireless networks are used daily by millions of people. We use this technology for wireless Internet access with our laptop, for data transfer between phones, and even to play multiplayer games with portable game consoles. However, hardly any of these wireless networks operate in ad hoc mode. These kinds of networks have many advantages over wired networks: ad hoc networks do not require infrastructure, they can be deployed instantly and they are highly flexible. An ad-hoc network can increase both the range and the entire coverage area of the network. The scenarios in which this type of networks can be used are varied, and the application areas range from Internet access to video streaming to live conferencing up to disaster recovery.

There are different technologies and protocols available that are suitable for the use in ad-hoc networks. Particularly well suited is the IEEE 802.11 standard that meets all requirements for a use in ad hoc mode. Today's Wi-Fi standards have a sufficient transmission range and a high data rate. Upcoming Wi-Fi standards will achieve data rates, which have never been possible previously. But even older standards like Bluetooth have ad hoc capabilities that can be useful for wireless data exchange.

On the other hand, a transmission of data over a wireless medium involves adverse effects like noise, fading and interference that the nodes have to deal with. These effects reduce the effective bandwidth compared to a wired network connection. There is a higher overhead due to bigger headers, Interframe space times and collision treatment. The overhead is continuing to increase, as soon as data is transmitted along multiple hops in an ad-hoc network.

Before the technologies are presented in detail, we should define the term "ad hoc network". The differences between mobile ad hoc networks and mesh networks should be made clear as well.

1.1 Ad Hoc and Mesh Networking

A wireless ad hoc network is a collection of independent nodes or stations which communicate with each other by creating a multihop radio network. A network where nodes are all connected to each other can be called mesh network. A significant fact is that the connection is maintained in a decentralized way. Every node of a wireless ad hoc network is a user terminal and a router at the same time. The management of the network is distributed between all nodes. Therefore, it is extremely necessary to have efficient routing algorithms which make it possible to exchange data over paths consisting of multiple nodes, in other words hopping over multiple nodes. This approach is called multihop transmission. It is important to ensure that such transfers do not waste more resources than they should. The efficiency of a multihop data path depends on the routing algorithm for the most part [1].

An important feature of mesh networks is the ability of self-healing. The network can still function when a node fails or a path gets congested. In that case, nodes can discover different routing paths and the data can be transmitted along an alternative path. Redundancy makes a mesh network very reliable.

The decentralized structure makes ad hoc networks suitable for applications where a centralized structure could be unreliable. Another advantage is the better scalability of ad hoc networks in contrast to centralized wired networks. Ad hoc networks can be easily extended with further nodes at any point in the network. Adding more nodes to the network enables to choose more alternative paths. This also increases the capacity of the network.

Wireless ad hoc networks abandon the usage of cables to wire neighboring nodes. This characteristic makes them very flexible. Usually distances between neighboring nodes remain

short. But it is also possible to use these networks for longer distances. Ad hoc networks can maintain the signal strength by splitting a longer distance into a series of shorter hops. Intermediate nodes can make routing choices based on their knowledge of the network.

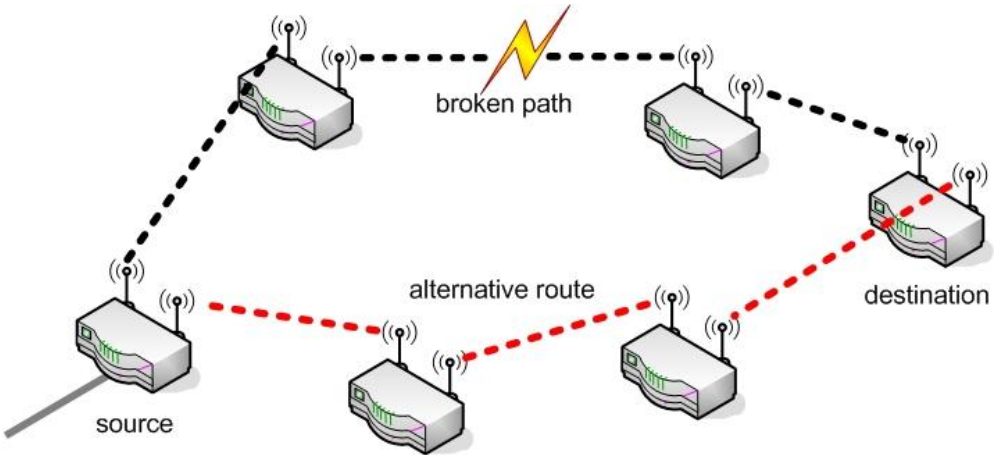

Figure 1: ability of self-healing in a wireless mesh network

In Figure 1 we can see that the path between the two upper nodes has broken down. Because a mesh network has the ability of self-healing, nodes can discover alternative routes to the destination. This example also makes clear that nodes self-organize and thereby the mesh network is created. In Figure 1 every node can operate as source, destination or a relay for other node's traffic.

The topology of the network can also change at any time. Nodes can always leave the network and new nodes can be added. Movement of individual nodes is possible as well, i.e. mobile nodes may exist. A mesh network where movement of nodes is allowed is called Mobile Ad Hoc Network (MANET). Scenarios such as emergency services, disaster recovery and transportation systems are examples of use for the deployment with mobile networks. Usually there is no previously established network infrastructure provided for this kind of scenarios, and this kind of applications cannot rely on a centralized network. The MANET has a decentralized structure and all participating nodes are responsible for discovering the network topology and for delivering messages by themselves. Because the users are mobile, the network topology can change unpredictably during an ongoing data transfer. Unpredictable mobility of nodes introduces more routing problems.

Now the question arises whether applications as Internet access or video streaming would work in an ad hoc environment where data would be transmitted over several nodes from source to destination. Do wireless ad hoc networks have the capabilities to support multimedia applications? Can mesh-like networks guarantee the throughput and the latency that is required for multimedia applications? We will try to answer these kinds of questions in this thesis. Furthermore, we will introduce technologies that are suitable to operate in a multihop ad-hoc mode. Also, we will introduce real life scenarios where the use of ad-hoc networks would involve an advantage.

This thesis is organized as follows: In this first chapter we define the concept of ad-hoc networking. In Chapter 2, we present several wireless technologies, and we calculate their maximum theoretical throughput. Chapter 3 presents a variety of real-life scenarios where an ad hoc network is used. In Chapter 4 the technologies are confronted with the real life scenarios presented in Chapter 3. In the last chapter we discuss the suitability of each standard for the use in the presented scenarios. Thereafter, we demonstrate for what purpose which technology can be used, and we suggest further recommendations.

2. Wireless technologies capable of Multihop Ad-hoc

This section introduces several wireless technologies that are able to form a wireless ad-hoc network. A theoretical throughput analysis of these technologies is presented. The investigation of the technologies' maximum throughput is based on a static topology where nodes are not in motion but are stationary. As already mentioned in the introduction, we do not need infrastructure in ad-hoc mode. Instead a scattered set of wirelessly connected nodes provides us with an area-wide access to the wireless medium. This fact is identical in each of the technologies we will discuss. In this chapter, we want to find out how much the maximum throughput of a data transfer will decrease, as soon as we send data through the network via multiple hops. Our aim is to find out how much the channel capacity is affected by the fact that nodes have to forward each other's traffic. Furthermore, we identify other factors that are limiting the maximum theoretical throughput in an ad hoc network.

The focus of this investigation is put on IEEE 802.11, one of the most widespread wireless transmission protocols today. We take a look at several variations of this technology, which is also known under the term Wi-Fi. We also review a new version of Wi-Fi, the 802.11n 2.0 draft. We illustrate which speed advantage this new version of 802.11 entails. Bluetooth is a technology that already supports ad-hoc capabilities. There is Bluetooth 3.0 currently in development. This fact makes this standard also very interesting for an analysis. The last part of this chapter examines the ad hoc mode of Bluetooth.

2.1 Preconditions

Before the limitations of wireless networks can be examined and a maximum throughput can be calculated, we must first point out the characteristic of wireless networks compared to wired networks. While Fast Ethernet almost offers 100 Mbit/s, the efficiency of 802.11 is nowhere near as high as that of Ethernet. At lower OSI layers, i.e. at the Physical Layer and at Data-Link layer, there are significant differences to Ethernet. New headers were added, several Interframe space times must be respected during a transfer and the collision treatment has been revised. Also packet sizes are smaller in 802.11. Overall, these factors produce a larger overhead. In addition, radio transmissions have to struggle against other difficulties such as packet losses due to fading, reflections and interferences. However, these problems are not part of this work. Our calculations are based on optimal conditions; this means that there are no bit errors, packets are not fragmented and never get lost. Regardless of theoretical calculations we will try to show figures that reflect actual throughput performances of available devices at the end of every section.

2.2 IEEE 802.11 Wi-Fi

Today's operating ad hoc networks are mostly based on the IEEE 802.11 standard from 1999. This standard was enhanced and improved over the last years. This concerns substantially the PHY and MAC layers of the original standard. There are extensions in different directions; some improve throughput, other security (i), quality of service (e) or transmission range (h). However, the versions used today are almost only types a, b and g. Since version a, the faster OFDM modulation is used and data rates of up to 54 Mbit/s are possible. In comparison: legacy 802.11 only offered a maximum data rate of 2 Mbit/s. Table 1 gives a brief overview of used frequency ranges and the transmission speeds. In the following part of this section we take a look at the basic characteristics and functions of 802.11.

	802.11a	802.11b	802.11g	802.11n
Band	5 GHz	2,4 GHz	2,4 GHz	2,4 / 5 GHz
Data rate	54 Mbit/s	11 Mbit/s	54 Mbit/s	300 / 600 Mbit/s
Channels	19	11 USA / 13 EU	11 USA / 13 EU	> 30
Modulation	OFDM	DSSS	ERP-OFDM DSSS-OFDM	OFDM

Table 1: different extensions of the 802.11 standard from 1999

The IEEE 802.11 standard [3] defines a Distributed Coordination Function (DCF) where a randomized wireless medium access mechanism is described. This DFC is based on the CSMA/CA scheme where every device in a wireless network has a fair chance to access the medium.

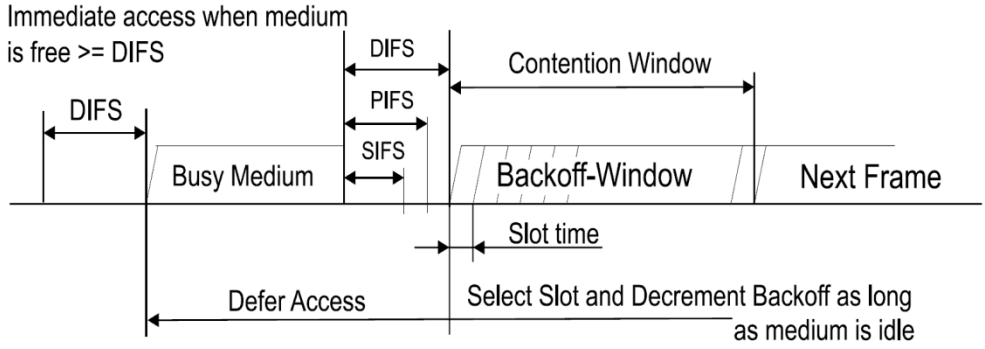

Figure 2: Interframe space relationships [3]

To obtain access to the transmission medium the coordination function defines different inter-frame spacing that are used for the transmission of frames. Figure 2 illustrates the dependency of the inter-frame spacing for 802.11. We will see later that the function uses shorter Interframe Spaces for cases in which the network is composed of only 802.11g devices (compare with Table 2) and longer inter-frame spacing for cases in which there are b and g devices combined in a network.

Our aim is to investigate the factors that have a negative influence on the throughput of the standard. The throughput is mainly affected by the overhead. Real overhead is first added at each OSI layer. Due to protocol headers added at different MAC and PHY sublayers (Figure 3: MAC layer, PLCP sublayer, PMD sublayer), the maximum throughput decreases when a Service Data Unit is transmitted. When a user packet is pushed down to the MAC layer a MAC header and trailer (FCS) is added. The new packet forms a MAC Protocol Data Unit that is again pushed down to the PHY layer where a PLCP preamble and a PLCP header are added. This is illustrated in Figure 3. Not until then the inter-frame spacing is inserted (IFS) before and after every bit stream that is ready for transfer. Even a time-frame for 802.11's backoff scheme (BO) must be added at the end. A larger payload has a positive effect on the efficiency of a transmission, which means that the percentage of the overhead is lower with a large payload.

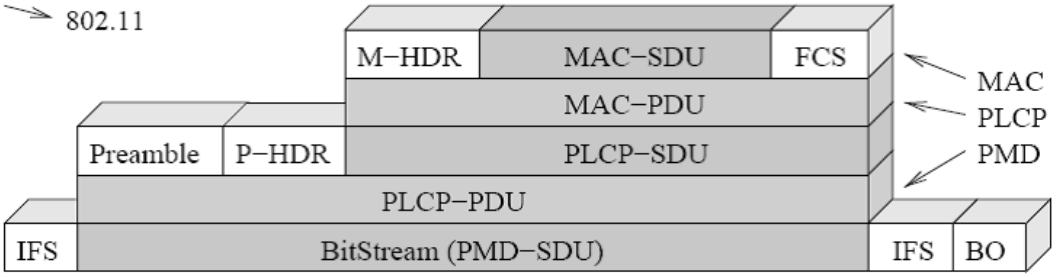

Figure 3: overhead at different sublayers [2]

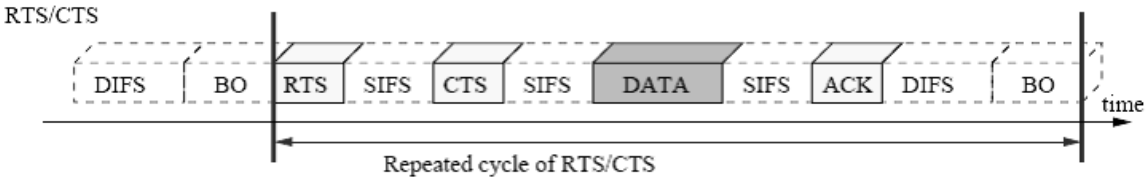

Figure 4: timing diagram for CSMA/CA and RTS/CTS [2]

It should be noted that Service Data Units (SDU) represent the actual user payload at the transition between two layers. Unlike SDUs, Protocol Data Units (PDU) include the payload and the overhead at each sublayer. At the bottom of the chart in Figure 3 we have the actual bitstream, which contains the entire overhead that accumulated in the layers above. In a larger context, exactly this bitstream is the DATA-field of Figure 4.

In Figure 4 we can see that 802.11 uses different Interframe Spaces (IFS). The Short Interframe Space (SIFS) is inserted before high-priority frames like RTS, CTS and ACK frames. The DCF-Interframe Space (DIFS) is used during every contention based operation and can be followed by a backoff period if the medium is occupied. We can conclude that the time it takes to transmit a MSDU at MAC layer while using the access method with RTS/CTS is defined by:

$$MSDU_{\mathrm{RTS/CTS}} = (DIFS + 3\,SIFS + BO + RTS + CTS\ + ACK + DATA)\mu s$$

With switched off RTS/CTS the delay per MSDU is defined by:

$$MSDU_{\mathrm{CSMA/CA}} = (DIFS + SIFS + BO + ACK + DATA)\mu s$$

DATA represents the time required to transmit the MAC Header (30 byte), the FCS trailer (4 byte) and the MAC-SDU with the payload. The MAC-SDU can have a maximum size of 2346 Bytes which includes a frame body of a variable size of 0 – 2312 Bytes and 34 Byte long header and trailer. *DIFS*, *SIFS*, *BO* and *ACK* represent the time to transmit these control frames. The time that we need for the transmission of each element of the equation above depends on the chosen modulation and transmission speed. In the next section, we do this calculation for 802.11g. The maximum MAC throughput of 802.11 with CSMA/CA is defined as:

$$Throughput_{\max} = \left(\frac{MSDU_{\mathrm{payload\_duration}}}{MSDU_{\mathrm{CSMA/CA}}}\right)\mu s * \text{bitrate Mbit/s}$$

2.2.1 The 802.11g Standard

Now that we know how timings and overhead are connected, the throughput calculation can be carried out. We decided to use 802.11g because it is most widespread. The IEEE 802.11g standard defines additional operational modes for the PHY layer and extends the MAC layer functions. IEEE 802.11g [5] was approved in 2003 and builds on the specifications defined for 802.11. The 802.11g standard defines several rate extensions of which the mandatory ERP-OFDM spread spectrum technology allows to transmit with a theoretical speed of 54 Mbit/s. Because of the hidden node problem that influences transmissions in multihop environments, we have to consider the Ready-To-Send/Clear-To-Send protection mechanism for our calculation. Though ERP-OFDM can transmit faster with switched off RTS/CTS, we are using this protection mechanism to reduce the hidden node problem that causes collisions especially in a multihop network.

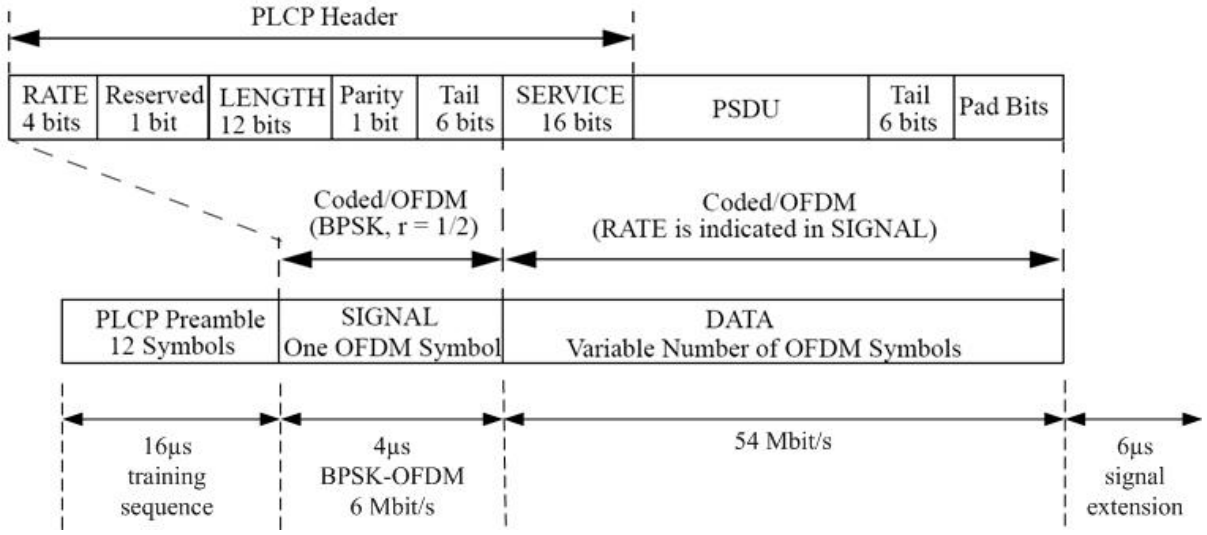

Figure 5: ERP-OFDM-54 PHY layer frame [4]

Figure 5 represents the constituent parts of a PPDU ERP-OFDM frame at PHY layer. The frame includes the PLCP preamble, the PLCP Header, tail bits and pad bits. Every PPDU packet is followed by a signal extension of 6 µs that has to be added to the calculation. During this period no transmissions can be carried out. The purpose of this extension is to make sure that the ERP modulation scheme can be finished on time [5].

Now we are able to define an equation that specifies the time it takes to transmit a PPDU frame with ERP-OFDM-54 modulation:

$$PPDU_{\text{OFDM-54}} = 16\mu s + 4\mu s + \left(\frac{16bits + PSDU_{Size} + 6bits}{54\text{Mbit/s}}\right) + 6\mu s$$

Where $\text{PSDU}_{\text{Size}} = 30\,Bytes + MSDU_{\text{Size 0-2312 Bytes}} + 4\,Bytes$ as we already specified in paragraph 2.2. From this it follows that the transmission of a PPDU frame with a payload of 2312 Bytes needs 373,96µs. Now we only have to add the various Interframe spaces to the calculation to be able to determine the theoretical maximum throughput of 802.11g. The lengths of the standard's Interframe spaces are defined in the following table.

	long	short
slot time	20 µs	9 µs
SIFS	10 µs	10 µs
DIFS	50 µs	28 µs
BO ($CW_{min}/2$)*	150 µs	67,5 µs
RTS	20 bytes	
CTS	14 bytes	
ACK	14 bytes	

* CW_{min}=15 time slots

Table 2: delay components for OFDM-54 with different time slots [5]

Table 2 shows various Interframe space values that are defined in [5]. There are two different time slot lengths defined in 802.11g. A time slot of 20 µs allows backwards compatibility for 802.11b. In our calculation we don't consider a heterogeneous network composed of 802.11b and 802.11g devices because it affects the maximum throughput negatively. Therefore we use the short time slot of 9µs. The minimum size of the Contention Window is set to the length of 15 time slots while using OFDM modulation. The Contention Window (CW) is always the multiple of a time slot. The Backoff duration (BO) is a random variable in the range [0, CW_{min}]. In this calculation we are using an average Backoff duration of $CW_{min}/2$. The average is the mean of the two bounds (uniform distribution). To determine the transmission delay of RTS, CTS and ACK packets we need to insert the size of each packet from Table 2 into following formula:

$$\mathrm{RTS/CTS/ACK_{OFDM\text{-}54}} = 16\mu s + 4\mu s + \left(\frac{16bits + packet_{Size} + 6bits}{54\mathrm{Mbit/s}}\right)$$

The transmission of RTS frames takes 23,37µs while the transmission of CTS and ACK frames takes 22,48µs. If there are 802.11b devices in the network, this frames may only be transmitted with a maximum rate of 11 Mbit/s. Otherwise, 802.11b equipment might not detect a transfer and would start transmissions during a current transfer. In total we require 28µs + 10µs + 57,5µs + 22,48µs + 373,96µs = 491,94µs for a complete CSMA/CA transmission of 2312 Bytes. This results in a maximum throughput of 37,59 Mbit/s.

This value represents the theoretical maximum, which we can achieve if we consider the overhead of PHY and MAC layer. In a scenario where collisions might occur, the backoff algorithm would increase the BO duration exponentially if the medium is busy. This, of course, would have a significant impact on the throughput. On the following pages we will demonstrate that contention and collisions are inescapable in a multihop scenario and what effect this can have on the throughput.

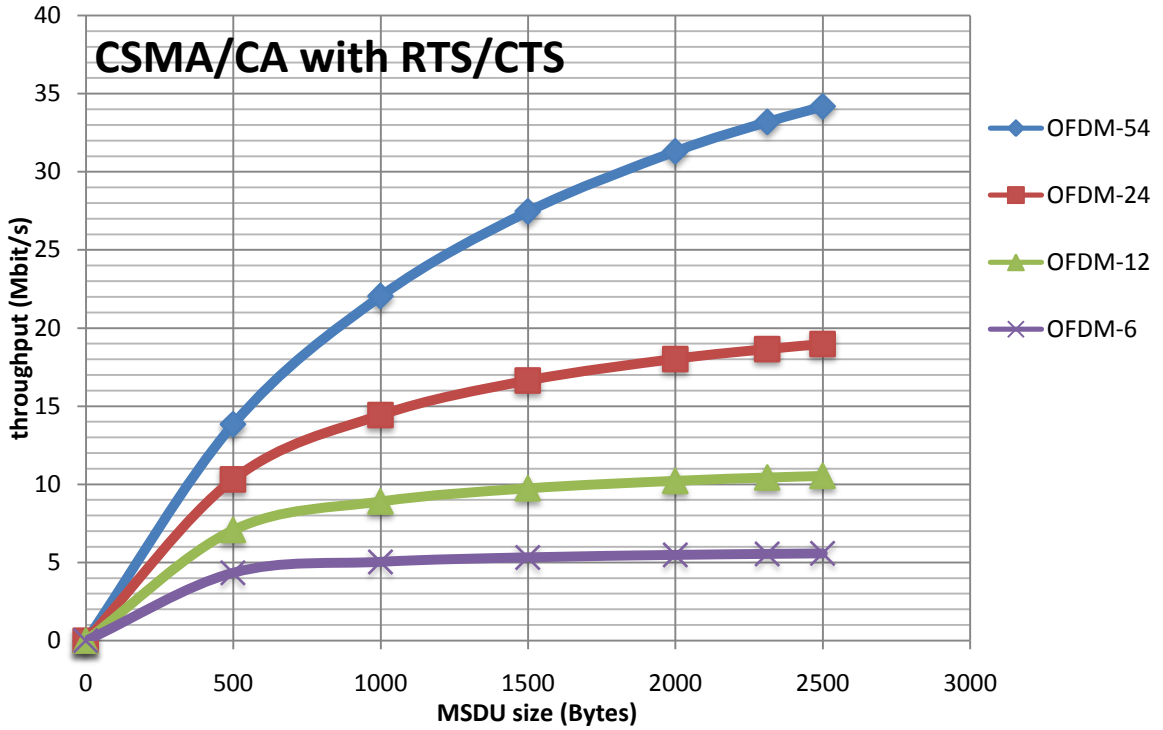

Figure 6a: theoretical maximum throughput curve for ERP-OFDM with RTS/CTS

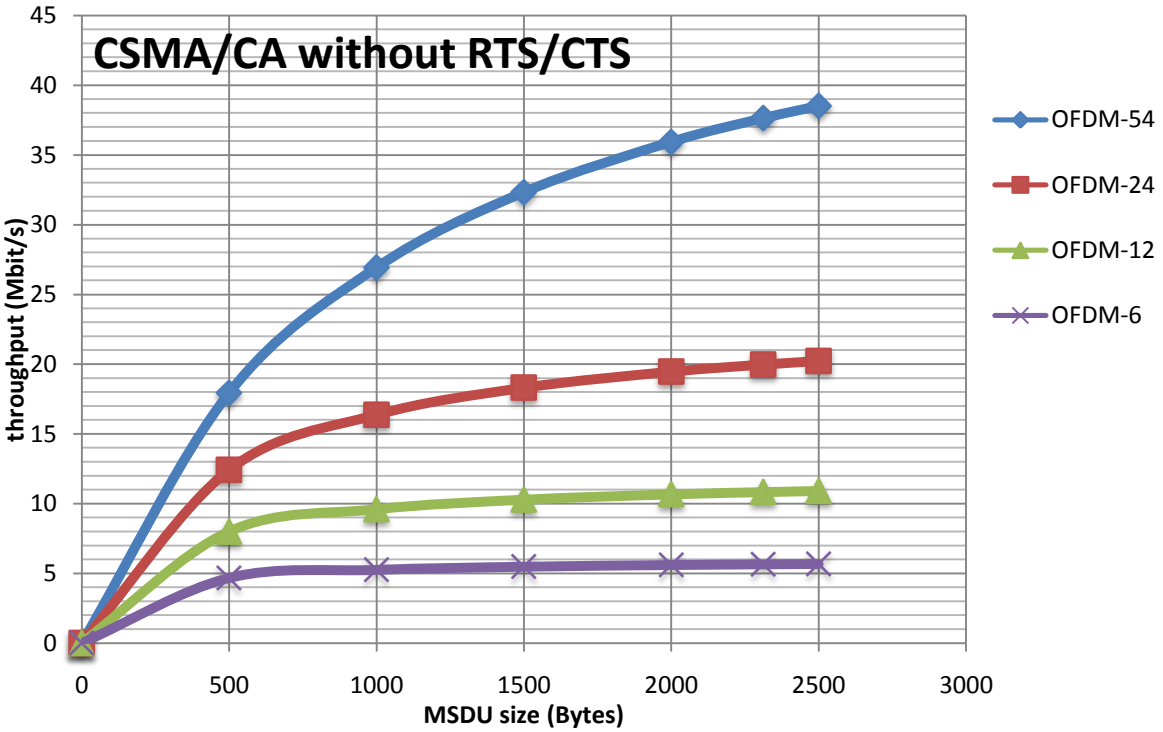

Figure 6b: theoretical maximum throughput curve for ERP-OFDM without RTS/CTS

	data rate (Mbit/s)	packet size (Bytes)						
		0	500	1000	1500	2000	2312	2500
CSMA/CA		**throughput (Mbit/s)**						
OFDM-6	*6*	0	4,67	5,25	5,48	5,60	5,65	5,67
OFDM-12	*12*	0	8,00	9,60	10,28	10,66	10,82	10,90
OFDM-24	*24*	0	12,42	16,37	18,31	19,46	19,97	20,22
OFDM-54	*54*	0	17,92	26,92	32,32	35,92	37,62	38,50
CSMA/CA (RTS/CTS)		**throughput (Mbit/s)**						
OFDM-6	*6*	0	4,33	5,03	5,32	5,47	5,54	5,57
OFDM-12	*12*	0	7,06	8,89	9,73	10,21	10,42	10,53
OFDM-24	*24*	0	10,31	14,42	16,63	18,02	18,64	18,96
OFDM-54	*54*	0	13,84	22,03	27,45	31,30	33,18	34,17

Table 3: theoretical maximum throughput for ERP-OFDM

Table 3 above shows the results of our throughput calculation. The two curves 6a and 6b represent the ascertained figures graphically. The results show a theoretical maximum throughput of 34,17 Mbit/s (with RTS/CTS) and 38,5 Mbit/s (without RTS/CTS). This represents a bandwidth efficiency of 64% (with RTS/CTS) and 71% (without RTS/CTS) with a data rate of 54 Mbit/s and a packet size of 2346 Bytes. Using smaller packet sizes will decrease the throughput. Disabling RTS/CTS increases the throughput.

802.11g also offers other modulation techniques like DSSS-OFDM and ERP-DSSS that have a different frame structure, longer preambles and longer delay components. The disadvantage of the other techniques is the lower data rate of maximal 11 Mbit/s. This fact makes them less interesting for further investigations. The theoretical maximum of almost 40 Mbit/s remains unmatched in real world conditions. In reality wireless devices with 802.11g only achieve 20 – 30 Mbit/s in tests. We can see that the throughput efficiency decreases significantly when we transfer smaller packets. Since IP packets make up the largest proportion in each networks, we can never reach the theoretical maximum.

In reference [2] has been performed a more detailed analysis that concentrates on modulation techniques and bandwidth efficiency and presents similar findings.

2.2.2 The 802.11n Standard

Although the 802.11n standard is still in a draft phase and a final throughput calculation is not possible, a preliminary calculation is still possible based on the latest draft. According to IEEE, 802.11n is expected to be finalized in November 2008 and to be finally approved in June 2009. Many hardware manufacturers already sell 2.0-certified hardware that is based on the 2.0 draft. The certification is carried out by the Wi-Fi Alliance. The final version is supposed not to be significantly different from the draft.

802.11n operates like 802.11a/b/g in the 2.4 GHz band plus the 5 GHz band. 802.11n uses a bandwidth of 40-MHz while 802.11a/b/g only operates in a 20 MHz channel. The indoor range has a radius of 70m; the outdoor range is 250m. The 802.11n standard is expected to be significantly faster than previous standards, with a maximum throughput of at least 100 Mbit/s at the MAC service access point. 802.11n will provide physical layer and MAC enhancements.

The IEEE 802.11n MAC keeps contention-based channel access (DCF) and adopts CSMA/CA with the binary exponential backoff algorithm. 802.11n is adding multiple-input multiple-output (MIMO) to the PHY layer. MIMO is basically the use of multiple antennas at the transmitter and receiver to improve communication performance. 802.11n devices are able

to send several data streams simultaneously. The 802.11n standard includes two MIMO techniques: spatial multiplexing and beamforming. Spatial multiplexing divides data into multiple streams and sends them simultaneously over multiple paths in the channel. Beamforming is a technique that uses several directional antenna elements to spatially shape the emitted electromagnetic wave to beam the energy into the receiver over some optimum path [8].

The OFDM in 802.11n increases the symbol rate, shortens guard intervals and introduces Frame Aggregation and Block-ACK. Frame Aggregation is a method of combining several frames into one what results in a reduction of inter-frame gaps and ACK frames. Block-ACK is a single acknowledgement packet that confirms the receipt of multiple frames. Block ACK improves the efficiency because an ACK frame is not sent after every receieved packet and only the missing frames will be resend after a loss [9].

	Streams			
	1	**2**	**3**	**4**
	20 MHz (Single Channel) 2.4 GHz or 5 GHz Band			
Standard Guard Interval	65	130	195	260
Short Guard Interval	72,2	144,4	216,7	288,9
	40 MHz (Channel Bonding) 5 GHz Band			
Standard Guard Interval	135	270	405	540
Short Guard Interval	150	300	450	600

Table 4: Maximum 802.11n Transmission Rates in Mbit/s [10]

Table 4 presents an overview of transmission rates of the 802.11n standard. The numbers are taken from a member of a 802.11n task group [10]. We can see that 802.11n has a theoretical transmission rate of 600 Mbit/s using channel bonding (40 MHz bandwidth) and 4 simultaneous data streams. Wireless devices that could accomplish these data rates do not exist so far. The majority of 2.0-certified devices support 2 spatial streams. This gives us a maximum transmission rate of 130/144 Mbit/s for 20 MHz single channel and 270/300 Mbit/s for 40 MHz channel bonding [10]. As we already know from section 2.2.1 the MAC throughput of a standard is much lower than the transmission rate. We were not able to get the official 802.11n specification from IEEE. For this reason it was not possible to do an accurate calculation. Instead of that we refer to a review from InformationWeek [12] that did throughput experiments with first draft-2.0-certified devices. Table 5 shows the throughput of three draft-2.0 wireless router in a real world enviroment:

	Apple's Airport Extreme Base Station	**Buffalo Wireless-N Nfiniti WZR2-G300N**	**D-Link Xtreme N Gigabit Router**
maximum data rate	*300 Mbit/s*	*270 Mbit/s*	*300 Mbit/s*
throughput 10 feet	98 Mbit/s	148 Mbit/s	120 Mbit/s
throughput 50 feet	75 Mbit/s	137 Mbit/s	95 Mbit/s
throughput 200 feet	35 Mbit/s	78 Mbit/s	35 Mbit/s
mixed mode 10 feet	14 Mbit/s	65 Mbit/s	77 Mbit/s

Table 5: throughput of 3 draft-2.0 routers measured with Ixia's IxChariot software [12]

We can see that all of those routers are far away from the maximum data rate for which they were specified. On average the bandwidth efficiency seems to be much lower than 50%. Nonetheless, although the efficiency is lower, new devices based on draft-2.0 perform much better than 802.11g devices.

The real question is how the new 802.11n devices would perform in an environment where data has to be transferred across multiple nodes. Since we have no final specification of the standard, we cannot provide a throughput analysis. Nevertheless, based on the given data we may express assumptions regarding the actual throughput. Since the 802.11 standards are based on the Distributed Coordination Function with CSMA/CA, the similarities of type n and g of the PHY and MAC layers are large. 802.11n will suffer from the same problems as 802.11g. The factors that significantly reduce the multihop throughput of all 802.11 types are discussed in detail in section 2.2.4.

As shown in Table 5, today's 802.11n-270 throughput is many times higher than the throughput of any 802.11g devices. Devices with channel bonding and 2 out of 4 possible simultaneous streams achieve a throughput, which is five times higher than the throughput of 802.11g devices. We have to wait until 802.11n is completely standardized and capable of 4 simultaneous streams. It is quite possible that such 802.11n devices will have a 10 times higher throughput as today g-devices have. This advantage in speed will also be transferable to the performance of devices in a multihop environment.

2.2.3 The 802.11s Standard

A wireless Mesh network consists of several wireless devices that are able to communicate directly with each other (in a peer-to-peer approach) instead of communicating via base stations. Wireless mesh networks have the characteristic that the communication between nodes is carried out over multiple hops. The 802.11s standard allows a transparent extension of the network coverage without the need to attach the Access Points by wires. Mesh networking demands efficient routing algorithms which can find paths through the network and react to changes in the topology. The 802.11s technology additionally solves some problems regarding routing, congestion control and other MAC layer problems that will be described later in 2.2.4. This is done by introducing a new mandatory Hybrid Wireless Mesh Protocol (HWMP) that is able to handle such problems.

A mesh network consists of Mesh Points (MP). A Mesh Point is an IEEE 802.11 station that is capable of the 802.11s mesh routing protocol and is able to forward the networks traffic. The major difference between mesh networks and IEEE 802.11a/b/g/n standards is the MAC layer. IEEE 802.11s only defines changes to MAC layer where a mandatory mesh routing protocol is realized. HWMP is the default routing protocol that provides both on-demand routing for mobile topologies and proactive routing for mainly fixed networks. Other protocols can also be integrated by vendors of wireless devices. Changes to PHY layer are not required in 802.11s. Changes of routing and frame format details can be found in [13]. The MAC frame format was extended with a control field that is adjusted for mesh requirements. The new frame format is helpful for mesh management because it forwards control messages for path selection and routing.

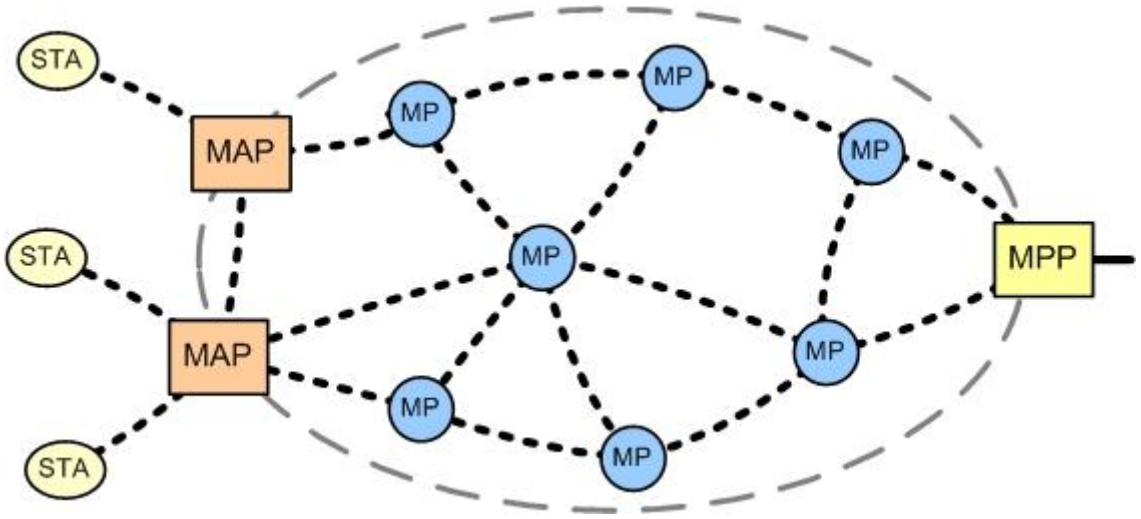

Figure 7: mesh network

Figure 7 shows a mesh network consisting of several mesh points (MP) and Mesh Access Points (MAP). Mesh Access Points are ordinary mesh points that have additional access point functionality. Other non-mesh IEEE 802.11 stations can connect to these MAPs. A Mesh Portal (MPP) is a mesh point that provides a connection to a wired network.

A throughput calculation over mesh networks, where data is routed from source to destination over multiple wireless nodes, is immensely more complex than single-hop networking. Spatial reuse for increased capacity, coverage enhancement or load balancing through route diversity – these are only some factors that influence the network and the throughput. The right choice of a routing algorithm for a specific scenario has another impact on the efficiency of the network.

It is arguable if a throughput calculation for a chain of several devices in one established path makes sense for 802.11s. Mesh Networking was developed to provide wireless connectivity over large areas without the use of infrastructure. A throughput calculation of several communicating nodes in a path will be done in 2.2.4 for 802.11g. We also found out that higher transmission speeds are possible with 802.11n. The serious question is how a mesh network of n randomly located nodes would perform inside a closed area where all nodes have data to send. And how do things change if our network has the ability to share the available spectrum among the users? The original 802.11 DCF does not offer the ability of concurrent network transmissions. However, there is an alternative MAC protocol, which allows distributed and concurrent transmissions. The Mesh Network Alliance protocol (MNA) represents a distributed, reservation-based approach that is described more detailed in [14].

In the following example we examine a mesh network consisting of relay nodes that cover a given area and provide wireless connectivity. Each node can forward the traffic of other nodes. The limiting factors in this example are interferences of other transmissions of the network and the resulting packet collisions. It is a matter of using the scarce resources of the wireless channel as efficiently as possible. The MAC MNA coordination function for 802.11s is able to announce upcoming transfers with the help of beacon frames. A station can reserve the wireless medium for exclusive access for a certain period of time. Other stations detain during this period. While sending, a station can rely on a collision free access to the medium and carry out its transmission undisturbed.

In [14] such an analysis was carried to find out the theoretical potential of the spectrum sharing with the presented MNA MAC protocol. Several scenarios were considered to identify the maximum achievable throughput precisely. The calculations were based on an

optimal scheduling of transmissions where no collisions could occur. The researchers wanted to find out how big the benefits of an intelligent spectrum sharing could be.

The results of the simulation show a significant increase of the throughput for the use of simultaneous parallel transfers compared to a single multihop transfer using the standard 802.11 DCF. The MNA proposal also solves the hidden node problem by reserving the entire medium between sender and recipient, which is a reason for the improvement. Through intelligent spatial reuse an overall throughput increase of 80% was achieved. While the 802.11 DCF was not able to benefit from spatial reuse, the presented intelligent MNA MAC protocol was able to almost double the throughput. Overall, it has turned out that in environments with unknown topology the throughput heavily depends on the underlying MAC protocol.

2.2.4 Effects of Topology

In this section we want to show how a wireless data transmission can be carried out over multiple devices that are organized as a chain of nodes. Nodes in the middle of the path will have to forward the traffic of all preceding devices. Furthermore, we will identify the factors that reduce the throughput of 802.11 in a multihop transmission.

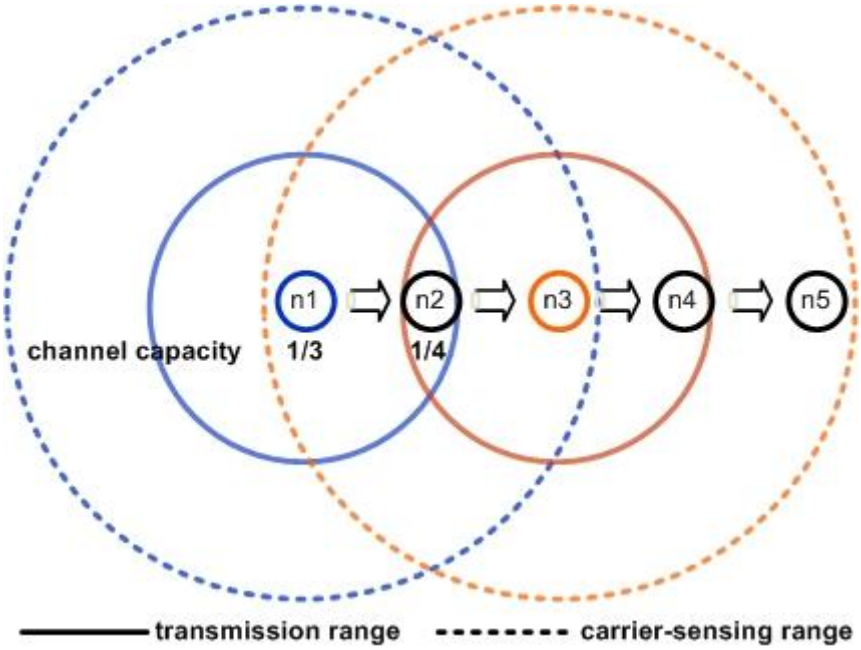

Figure 8: channel capacity at nodes 1-5

Figure 8 shows a typical situation that can occur in a multihop scenario. Data has to be transferred from node 1 to node 5 over four hops. Sender and receiver are so far apart that they can not sense each other. The following ranges have to be distinguished: transmission range and sensing range. The transmission range is presented by the continuous line in Figure 8. The discontinuous line represents the carrier-sensing range that is more than twice as big as the transmission radius. In this scenario we have numerous factors that have an impact on the maximum throughput. The following three problems were identified in a throughput analysis [6]:

1) A high packet-drop rate
2) A re-routing instability
3) A hidden node problem

The high packet-drop rate that is caused by the fact that neighboring nodes must share their channel capacity. Because the carrier-sensing range (550m) is much greater than the transmission range (250m) every node can sense transmissions of all nodes within the 550m radius. It can be seen in Figure 8 that node 1 has to share the medium with node 2 and 3. Because of this the throughput of the first hop at node 1 is limited to 1/3 of the total capacity. Node 2 has to share its channel capacity with three other nodes, the foregoing node 1 and the two successice nodes 3 and 4. From this it follows that the throughput at node 2 cannot go beyond ¼ of the total capacity. The packets are dropped at node 2 and 3 because the first nodes in the chain forward more traffic than later nodes can process. Till now the theoretical throughput of an optimal chain could be ¼ of the total capacity.

The re-routing instability that is caused by nodes in the middle of the chain which report the path as being broken decreases the throughput. This happens because first nodes of a path send more packets than later nodes can process. The result is a high contention at these later nodes and after several retries the packet transmission fails. In that case the routing agent is supposed to search for a new route. Till it rediscovers the same route again no packet can be sent. So the throughput drops because of a greedy sender at the beginning of the chain.

The hidden node problem appears for example when node 4 in Figure 6 is transmitting data to node 5. Because node 1 cannot sense this transmission it could attempt to initiate a transmission to node 2 with a RTS packet. This causes a collision because node 2 is aware of the transmission from 4 to 5 and will drop every packet from node 1. While node 4 is transmitting, node 1 will back off and increase its backoff window exponentially. When the medium is free again, node 1 could still remain backed off. The percent of time nodes spend in wasted backoff has another negative influence on the throughput [7].

In summary, we would like to stress that the upper bound of an ideal ad-hoc chain is ¼ of the throughput that a single-hop transmission could achieve under optimal circumstances. Because of the described re-routing instability that is a result of a greedy sender, and the hidden node problem, simulations show that only 1/7 of a single-hop throughput can be achieved in a 6 node chain [7]. Simulations in [6] not only show similar results, but also point out possibilities for improvement. Controlling offered load at the first node of the chain can prevent the instability problem. A constant throughput can be achieved at a particular offered load. Another strategy called “don’t-break-before-you-can-make” continues to use the old route when the route is congested and appears to have failed. Such modifications in the receiver design could make improvements of 50% of the throughput possible, according to [6].

On the other hand disadvantageous scenarios can reduce the throughput drastically if a multi-hop network has multiple hidden nodes. In other words: if there is a link in the network that suffers from 5 hidden nodes, the throughput will reduce by 40% compared to a linear flow [6].

As a conclusion it can be said that the achievable throughput of 802.11 in a multihop network consisting of 6 nodes is within a range of ¼ and 1/7 of a standard’s maximum throughput. In numbers: the transmission rate at MAC layer is in between 5 and 10 Mbit/s. An interesting point is that the throughput does not decrease much more if we add more nodes to the chain. As long as the distance between nodes remains the same and hidden nodes are avoided, the transmission speed remains stable also in longer chains.

2.3 Bluetooth

Bluetooth operates in the unlicensed 2.4 GHz band. Bluetooth radio employs a fast (1600 hops/s) Frequency Hopping-CDMA technique and offers a set of 79 1-MHz carriers. The hopping sequence is carried out pseudorandom. Each device has a unique address. Bluetooth is a connection-oriented technology that requires presetting of communication channels between two devices. The initiating master device starts a piconet and invites other devices (slaves). When the described Inquiry and Paging Process is done, the master can contact every desired neighbor. After the setup of the physical channel, the control is moved from the Baseband (the PHY layer of Bluetooth) to the Link Manager Protocol (LMP). The Logical Link Control and Adaptation Protocol (L2CAP) and its above layers can now start transmitting data. Time multiplexing allows one device can participate in two or more overlaying piconets (different piconets use different FH-CDMA channels). Devices that participate in multiple piconets serve as bridges and allow intercommunication between different piconets [11].

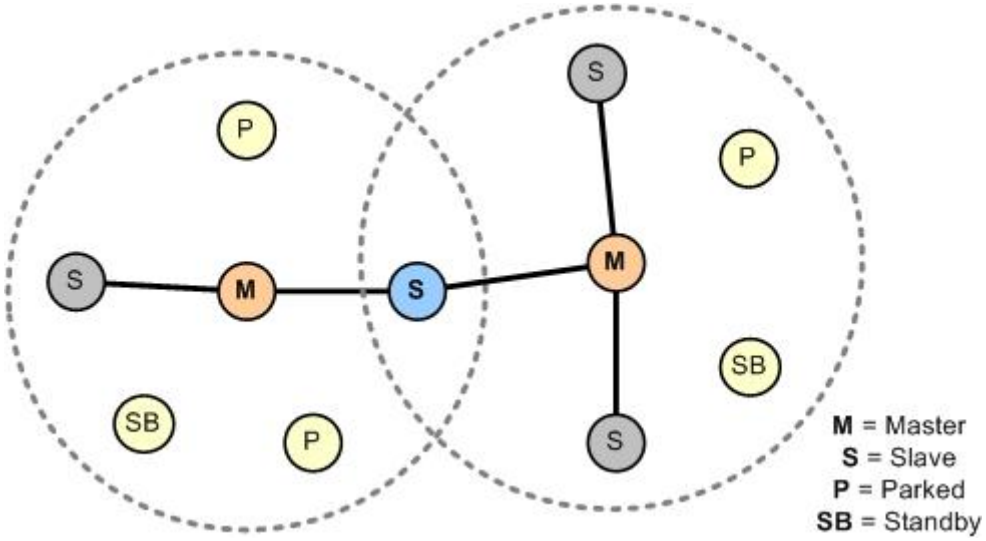

Figure 9: Scatternet with Master and Slave devices

In Figure 9 we can see two piconets with one overlapping Slave device that is jumping between both piconets (bridge). This structure is called scatternet. Furthermore devices can be parked or in standby mode to save energy. Each piconet can have one master and up to 7 slaves, about 200 devices could be parked.

A lot of research had been done in the area of ad-hoc routing protocols for Bluetooth in the last few years. However, the transmission rate of Bluetooth turned out to be too low for serious applications; also its low transmission range was widely criticized. But Bluetooth offers a lot of advantages: it has powerful ad-hoc properties, it suffers less from interferences in multihop mode as 802.11, and as it has no hidden node problem. Furthermore neighboring Piconets use different FH-CDMA channels, which in turn is the reason for Bluetooth's reduced vulnerability to interferences. A lot of routing algorithms were developed for this standard, which support mesh-like structures and achieve higher data rates compared to the standard ad hoc protocols of Bluetooth.

2.3.1 Bluetooth 1.x and 2.x

Bluetooth 1.0 and 1.2 supports a data rate of 1 Mbit/s. Bluetooth 2.0 and 2.1 specified in 2004 support data rates of about 2 Mbit/s and bring in some other enhancements. Bluetooth 2.x with EDR (Enhanced Data Rate) supports 3 Mbit/s. Both versions operate in the same way described in paragraph 2.3.

The following paragraph describes how a route over several hops in a multihop scenario is formed up. At the initial network startup stage all devices get interconnected, a big scatternet consisting of several piconets is formed. The connectivity of the network is maintained at data link level. Once the network is established, all Bluetooth links are maintained all the time even if no traffic is present. The formation of a scatternet route is initiated by a device that wants to contact another device in the network. The establishment of such a route is quite complex and can take several seconds. The routing and formation algorithms are not part of this work and can be looked up in [11].

Figure 10: scatternet route [11]

At this point, we assume that the path from sender to recipient has been formed like shown in Figure 9. Of course, our path only contains devices along the traffic path and all other devices connected to Master nodes have to stay in another power state (P, SB). As shown in Figure 10, a scatternet route consists alternately of Master and Slave devices. The Master devices form Piconets, while Slave devices serve as bridges between Piconets. There is another more robust scatternet structure called double role structure, where all devices have a double role of master and slave. Because the single role structure (like shown in Figure 10) is easier to analyze and has a higher throughput, we will only examine this structure.

For the calculation, we assume that a path from source to destination has been established, a single role structure is used and no synchronization overhead exists. Then the theoretical throughput is defined as

$$\frac{n * p_{size}}{2 * n * m * \ time_{frame}}$$

where n is the amount of packets to send, the transmission of one packet with the size of p_{size} costs m time frames and each frame has the length of $time_{frame}$. A Bluetooth time frame lasts 625µs. In this scenario only the packet size has an impact on the throughput. Table 6 shows throughput and network utilization for different packet sizes using Bluetooth 1.x with a maximum data rate of 1 Mbit/s for a scatternet route.

Packet Type	Packet Length	Bluetooth Slots	n	Throughput	Network Utilization
DH1	27 Bytes	1	1	86,4 Kbit/s	8,64 %
DH1	27 Bytes	1	3	86,4 Kbit/s	8,64 %
DH1	27 Bytes	1	5	86,4 Kbit/s	8,64 %
DH3	183 Bytes	3	1	292,8 Kbit/s	29,28 %
DH5	339 Bytes	5	1	361,6 Kbit/s	36,16 %

Table 6: Scatternet route throughput of different packet types [11]

As shown in Table 4, the throughput does not increase while sending multiple packets through the route at a time. Larger Bluetooth packets like DH3 and DH5, however, represent a real improvement: they raise the network utilization in a multihop ad-hoc network to 36,16%. This amazing network utilization was not possible with 802.11 networks. The reasons for this are that Bluetooth is a contention free technology with a multichannel MAC mechanism. Moreover, it does not suffer from the hidden node problem and its routes remain stable during transmission. While the throughput of 802.11 ad hoc networks quickly drops if the path length is extended, the throughput of a scatternet route remains almost constant. The throughput is independent from the route length. To sum up, the network utilization of an established multihop path can reach up to 50% if every other piconet uses a different channel and piconets do not interfere each other's transmissions.

2.3.1 Bluetooth 3.0

Bluetooth 3.0 is a new standard currently in development by the Bluetooth Special Interest Group and the WiMedia Alliance. It will use the ultra wide band (UWB) technology and will operate in the 6-9 GHz range. The multiband orthogonal frequency division multiplexing (MB-OFDM) modulation was chosen for integration with the new Bluetooth technology. By using UWB it will be possible to offer multiple carriers that are 100 MHz or even wider. Thereby data transfers of up to 480 Mbit/s become possible. New Bluetooth 3.0 devices will also include a 2.4 GHz radio that allows backwards compatibility with older devices. This next version of Bluetooth will keep the core attributes of Bluetooth (low power, low cost, ad-hoc networking). Key functionalities of Bluetooth 3.0 are following. A revised Topology Management enables the automatic arrangement of piconet topologies (especially in scatternet situations). Modified MAC and PHY structures enable the use of alternative transport of Bluetooth profile data. The previous Bluetooth radio will still be used for device discovery and communication setup. As soon as a lot of data needs to be sent, the high speed MAC and PHY structures will be used to transmit the data. Thus, the low power connection mode is used while the network is in standby, and the UWB radio is used when a lot of data needs to be sent. Finally, QoS improvements will enable audio and video data to be transmitted at a higher quality.

Because no specifications of Bluetooth 3.0 are final, a calculation is not possible. As we have seen Bluetooth 1.x already achieves very high network utilization, especially in ad-hoc mode. We expect that Bluetooth 3.0 will keep all its advantages and make an efficient communication in a multihop environment possible.

3. Real life scenarios for Ad-hoc networking

This section of the thesis deals with real life scenarios in which the possible uses could be increased through an ad hoc network. We will present a list of possible and desirable examples that would enhance with ad-hoc networking. Today there are various data-rate-intensive applications that are dependent on broadband and reliable networks. Concrete examples for this kind of applications that would benefit from ad hoc networking are: multimedia conferencing, video streaming, network storage, file transfer, transmission of HDTV signals, transmissions of multiple audio signals and online gaming. A large number of new and interesting applications is in development. The aim of this part is to identify a multitude of possible applications that would profit from ad hoc networking.

3.1 Internet access

Ad Hoc networks can also be used to provide internet connection to areas without infrastructure using wireless adapters that are able to form a mesh network. The purpose of the deployment of a broadband wireless mesh networks is not only to provide internet access as a commodity but also an economic and cost-effective way of interconnection.

Many internet service providers are looking for solutions to realize public internet access that can focus on the market of residential or business purpose. To provide wireless broadband internet access, more and more internet service providers are already installing solutions based on Wi-Fi technologies. Wireless mesh networks could be the perfect solution to offer indoor and outdoor wireless connection to access the internet. This can be realized not only for urban environments but also for rural environments. Especially the installation of internet access in a rural environment could save the cost of an expensive wired network infrastructure. For instance, a more or less populated area can be covered with several hundred outdoor access points that are organized as a mesh network. Only a small amount of those APs needs to be connected by wires to the internet. The installation of such a network can be carried out easily and cost effectively. Particularly for rural areas or regions that are hardly populated this is probably the best solution.

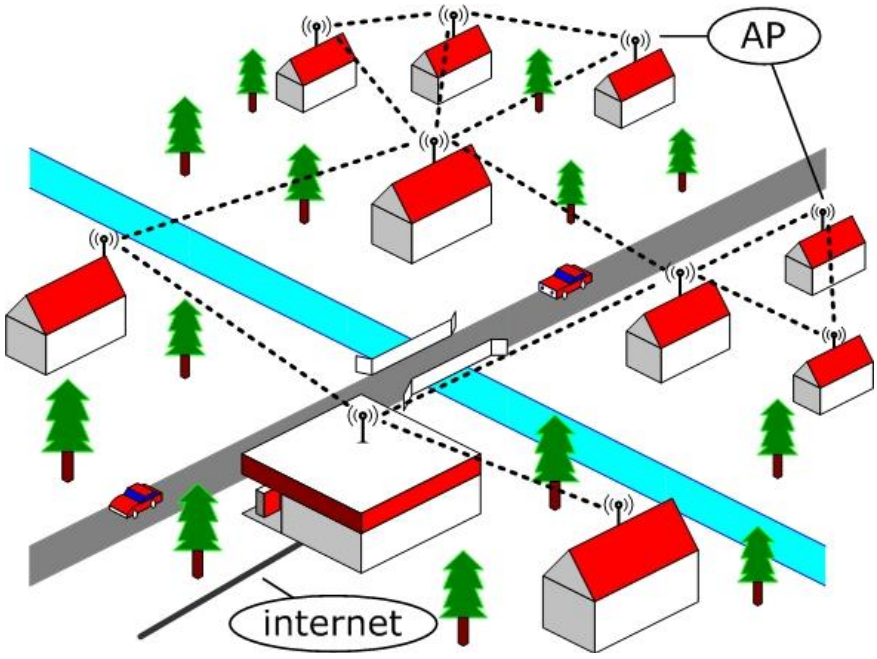

Figure 11: residential broadband internet access in hardly populated area [15]

Figure 11 shows a rural countryside with woods and rivers. To connect every household with a wired internet connection could be very costly. An easier way is just to wire only a few buildings and provide the connection via a net of Access Points that form a mesh network.

Another desirable scenario in which mesh networks would expand the usability is the establishment of internet connectivity for the population in less developed countries. Those countries do not possess the infrastructure that is needed to have internet access and the installation of such an infrastructure is not affordable. This is where the One Laptop Per Child (OLPC) project could come into play. The OLPC project intents the deployment of so called XO-Laptops to third world countries. The XO-Laptop is a mobile and robust computer specially designed for the needs of children and for the use in schools. Every XO-Laptop is also a wireless router that enables the establishment of wireless LANs without the need of additional hardware. To guarantee the forwarding of other device's traffic the network adapter of the XO-Laptop is still in operation even if the laptop is switched off. So every laptop is also a permanent wireless router always available for the network. To forward traffic over multiple hops the XO-Laptop uses the 802.11s protocol. In a sparsely populated environment a network adapter of a XO-Laptop is supposed to achieve an operating distance of 1,6 km above ground under optimal conditions [22]. All laptops that are in the same coverage area will interconnect with each other using the mesh protocol. A manual configuration of the mesh is not necessary.

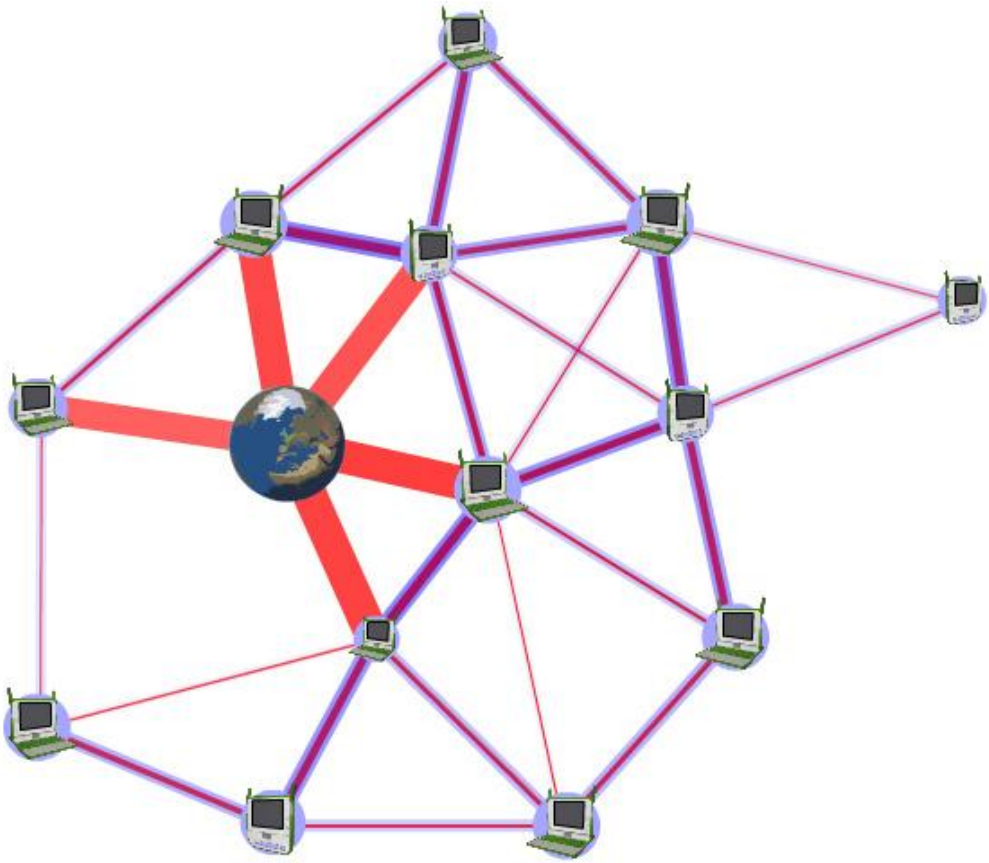

Figure 12: a mesh network formed by XO-Laptops [16]

Figure 12 shows a configuration of several XO-Laptops organized in a mesh structure. The thickness of the connecting lines represents the strength of a wireless connection. Because the laptops do not have a hard drive, all information is stored on a school server. The school server, represented by the globe in the middle of the picture, is also the gateway to the internet.

To sum up, in a scenario where a limited amount of people wants to share information and access the internet, the formation of a mesh-like network is profitable. A mesh network for internet access is at the same time a multipurpose networking platform. Because the network is made of user devices, no additional infrastructure is needed. All devices are routers and user terminals at the same time. The use of mesh networking how we showed in the previous two examples is a flexible and low-cost extension of a wired infrastructure. Where cost plays a role, the deployment of internet access to an area without infrastructure can be carried out more advantageous with mesh structures. Even a coexistence with wired networks is possible and favorable.

The presented scenarios have following advantages: first, the installation costs can be reduced. Cabling infrastructure can be avoided, only a few points of the network need to be connected to the internet. Secondly, because a mesh structure provides multiple paths from source to destination, the reliability increases in case of failures of single points. This makes the network also more robust against interferences. In addition network capacity adds with every user added. Finally, a mesh network offers the ability of self-management and self-configuration. If new nodes are added to the network, these nodes can discover optimal paths to a destination. This makes the network transparent to users and easy to expand.

3.2 Mobile Ad Hoc Networks

A Mobile Ad Hoc Network, also called MANET, is a collection of mobile interconnected nodes. In a MANET, the network topology can change unpredictably during data transmissions. Every node in this kind of a network is responsible for discovering new routes and for delivering messages.

There are lots of applications for MANETs that range from small and static low power networks to large and mobile communication systems. In this thesis we are interested in large-scale and dynamic examples of use of mobile ad hoc networks. MANETs are often used in Wireless Sensor Networks. These wireless networks consist of distributed autonomous nodes using sensors to monitor environmental conditions, such as temperature, sound or motion at different places. Sensor Networks are not part of this thesis.

The design of MANETs is more complex than the design of static ad hoc networks. MANETs need more efficient and distributed algorithms for link scheduling and routing. The biggest problem is the determination of usable paths in a decentralized environment where the topology can change every minute. Factors such as inconsistent link quality, fading, interference and topological changes make it hard to determine the shortest path from source to destination. The network should have the ability to alter the routing paths in a flexible way. Furthermore it is important to maintain latency, security and reliability in an emergency or public safety network. A defect in one of these requirements could reduce the system stability of the network.

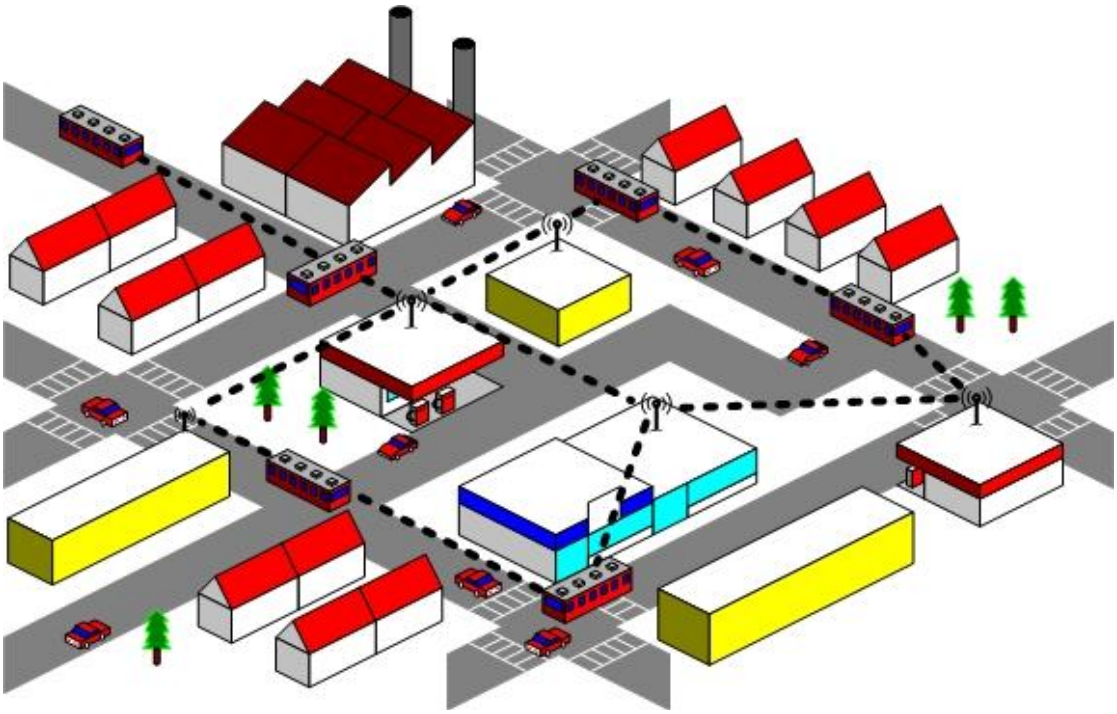

Figure 13: intelligent public transportation system

Mobile ad hoc networks can be used for intelligent transportation systems. This concept refers to systems that add information and communications technology to transport infrastructure and vehicles. The aim of these systems is to manage factors like shipment, routes, improve safety, reduce transportation times and fuel consumption. Intelligent transportation systems differ in technologies, they vary from basic management systems like car navigation, traffic signal control, container management systems, variable message signs, and license plate recognition to more complex applications that contain live data and feedback from other sources. Examples of more advanced scenarios are parking guidance systems, information systems of any kind, weather information and so on.

We can exemplify the advantage of an intelligent transportation system on a city wide real time travel information system in buses shown in Figure 13. A multitude of public transportation buses can be equipped with the system named above. The system is a city wide communication network based on mesh technology. Its purpose is to offer real time travel information for the passengers of the busses. It allows displaying real time information all over the city. Information like the location of the bus, its destination and an up-to-date time schedule can be displayed. The system is also designed to reduce congestion problems, control pollution and improve safety and security [15].

Cars can also create an ad hoc network in the future. They could broadcast general traffic information and traffic jam warnings or accident warnings on highways. Vehicles could operate as a mobile ad hoc network in which a single vehicle could detect traffic events and initiate a broadcast to other vehicles. To solve the routing problem, all vehicles must support location management, for example by using GPS. A further ambition is to provide universal internet access to trains or cars. Vehicles can as well route internet data traffic using an ad hoc approach. But even if vehicles on a highway or high-speed trains can route and forward their traffic, a wired connection is still mandatory. As a solution internet access points could be placed at regular intervals near the road or railroad line, for example every kilometer. This would have the advantage that car accidents would not only become noticed within a small radius of the surrounding cars, they would get immediately noticed by the

whole network. A possibility would be provided to broadcast accident warnings on the radio shortly after they happened.

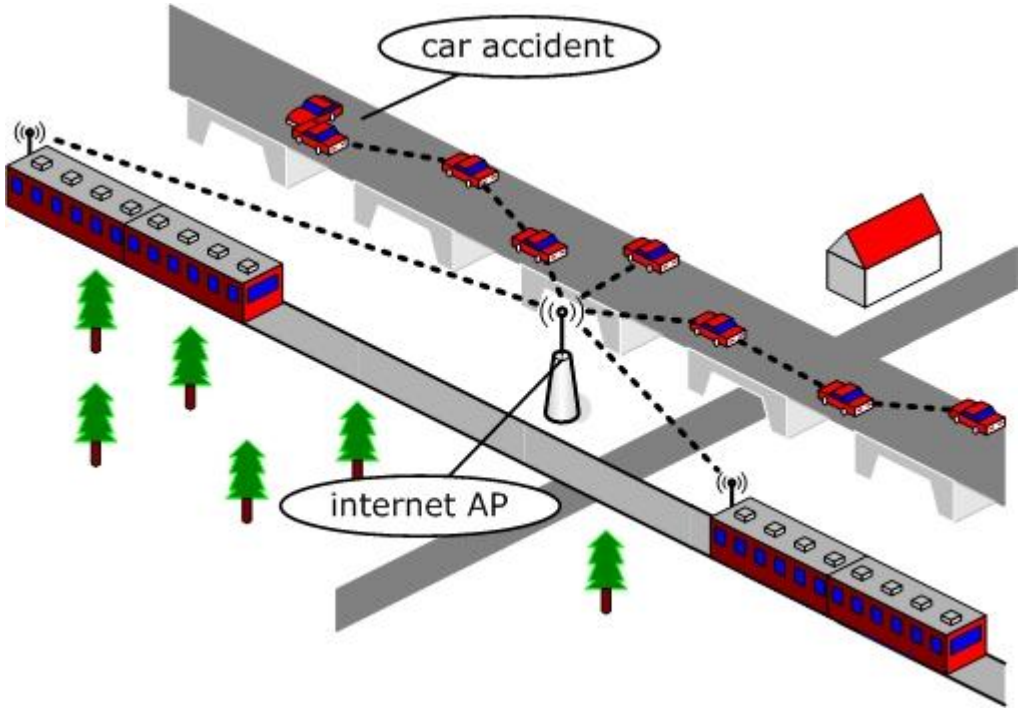

Figure 14: cars and trains create a mobile ad hoc network and detect traffic events

Figure 14 demonstrate the possibility to create a traffic information and warning system combined with the scenario to access the internet from fast moving vehicles. A car involved in an accident broadcasts a warning to other approaching cars. Internet access is realized by fixed access points near the highway. Vehicles that are out of the access point's range can still access the internet. This can be via a multihop transmission between several cars.

A mobile ad hoc network can also serve for public safety issues. They can be implemented to enhance the work of police, fire departments and emergency services. The demand for this kind of services combined with a high bandwidth network is increasing. This type of services requires high mobility, flexibility and reliability. So far this problem was solved with cellular technologies that now become unsatisfactory. Cellular technologies are extremely mobile but have a very limited bandwidth. Following mobile ad hoc security scenario is possible and could improve security in cities: A district or even a whole city can be covered with mesh points that are equally distributed. The mesh points form a mesh network and cover the entire region. A police department would have to equip its cars with laptops that possess a wireless link. Every police car and even every police officer can now connect to a central database and receive or send data.

In disaster areas or resque operations it is very useful to be able to arrange a wireless ad hoc network without being dependent on a fixed infrastructure. In a disaster recovery scenario firefighters or emergency aid staff could carry little cameras and transceivers. This would allow to send the emergency scene back to a command center. A supervisor could keep track of his men's positions and direct the operation.

3.3 Audio and Video Streaming

Streaming of audio and video is a procedure where media is constantly received and displayed to the end user while it is being transmitted over a network. The challenges of video and audio streaming in a ad hoc environment are low latency, congestion limited networks and overall video and audio quality.

In the following streaming scenarios the nodes are rather not in motion, so a constant search for new paths like in MANET scenarios is normally unnecessary. However, video streaming is a time-critical multimedia application with high data rates. It requires strict bandwidth and delay guarantees. While accessing the internet the necessary time to load a web content is not important, while watching a video a congested path would cause breaks in the audio signal and video framedrops. The streaming of video data is dependent on a low latency, especially in the case of live conferencing where two or more people are in a conversation. Live conferencing is a real-time scenario where problems like packet loss or interference could interrupt and fail the whole conversation. But video streaming can also be useful as a client-server application, for instance the reception of a video stream from a server is a one-way link. Because we want to achieve the best possible video quality while using a video service, the streaming of video data is bandwidth constrained in this situation. In this example a buffer could solve the problems of breaks while the path is temporary congested. However, a buffer cannot solve the problem of insufficient bandwidth. The situation gets more complex if we want to stream video in an enviroment where nodes are moving. If there is no fixed topology, links get constantly broken and new links get established. In the following part of this chapter we will take a look at various possible scenarois for video streaming.

The first scenario is a wireless home network. In future, it is possible that every household will have a network of typical mutlimedia devices like video displays, TVs, speakers, cameras, microphones, storage devices etc. All these devices we already have today, but they are not interconnected in a high degree. The signal of a sat-receiver on the roof of the building could be received from every transceiver and could also be forwarded to other nodes futher away. At the same time it would be possible to listen to music that is being transmitted from the server-like storage device in the basement of the building. And this could happen from every room of the house over several hops. Figure 15 shows such a scenario where many server-client applications are taking place at the same time. Each audio or video stream occupies large capacities of the channel for several hours. We can see that our example contains a high density of sending and receiving nodes. The major problem is, how to achieve the maximum efficiency while using multiple real-time video and audio transmissions simultaneously [17].

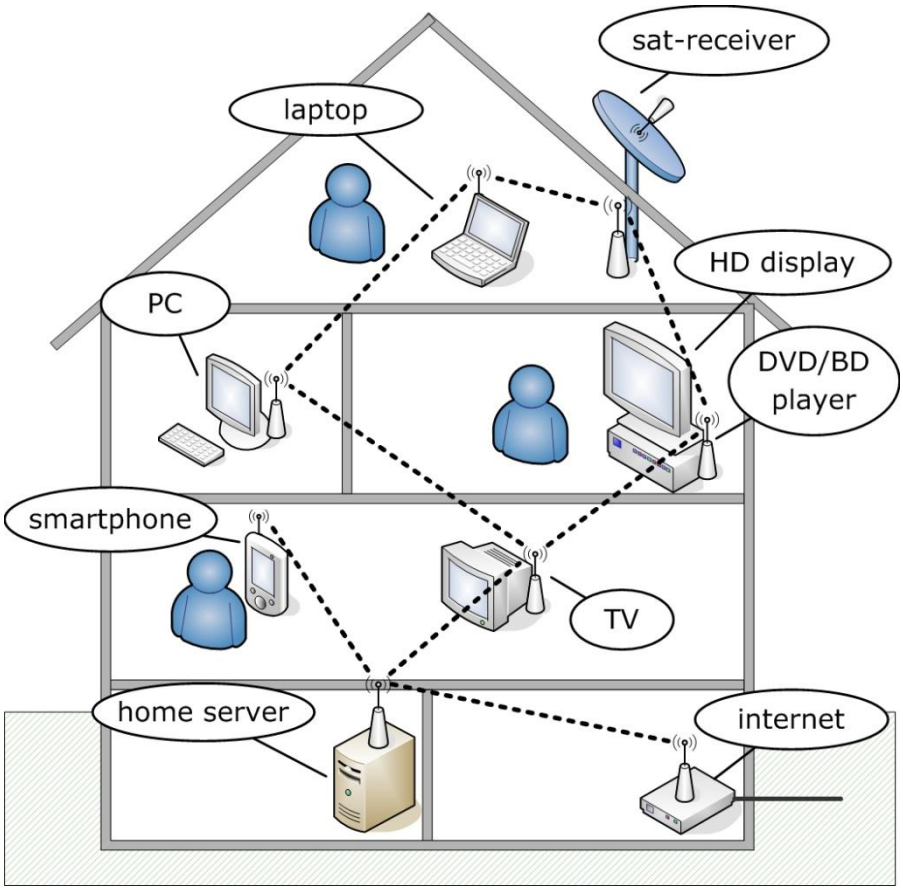

Figure 15: wireless home network consisting of input, output and storage devices

Every node in our wireless home network scenario shown above has routing functions. No coordinating or central device is needed. The network must be self organizing and act like a mesh network, every device has to be able to forward video and audio streams. We have to consider that the wireless home network should also be expandable. It must be possible to add new devices to the network and easily replace broken ones. This scenario is not limited to one household. It can be expanded without difficulty to a whole apartment building where residents can share one satellite receiver or video server by getting the signal wireless to their TVs. Apartments that are farther away from the sat-receiver can access the video stream over several hops. Every TV itself could have routing functions, or a special routing device connected to the TV could forward the traffic.

This scenario is also applicable to wireless video projectors for presentations or video playback. Projectors could receive the data from a computer or DVD player which is in another office of the same building. If the signal is not strong enough, the streamed data could be transferred by hopping over other computers that are located in between the sending device and the receiving projector.

Another interesting streaming scenario is video conferencing and surveillance. Today most security and video cameras are wired. Wireless cameras have two major advantages, first, the installation and cabling causes less problems and costs. Secondly, more cameras can be deployed because they can be easily installed and controlled. A camera network consisting of surveillance cameras monitoring places like public buildings, banks, stores, train stations etc. could work similarly to the mesh network for internet access in part 3.1 of this chapter. Only a few points of the network would have to be wired, the rest could stream the data wireless. The same scenario would as well work for video conferencing; the cameras would

be distributed in office buildings and meeting rooms. Several cameras could be deployed for a conference. Even one camera per participant is thinkable. This would improve the quality of a streamed video conference and allow multiple viewing angles.

The real-time surveillance of moving objects like trains or busses is a scenario that probably is most difficult to realize. To deploy a mobile ad hoc network of security cameras in a setting like we already introduced 3.2 (intelligent transportation system) is problematic because streaming of video signals is a time-critical application with a high data rate. To guarantee a minimal delay and a high bandwidth while all nodes are moving is an enormous challenge. All the time links would get broken and new paths would have to be found. It would have to be ensured that at a low density of nodes, the connection if individual nodes would not break.

3.4 Short Range Data Transfer

To interconnect computer peripherals like printers, scanners, digital cameras etc. without the problem to wire them is another attractive idea. In office buildings where we have a massive density of computer and peripheral devices, wiring difficulties could be reduced. Computers and other peripheral devices of an office building could once form a network where computers could send data over several hops to a printer. As well portable devices like laptops or PDAs need access to a great number of computer peripherals. This could be realized in the context of an ad hoc network for computer devices. The transmission range is not deciding in this case; a transmission range of only a few meters is completely sufficient to cover a conference room. To provide a highly flexible and robust wireless network for this kind of appliance would solve the increasing communication needs of all kind of electronic devices and reduce the cable management problem at the same time.

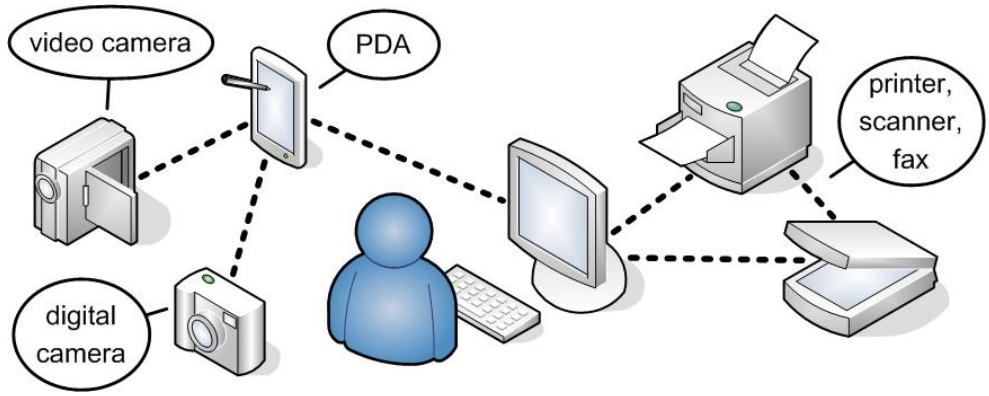

Figure 16: ad hoc communication of devices in an office environment

Figure 16 exemplifies such a scenario of devices that are dependent on a robust high-speed and short-range transmission system. This can be achieved by a wireless ad hoc connection between computers and peripheral equipment. Continuous connectivity, security and access restrictions would have to be ensured in this scenario.

A nice scenario is the support for multi-user ad hoc games. An ad hoc network technology would make it possible to play multiplayer games wirelessly with friends without the need of setting up a wired network. The ad hoc communication in this case is limited to indoor transmissions of a distance of only a few meters or one room, respectively. At home, at school or even in a subway station could be a place where young people meet and form

spontaneous groups. If there are mobile devices and specially specified games that would support ad hoc group formation, children and teenagers could spend time with multiplayer games. For example, they could compete in racing games where high scores would be displayed and every player would have a unique nick-name. The devices could search for target nodes that are out of range by flooding the network. Connections would be possible over multiple nodes. Efficient routing algorithms would have to provide a steady connection, even if some players were moving around. Multiplayer gaming is a time-critical application, to guarantee for a minimal delay is easier in this scenario because of the proximity.

Figure 17: established wireless link with mobile gaming devices

Figure 17 shows several small handheld devices like the Sony Play Station Portable or the Nintendo DS that are developed for gaming. These devices are connected wireless; a direct connection of two distant devices is not needed. Game data can be transmitted over multiple hops and new devices can easily join the game.

3.5 Home automation and other scenarios

Home automation specifies automation requirements of private homes for automating systems for the comfort and security of residents. Techniques of building automation are also included in the concept of home automation. These include applications such as light and climate control, control of doors and window shutters and security systems. Further applications of home automation can include the control of home entertainment systems or even automatic watering of plants. All of these applications have a user-friendly monitoring and user interface. Home automation usually requires control wires inside of interior walls. They are usually installed during the construction of a house. To equip a house with home automation later can become a complex and costly issue. This problem could be as well solved with a wireless ad hoc network. The provision of a secure wireless network for this kind of appliance would solve the communication needs of home automation and reduce the wiring problem at the same time.

Another scenario that can be categorized as a mobile sensor network is a system of cooperative mobile robots and vehicles for industrial applications. This scenario includes monitoring, tracking and controlling of objects like robots, machines and driverless transporters in factories, power plants and areas that are difficult or expensive to control with wired sensors. A wireless ad hoc network could provide the communication among these robots. Each node could exchange the information collected through its sensors and coordinate tasks with other nodes. Complex tasks could be scheduled in this way. A distributed group of mobile robots could autonomously monitor an area and transmit the data to a base station. If the transmission range of these robots is too short to communicate with a base station, the communication could take place in an ad hoc manner over multiple hops. Such a dynamic network has a lot of advantages. It is more robust to node failures, it is self-organizing and the deployment of base stations is not needed.

4. Challenges and recommendations

In Chapter 2 we have described several technologies that were developed for wireless transmission of data. We have identified some standards which are suitable for the transmission over short distances. We have found out that this is possible with Bluetooth in version 2 and 3. Transmissions over long distances can be implemented with 802.11. We have presented different variants of 802.11 and we have highlighted the differences regarding modulation techniques and data rate. In addition, an analysis of the maximum throughput of each standard has been performed. Finally, we have checked every standard for the suitability for multihop transmissions and in doing so we have observed diverse characteristics.

In Chapter 3, different scenarios for the use of ad hoc networks have been presented. We have discussed examples where internet access could be realized with the help of mesh networks in areas without infrastructure. Scenarios for mobile ad hoc networks have been presented, where a data exchange between mobile devices takes place. Likewise, we have identified applications that would benefit from a multihop video transmission, such as the wireless home network, in which video and audio signals are transferred wirelessly over multiple nodes. Already in Chapter 3 several scenarios turned out to be difficult to realize, for example the wireless surveillance of buses and trains, where a high bandwidth and a low delay is crucial.

Finally, in this chapter we analyze to which extent the technologies that we have discussed in Chapter 2 are suitable for the scenarios presented in Chapter 3. In this section we want to find out whether our scenarios, in which the use of ad hoc networks would bring a clear benefit, can be realized with the described technologies. In this Chapter we will try to give recommendations for the implementation of these scenarios. We will also demonstrate which difficulties and disadvantages an actual implementation entails. At last, we will find out the limits of ad hoc networks and we will show meaningful alternatives.

4.1 Recommendations for Audio and Video Streaming

The benefits of video streaming are undoubtedly enormous. Video streaming can function as a one-way link, for instance the reception of a video stream from a server, or in both directions, for example as it is done in live-conferencing. In Part 3.3 we got to know various useful ways to transfer audio and video signals over a wireless medium. At the centre of our considerations there were ad hoc capable applications. A complex example of a streaming scenario is the wireless home network, in which various devices such as satellite receivers and storage devices simultaneously transmit video and audio data to players and computers. This transfer takes place over several hops and occupies the medium for several hours. The problem that has to be addressed is to achieve a good efficiency of video transmissions.

First, we have to decide what kind of audio and video data we would like to transfer. An uncompressed video signal has such a high data volume that a wireless transmission is unrealistic. We can only achieve reasonable results with the transmission of compressed video. We should have a look at data volumes of video compression schemes. Video compression schemes vary in quality, computational costs and data volume. The following table presents an overview of possible video compression methods.

	compression standard	typical resolution	average bitrate
Online Video	MPEG-1	352 x 288	1150 Kbit/s
DVB-T	MPEG-2 MPEG-4	720 x 576 576 x 352 480 x 352	3 – 3,5 Mbit/s
DVD video	MPEG-2	720 x 576	4 - 5 Mbit/s
HD video (Blue-ray Disc)	MPEG-4 H.264 / VC-1	1280 x 720 1920 x 1080	20 - 40 Mbit/s
DivX video	MPEG-4	352 x 288 720 x 576	0,7 Mbit/s 4 Mbit/s
uncompressed digital video	DV (8-bit 4:2:2)	1280 x 720 1920 x 1080	42 Mbit/s 190 Mbit/s
Audio (dolby digital)	AC-3		32 - 448 Kbit/s

Table 7: compression standards of video and audio

Table 7 presents an overview of some common compression methods. The audio stream is already included in these video compression methods. We can see that different compression methods achieve diverse bitrates. Video encoded with MPEG-1 usually has a low resolution and a low image quality. The advantage of MPEG-1 is the low bitrate and the resulting small data volume. DVD and DVB-T video are encoded with MPEG-2 and use a standard definition of maximal 720 x 576 pixels. The average traffic volume of these standards does not rise beyond 5 Mbit/s. High Definition video is known for a sharp and clear image, what is due to a very high data rate. The DivX codec is quite interesting because it is known for its ability of high compression and low data volumes while maintaining a relatively good video quality. Video of 352 x 288 pixels encoded with DivX has a higher quality and smaller data volumes as video encoded with MPEG-1. The disadvantage of DivX video is a slightly higher computational cost. There is even a DivX Web-Player that demonstrates High Definition playback, streamed with an average bitrate of 4 Mbit/s, inside of a browser.

Let us now return to our main problem. We want to find out whether video transmissions can be carried out over multiple hops in one of the scenarios that we already presented. As we already know, a multihop environment decreases the maximum theoretical bandwidth of 802.11 standards by ¼ to 1/7. With 802.11g we were able to achieve a throughput of 5-10 Mbit/s. However, in real world situations we do not have optimal conditions. Absorptions and reflections at walls and other solid objects interfere with our signal. We have contention between stations to access the wireless medium. Under ad hoc conditions we will probably have a throughput of less than 5 Mbit/s.

This throughput seems barely sufficient for the transmission of DVD, DVB-T and DivX video in standard definition. In our scenario, the wireless home network, several stations are sending and receiving simultaneously over long periods of time. If all stations operated in the same frequency, they would have to share the wireless medium. Frequent collisions could result in connection losses. Moreover, the quality of a link can fluctuate due to moving objects or persons inside the house.

The applications of this scenario need a form of Quality of Service (QoS), which guarantees them a certain bandwidth and delay. Unfortunately connections in wireless ad hoc environments are based on best effort. Therefore no guarantee of bandwidth or delay can be given. Another problem is that compressed video is highly error-prone compared to uncompressed data. This means that bit errors that occur during the transmission can lead to synchronization problems, which finally results in image errors during the playback of the video. To increase efficiency, modern video compression techniques use methods such as

Motion Compensated Prediction, which makes frames depend on previously transmitted data. Consequently a packet loss does not only lead to an error within the frame, but also to errors of following frames. The traditional error correction techniques are not sufficient for transmissions of compressed video data. There are several approaches that could solve these problems. One solution is the Multipath Transport approach, which is discussed below.

The mesh topology allows establishing multiple paths between sender and receiver. The video signal can be split into several substreams. Each of these substreams is transmitted over one of these routes. Because the paths are independent of each other, errors in different substreams would also be independent. This path diversity would result in a higher fault tolerance of video transfers. At the same time, the transfer would be protected against a shutdown or a failure of intermediate nodes. A detailed analysis in [19] shows that a Multipath Transport (MPT) is accomplishable by simple modifications of common compression techniques as MPEG or H.264. In this scenario, the transfer is carried out on a Multipath Layer which is constantly monitored concerning QoS parameters. This architecture is able to set up multiple paths from sender to receiver, taking into account parameters like bandwidth, delay and packet loss probability.

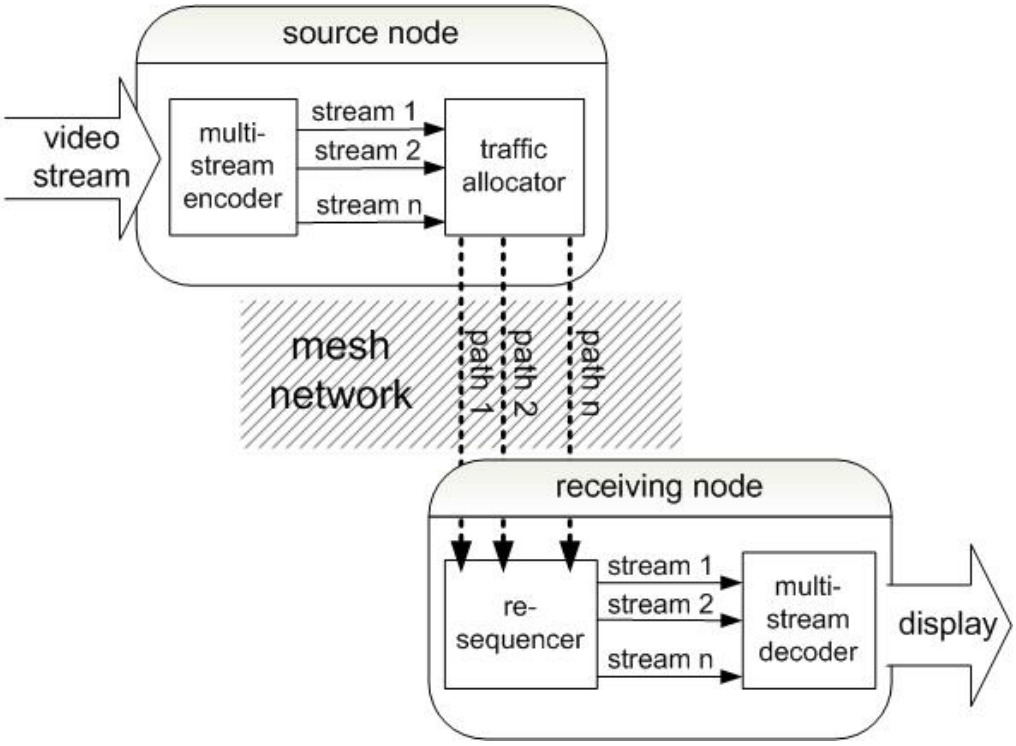

Figure 18: architecture of Multipath Transport and multi-stream coding [19]

Figure 18 demonstrates the principle of Multipath Transports. The source node contains a multistream encoder that splits the signal in n streams. These streams are sent from the traffic allocator on different paths through the mesh network. In the receiving node there is a resequencer that collects all n signals and passes them to a multistream decoder. The decoder will have to reconstruct the actual video from the substreams.

While designing the multi-stream encoder great importance should be attached to the fact that losses in one substream do not have a high influence on the decoding process of other substreams. It is imperative that this independence must not be achieved at the expense of the encoder efficiency. One possible solution is to design the encoder in a way that several equally important streams are being generated, each playable at acceptable image quality. The reproduction of the video in highest quality is only decodable from all substreams together.

Consequently, a reconstruction of the video in acceptable quality is possible, if only one stream is received. Because retransmissions are never necessary here, this method is particularly suited well for applications with strict delay requirements. At the same time, Multipath Transport has the advantage that no paths are being excessively used. This means that the network is evenly loaded and capacities for other applications still remain. Overall, the MPT approach features following advantages in ad hoc networks:

a) higher bandwidths are achieved compared with bandwidths of single links;
b) the decoding process remains independent from transmission errors and failures of single nodes of the network;
c) Load-balancing is achieved through path diversity.

The multistream coding principle results in an increase in robustness through path-diversity in multihop networks. Similar requirements can also be found in the scenario of the wireless home network, where multiple client-server applications take place at the same time that require large capacities. This home network has a high density of sending and receiving nodes, thus, the MPT makes full use of its potential here. Each application would only use a part of path capacities, and a congestion of the network would only lead to a reduction of video and audio quality. It would not result in an interruption of the data stream in this case. This approach also works with real-time video communication over lossy networks. Since low delay is essential in video conferencing, late packages are unusable. Only through redundancy it is possible to compensate dropouts and losses that occur during the transfer; this can be achieved while using packets from other streams. In earlier work [20], it has been shown that this method works well for multiple low-delay audio streams that are transferred over the Internet. To realize our wireless home network, the 802.11g standard would be sufficient to offer enough capacity for multiple simultaneous video and audio transmissions in standard definition. However, for the transmission of HD content, the bandwidth of the g-standard would not be sufficient.

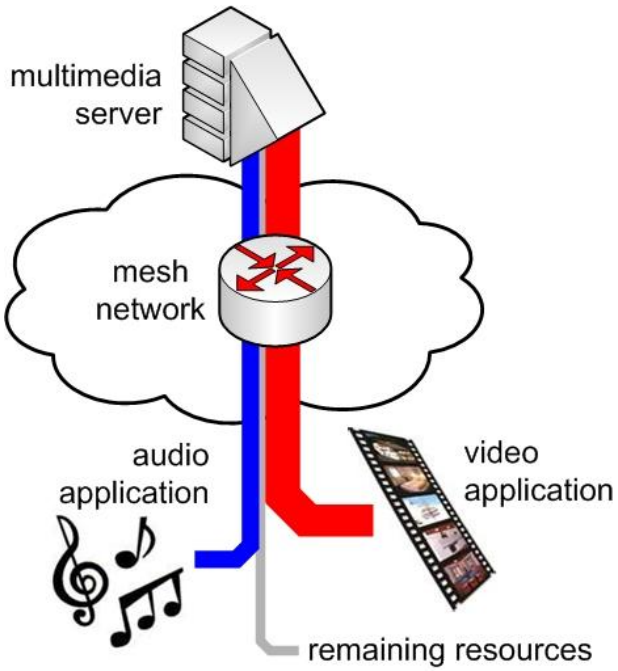

Figure 19: resource allocation technique in a wireless mesh network

Another possibility to ensure sufficient resources for video and audio transmissions in an ad hoc network is the use of protocols, which perform an allocation of the required resources. The concept of this solution is to ensure a reservation of resources at each node along the data path from source to destination. Every station has to be able to provide the requested resources. If a certain station cannot supply the required resources, the protocol must backtrack and find a different path to the destination. Only when a path is entirely reserved, a user can start sending data. It is also permitted to reserve multiple parallel paths for a higher fault tolerance. At the end of a session, the protocol releases all used resources, and makes them reusable for other sessions. Figure 19 shows how a split-up of the total bandwidth of a path in a network could look like. An audio and a video application share almost the entire bandwidth.

The approach of resource allocation techniques has the disadvantage that eventually all resources are occupied, and no further applications can be started. On the contrary, congestion would never occur and a definite quality of the transfer would be assured. For a scenario such as the wireless home network that only contains stationary nodes, this approach would also offer a satisfactory solution.

QoS can be achieved by over-provisioning, which is another easy way to provide service quality to ad hoc networks. This approach does not reserve or allocate resources; instead more bandwidth is added to the network than actually needed. This approach is only suitable for scenarios in which the topology of the network does not allow path diversity, or for scenarios in which a reservation of resources is not desired. In our example, the lack of service quality can be solved with the deployment of a faster standard. For example, 802.11n can meet all needs of our wireless home network in the same way as 802.11g can. 802.11n has, however, a much higher bandwidth, enabling transfers of video in standard definition to use only a fraction of the available bandwidth.

4.2 Delay-Tolerant Networks combined with Mobile Ad Hoc Networks

To deploy a mobile ad hoc network of surveillance cameras for trains, subways, busses etc. is a problematic issue. Streaming of video signals is a time-critical application that requires a high bandwidth. A key problem for video applications in MANETs comprises the support of QoS. To guarantee a low delay and high data rate while nodes are moving is probably not possible at present. In this ad hoc scenario paths get broken continuously, and new path via other nodes have to be found. A satisfactorily solution to this problem is not as easy as solving video streaming problems in multihop networks. There is, however, an approach that can solve this problem with minor restrictions. Delay-Tolerant Networks can bring a satisfactory solution.

Below, we describe the build-up of such a delay and disruption-tolerant network. The concept is an occasionally-connected network that can handle a frequent separation of its components. It can even consist of different protocols. This technology was developed in order to allow communication in high-delay environments. The Delay-Tolerant Network architecture can be used in various environments, especially environments that suffer from interference and disconnection and where a high-delay is unavoidable.

The reference [18] describes a Delay-Tolerant Network architecture that was designed to work in extreme environments that lack of continuous network connectivity. Messages of a variable-length that are called “bundles” are routed in a store and forward manner between nodes. This means that information that has to be transmitted can be stored at intermediate stations where it is kept and sent later to the destination. The transmission can take place over several intermediate nodes, where the data is cached over a short period of time. Because this specified “bundle layer” works above the Transport Layer, the transmissions can be carried

out over mixed network technologies (for example different types of 802.11). This procedure therefore can be easily combined with every ad-hoc compliant MAC/PHY layer, for example with 802.11s.

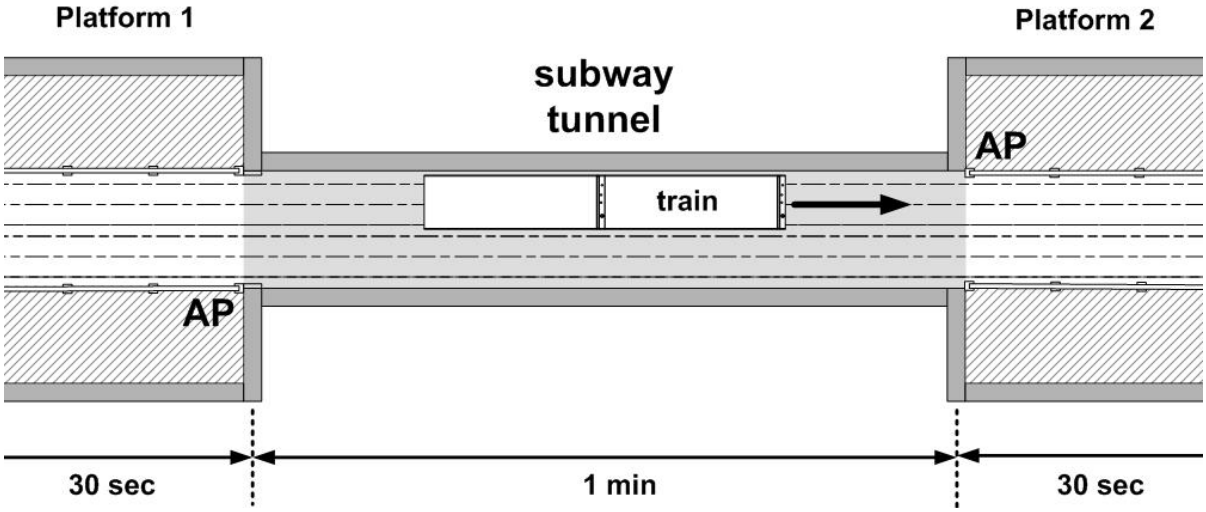

Figure 20: Delay-Tolerant Network for surveillance of subway trains

Figure 20 shows a possible realization of a video-monitoring system in subway systems. In each wagon of a subway train there is a surveillance camera which is constantly filming the inside of the car. The train contains a memory buffer that can cache several minutes of video. We assume that a train has an average travel time of 1 minute between two subway stations. During this time the video recording of the cameras is cached. Once the train reaches a station, it automatically connects to an access point. Each subway station has such an access point, where the video information can be transferred from the buffer.

The data transfer can be performed undisturbed with a high bandwidth at a train platform. During entering and exiting, there is a period of at least 30 seconds available. With cameras that encode the video using MPEG-1 and 1.5 Mbit/s, we would have a data volume of 11.25 MB at each camera. If we had 10 cameras on the train, 112 MB would have to be transferred within 30 seconds. To accomplish this, we need a bandwidth of 30 Mbit/s to the transfer the data within the available time. As we know from Chapter 2, this is manageable even with the 802.11g standard under good conditions.

The video data could be transferred to a control room. The only limitation of this procedure is a constant delay of 1 minute; this means that activities inside the train would be noticed after 1 minute by the security personnel in the control room. The data traffic could be reduced simply, as soon as we had cameras with automatic motion detection in the trains. Low occupied wagons would not be filmed. This could help to overcome a greater time between two stations.

A similar approach can be applied to Intelligent Transportation Systems that belong to the category of mobile ad hoc networks. These systems transmit information to vehicles that concern cargo, travel routes, traffic situation, weather data etc. The aim of these systems is to reduce transportation time and increase security. Live data such as position determination or information that is of tourist interest can also be transmitted.

At the Technical University in Braunschweig there is research in the area of this kind of networks. We will illustrate the advantage of Delay-Tolerant Networks on the example of the EMMA Project [23] that is currently carried out by the Institute of Operating Systems and Computer Networks in Braunschweig.

The aim of the EMMA Project is a decentralized and cost-effective architecture for the wide-scale recording of environmental values that are measured with the help of public transportation systems. Buses and trams are used as mobile measuring stations in this project. The recorded data is exchanged between the vehicles over 802.11 protocols. The difficulty lies in the fact that data has to be transferred between moving vehicles, as well as between stationary sources and moving objects. This problem can only be solved if we have a delay-tolerant network; vehicles may lose their connection and rebuild it at any time without data being lost. Vehicles can exchange data, as soon as they are in range. In this way, any information can penetrate the entire network. The disadvantage is that every transfer is being buffered and requires a certain amount of time, which means that minimum delays cannot be guaranteed. Each vehicle has a buffer that is able to store information until a new connection is set up.

The institute also investigates for possibilities to extend EMMA to a city wide communication network with the purpose to offer real time travel information for the passengers. Data like location information, destination and time schedules could be displayed.

Another scenario that can be solved with the approach of Delay-Tolerant networks is a mobile sensor network that consists of cooperative mobile robots or vehicles for industrial applications. Mobile nodes can coordinate and schedule their tasks with other nodes using an occasionally-connected network.

4.3 Recommendations for Internet access

The implementation of public broadband internet access is a goal, which is targeted by many internet service providers. A wireless mesh network could support internet access to both indoor and outdoor scenarios. The focus is, however, primarily on populated areas and rural areas, where there is no infrastructure for internet access (DSL/cable) available. The goal is to realize an area-wide internet access for municipal applications that benefit for residents, tourists, students and business. The internet access has to be implemented in such a way that the access will remain competitive with DSL/cable solutions in terms of costs and practical purposes.

Meanwhile there are companies that offer installations of commercial mesh networks. The company “Strix Systems” [21] offers a mesh solution called “Strix Mesh” based on the 802.11a/b/g standards. The network has the capability of automatic route discovery, load-balancing, self-healing and self-tuning. Additionally it is secured with the WPA and AES standard. Once a new node is inserted into the system, the node scans all available channels and creates a list of potential client devices that are within its range. This network is also capable of prioritizing voice packets over data packets. Strix Systems claims that the mesh network could reach a data rate of 108 Mbit/s with Super G technology. Super G is a technique of bonding two 54 Mbit/s 802.11g channels.

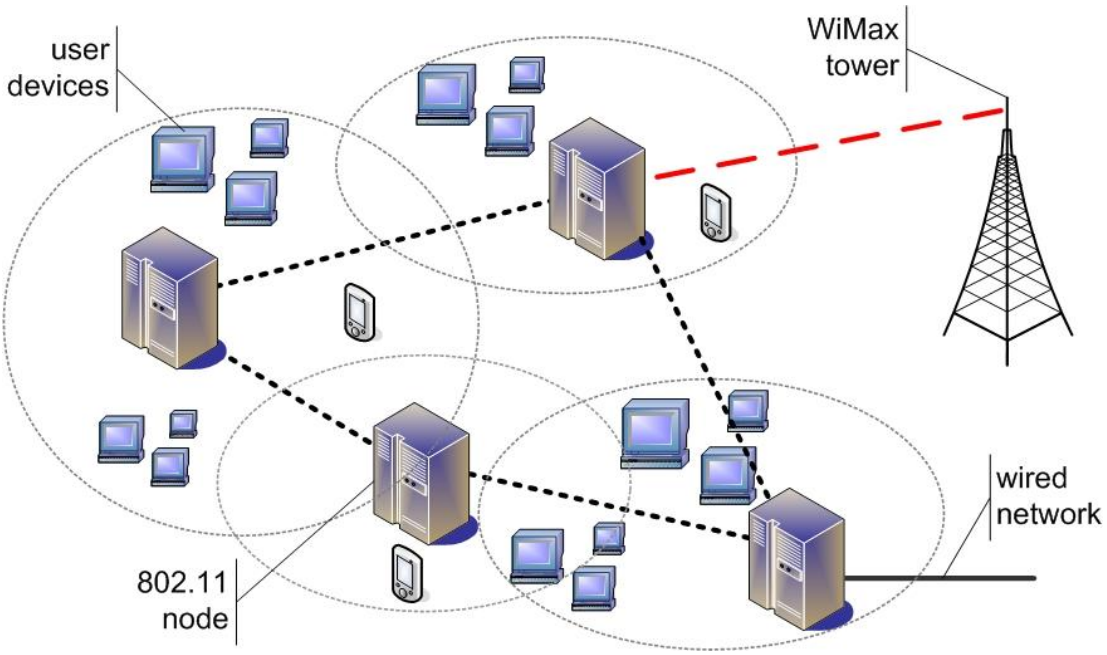

Figure 21: public broadband internet access with mesh technology

Figure 21 gives an overview of a wireless mesh network, which is similar to the Strix Mesh. Once the nodes are installed, they configure themselves to form the full network. While the network is operational, the nodes constantly optimize the performance based on path accessibility and traffic flow. No wires have to be deployed except of one wired internet connection to one or several nodes in the network. The nodes are routing the traffic amongst each other using an 802.11 technology. The network scales proportionally with the user growth.

Ideally, each node features dedicated antennas for sending and receiving in order to increase range. The system intelligently chooses the least congested channel while sending. In order to facilitate smooth transmission, carrier-sensing range should not be larger as transmission range. Furthermore, each node has knowledge of the location of every other node. This would greatly reduce the hidden node problem, and the throughput would remain relatively stable while transmitting over multiple hops.

When setting up mesh networks in rural areas or areas that are hard to reach, the wired internet backbone can be replaced by a wireless technology (Figure 21). One qualified technology that can overcome a distance of up to 50 km is 802.16, also called WiMax. WiMax works in the frequency band above 10 GHz and it can achieve a data rate of up to 108 Mbit/s. Unfortunately, line of sight is necessary for WiMax transmissions, which is the reason why the standard itself drops out for the use in ad hoc mode.

4.4 Recommendations for Short Range Data Transfer

In today's offices, homes and on the move there is an increasing necessity of data that has to be transferred. This concerns setting up networks, sending data to printers or copying presentations and documents from PDAs to desktop computers. In these circumstances, data should not be sent over long distances, but between neighboring devices that are located in the same room or in larger office spaces. These applications are now mostly carried out by cable, for example via USB cable, FireWire, Ethernet, etc.

In this context there is the problem that new devices have to be connected and integrated into the network. A desirable solution is the operation of the peripheral devices in a mesh network, where devices can detect each other independently, and where all devices can

relay data among each other. For this purpose, we first have to know what kind of data we want to transfer and what data volumes are existent. The following Table 8 presents an overview of some applications for short-range data transmissions.

application	type of data	data size
audio transfer to hands-free headsets	low rate audio	< 4 KB/s
digital audio transmissions to wireless speakers	AC-3 audio	< 56 KB/s
transmission of image data between printers, digital cameras, scanners	JPEG, Bitmap, GIF, etc.	>1 MB/file
transmission of video data between video cameras and computers	uncompressed video	< 24 MB/s
data of multiplayer games on mobile devices	TCP packets	>10 KB/s
file transfer (FTP, internet TCP/IP packets)	FTP, TCP, UDP packets	>500 KB/s

Table 8: applications suitable for short range wireless data transmissions

There is an appropriate standard, which makes a crosslinking of these devices possible, namely Bluetooth. As we have shown in Chapter 2.3, Bluetooth is ideal for the use in ad hoc environments, as it is not affected by the hidden node problem; it offers a constant throughput in transmission over several hops and it already has specific data packet profiles for every possible application. This standard is in a position to build up ad hoc networks and manage them autonomously (see section 2.3). Bluetooth 2.1 with EDR offers a transmission rate of 3 Mbit/s (= 375 KB/s). The following calculation makes clear that this transmission rate is not sufficient: a high resolution digital camera photo can take up to 4 MB of space; with the maximum rate of Bluetooth 2.1, the transfer would take about 10 seconds for a single photo, and for the copying of an entire memory card it would take an hour. This period of time is unacceptable. Transfers of video data are completely excluded with this data rate.

The new Bluetooth standard in the version 3 could become a robust high-speed and short-range transmission system. It adopts all characteristics of the previous version and expands its abilities with a UWB radio, which can reach up to 480 Mbit/s on short distances. This would fully suffice for all purposes of transfers within a small radius. With this standard, it would be possible to transfer even uncompressed video streams through a Bluetooth ad hoc network over several hops. Another advantage of this technology is the low power consumption, which makes Bluetooth preferable over Wi-Fi, which has a much higher energy usage for transfers. Just small and mobile devices like gaming consoles and digital cameras have high expectations of low energy consumption, which can be currently better provided by Bluetooth.

5. Conclusion

Different IEEE 802.11 types are mentioned and their properties are briefly described. The focus of the analysis is on the calculation of the theoretical maximum throughput of each standard. Our achievement in this calculation is the derivation of a formula with which the maximum throughput of Wi-Fi standards can be determined. Tests of purchasable wireless routers are also considered, and their performance is involved in the calculations. In these tests 802.11g and n routers turn out to have a bandwidth efficiency that is much lower than 50%.

Some problems are addressed that occur during multihop transmissions, and adverse effects are investigated that decrease the throughput in 802.11 ad hoc networks. An important observation is that the upper limit of a multihop transmission is a quarter of the total throughput what is caused by the hidden node problem. Other problems are identified that bring down the throughput to a seventh of a maximum throughput of a single hop transmission. Another observation is that Bluetooth technologies are less vulnerable to the known problems; this is identified as one of the reasons why Bluetooth offers a constant throughput during multihop transfers compared with 802.11 protocols.

In Chapter 3 of this thesis we introduce several real life scenarios in which wireless ad hoc networks can have an advantage compared with the deployment of wired networks. Some scenarios even cannot be realized with wired networks, such as, intelligent transportation systems, or the category of mobile ad hoc networks in general. In this analysis, we discover that there are scenarios, which require only a small transmission range, for example, as it is in the case of communication between devices in office environments. On the contrary, there are applications that are dependent on a high range, for example, the scenario of internet connectivity in rural areas. It is concluded that ad hoc networks cannot be ignored in the future, and that their importance will strongly increase. Scenarios, which have proved to be suitable for a deployment of ad hoc networks, range from large (temporary/mobile) networks to small-sized scenarios where a closed group of devices needs to communicate with each other (office environment, wireless home network).

In Chapter 4, we investigate whether a realization of the scenarios named above, is possible with the technologies from Chapter 2. We recognize that ad hoc networks cannot guarantee capacity and reliability for video transfer. However, possibilities to increase throughput in ad hoc networks are presented, namely methods for resource-allocation, multi-stream coding, over-provisioning etc. We also make a proposal, how the problem of mobile ad hoc scenarios can be solved on a limited scale with the help of delay-tolerant networks. It is demonstrated how these networks can be constructed, and what advantages and disadvantages are included in their deployment.

The problem of the deployment of a low-cost internet access with mesh networks is addressed as well. The key factors that are essential for the success of such a network are automatic route discovery, load-balancing, self-healing and prioritizing of packets. We analyze which applications are suitable for a short range data transfer of JPEG-files, low-rate audio and TCP packets. For the transfer of this kind of data between devices such as printers, PDAs or digital cameras, the Bluetooth standard proves to be suitable.

In this thesis we come to the conclusion that 802.11 standards can offer a satisfactory platform for the operation in ad hoc networks. Overall, it can be said that the deployment of ad-hoc networks involves following advantages:

- the costs of installation are lower than the cost of a fixed infrastructure
- the possible field of application is versatile (hard-to-reach areas, MANETs)
- we have a higher reliability in case of single node failures

- mesh networks have a high potential to be equipped with technologies like load-balancing, self-healing, automatic route discovery, etc.
- flexibility and expandability when nodes are added or removed

On the other hand, we have the disadvantages of a higher overhead. In the worst case, several protocols have to be added at different layers to ensure certain functionalities. This in turn decreases the actual throughput for the applications. The protocols should be further optimized and expanded in the future. However, nothing stands in the way of using mesh networks. The advantages are clear and outweigh the disadvantages.

6. References

[1] Advanced Network Technologies Division – Wireless Ad Hoc Networks – National Institute of Standards and Technology - www.antd.nist.gov
[2] Jangeun Jun, Pushkin Peddabachagari, Mihail Sichitiu, Theoretical Maximum Throughput of IEEE 802.11 and its Applications
[3] IEEE Standard 802.11-1999
[4] IEEE Standard 802.11a-1999
[5] IEEE Standard 802.11g-2003
[6] Ping Chung Ng and Soung Chang Liew, Throughput Analysis of IEEE 802.11 Multi-hop Ad hoc Networks
[7] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, Robert Morris, Capacity of Ad Hoc Wireless Networks
[8] Fanny Mlinarsky, Test & Measurement World, Testing 802.11n (p.35-p.42), April 2007
[9] Fanny Mlinarsky, Cabling Installation & Maintenance, Will 802.11n be a good neighbor? September 2007
[10] J. Scott Haugdahl, Inside 802.11n Wireless LANs – Practical Insights and Analysis, December 2007
[11] Tarek N. Saadawi, Yong Liu, Myung J. Lee, A Bluetooth Scatternet-Route Structure for Multihop Ad Hoc Networks, IEEE journal on selected areas in communications, Vol. 21, No.2, February 2003
[12] InformationWeek - Review: 6 New 802.11n Wi-Fi Routers - Is It Time To Switch From 802.11g? – www.informationweek.com
[13] Michael Bahr, Proposed Routing for IEEE 802.11s WLAN Mesh Networks
[14] Sebastian Max, Guido R. Hiertz, Erik Weiss, Dee Denteneer, Bernhard H. Walke, Spectrum sharing in IEEE 802.11s wireless mesh networks, 2007
[15] Raffaele Bruno, Marco Conti, Enrico Gregori, Mesh Networks: Commodity Multihop Ad Hoc Networks, IEEE Communications Magazine, March 2005
[16] One Laptop Per Child, official webpage http://laptop.org/laptop/hardware/meshdemo.shtml
[17] Rüdiger Kays, Klaus Jostschulte, Wolfgang Endemann, Wireless Ad-Hoc Networks with High Node Density for Home AV Transmissions, IEEE 2004
[18] Cerf. V. et al., Delay-Tolerant Network Architecture, IETF RFC 4838, informational, April 2007
[19] Shiwen Mao, Shunan Lin, Shivendra S. Panwar, Yao Wang, Emre Celebi, Video Transport Over Ad Hoc Networks: Multistream Coding With Multipath Transport, 2003
[20] Yi J. Liang, Eckehard G. Steinbach, Bernd Girod, Multi-Stream Voice Over IP Using Packet Path Diversity, IEEE 2001
[21] Strix Systems Inc., Access/One Network IWS System Description , www.strixsystems.com
[22] Computerworld.com, Coming to a watering hole near you: OLPC's mesh networking, http://www.computerworld.com.au/index.php/id;1228527977
[23] EMMA – Environmental Monitoring in Metropolitan Areas, Technische Universität Braunschweig, Institut für Betriebssysteme und Rechnerverbund, http://www.ibr.cs.tu-bs.de/projects/emma/

7. Abbreviations and acronyms

AP = Access Point
DSSS = Direct-Sequence Spread Spectrum
OFDM = Orthogonal Frequency-Division Multiplexing
DCF = Distributed Coordination Function
CSMA/CA = Carrier Sense Multiple Access/Collision Avoidance
RTS/CTS = Request-To-Send / Clear-To-Send
PLCP = physical layer convergence protocol
PMD = physical medium dependent
CTS = Clear-To-Send
RTS = Request-To-Send
ACK = Acknowledgement
FH-CDMA = frequency hopping code-division multiple-access
HWMP = Hybrid Wireless Mesh Protocol
OLPC = One Laptop Per Child project
XO-Laptop = 100 Dollar Laptop of the OLPC project
DVD/BD player = Digital Versatile Disc / Blue Ray Disc player
UWB = ultra wide band radio