MULTIMEDIA (SMS, MMS, AUDIO, VIDEO) OVER POSITION AWARE PERSONAL AREA MOBILE AD HOC WIRELESS NETWORKS (PAPAMANETS)

By

Ayesha Naureen

Kharia Ahmed

Humad Hafeez

Yaser Mirza

Submitted to the Faculty of Computer Science

National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements of a B.E. Degree in Computer Software Engineering

May 2005

ABSTRACT

An ad hoc network is a collection of mobile nodes using wireless network interfaces to communicate among themselves, discovering and routing along possibly multihop routes to each other without the assistance of fixed infrastructure. Multimedia conferencing on wired networks has been studied and implemented by several software vendors such as Microsoft NetMeeting. However, multimedia applications on wireless endpoint devices such as PDA's, iPAQs, etc. have not been researched and implemented widely. Personal communications and mobile computing requires a wireless network infrastructure which is fast deployable, multihop, and capable of multimedia service support on wireless endpoint devices such as iPAQs. Such rapidly deployable networks are categorized as mobile ad hoc networks (MANETS).

This project explores the difficulties of deploying multimedia applications on position aware personal area mobile ad hoc wireless networks (**PAPAMANETS**) and implements a prototype for it.

DECLARATION

No portion of the work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere.

DEDICATION

In the name of Allah, the most gracious and the most merciful

To our parents, without whose support and cooperation, a work of this magnitude would not have been possible

ACKNOWLEDGEMENTS

We would like to thank COL Raja Iqbal, our internal project supervisor, for his guidance, knowledge and support during this project. His assurance kept us going through the occasional bumps of the journey.

We also want to thank Dr. Shoaib, our external project supervisor, for the opportunity and support in joining the research project. We appreciate his guidance and

patience and do hope that that we have made a valuable contribution to the Multimedia over MANETs group.

Great appreciation goes to Maj Saad, who was always around to listen to any problems we had. Many times he has given us advice and new ideas in approaching our task.

We would also like to thank the CS lab administrators who were always there to help us.

We would also like to give a special thanks to our parents and families for their invaluable support and patience through the course of the project.

PREFACE

This thesis is written as a part of our B.E Degree in Software Engineering at the National University of Sciences and Technology.

Our deep interest in the field of computer networking drove us to do something in this field. Luckily, we were directed to the emerging field of ad hoc networks, in which little has been done so far. Development of multimedia applications for MANETS, with utilization of compression techniques for audio, video conferencing application, experimenting with a MANET routing protocol and the actual deployment of an ad hoc

network; has surely been the perfect assignment for us. It has been a lot of challenging, hard work, but at the same time it has been very rewarding and fun. Through this work, we have learnt a lot about network programming, routing protocols and computer hardware.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

Chapter 1

Introduction

In the recent years, mobile communications have increased in usage and popularity. Devices get smaller, batteries live longer and communication protocols get more robust and offer more throughput. Tasks earlier handled by wired communication can now be done using wireless devices and technology, thus giving users the advantage of mobility.

The vision of mobile ad-hoc networking is to support robust and efficient operation in mobile wireless networks, by incorporating routing functionality into mobile

nodes. Such networks can have dynamic, sometimes rapidly-changing, multi-hop topologies which are likely composed of relatively bandwidth constrained wireless links.

Support of real time multimedia streams, such as text/data, live audio and video over the network, in mobile ad hoc networks is particularly challenging due to the rapid changes in routing that may occur with node motion and due to occurrences of interference, bandwidth limitation, in order packet delivery, packet loss and congestion in the shared radio spectrum used by the nodes.

Multimedia over such mobile ad-hoc networks finds its usage in situations where spontaneous networking is needed. Examples are disastrous situations, emergency search-and-rescue operations, battlefields etc.

1.1 Implementation Work

The work on the project includes an entire implementation of the various multimedia applications, covering the basic aspects of network programming for all the applications, and compression techniques for audio and video conferencing applications. Advantage is taken from the fact that the implementation of OLSR is very modular in design and is easy to extend through the use of plugins. Thus the transfer of multimedia over MANETs is facilitated by supplying multimedia applications as plugins to OLSR. All these solutions are described in this report.

Due to space limitations, not every part of this report will include a full background presentation of the technical aspects of the material. It is assumed that the reader has some basic knowledge of things such as UDP/TCP IP networking and C programming.

1.2 Chapter Overview

Chapter 2 gives a literature review done for the project, covering the basic characteristics of MANETs and an overview of routing protocols.

Mobile ad-hoc networks are introduced in chapter 3. This chapter also introduces the basics of wireless data-communication and other related technology. Three of the routing protocols proposed by the Internet Engineering Task Force (IETF) are also presented in this chapter.

Chapter 4 gives an overview of the system architecture for the multimedia applications designed for the project. The operation of these applications is also explained in detail in Chapter 4.

H.323 standard is a cornerstone technology for the transmission of real-time audio, video, and data communications over packet-based networks. Chapter 5 provides an insight into the working of H.323.

OLSR operation is described in detail in chapter 6 with an overview of the various routing protocols available for MANETS.

An interface to enable the use of our multimedia applications as plugins to OLSR is described in chapter 7.

Chapter 8 focuses on the deployment of ad hoc network, utilizing 802.11g wireless LAN cards. It deals with the hardware configuration of the Wireless LAN cards to operate in ad hoc mode.

The future of the project covered in chapter 9 briefly explains the utility of the project in various fields, giving an overview of the possible applications of the project. Also future extensions to the project are suggested. Finally, concluding remarks are also made.

Chapter 2

Literature Review

For the successful completion of the project, an immense consideration of four major areas was obligatory. These were: an understanding of the field of ad hoc networking, comprehension of compression techniques for audio and video transmission and grasping the details of the configuration of wireless LAN cards to operate in ad hoc mode for the practical deployment of the project. Thus the initial study carried out for the project was organized in these four areas.

This chapter focuses on the literature reviewed for a basic understanding of ad hoc networking, routing protocols, compression techniques and ad hoc configuration of the hardware.

2.1 Wired Vs Wireless Networks

Wireless mobile computing and networking is very challenging. Most solutions developed for wired networks aren't applicable when used for wireless networks. Table 2.1 gives a comparison of wired and wireless networks based on the well-known network parameters.

Characteristics	Wired Networks	Wireless Networks
Bandwidth	High	Low
Bandwidth Variability	Low	High
Error Rates	Low	High
Connectivity	Symmetric	Possible Asymmetric
Security	Need Physical Access	Need Proximity
Delay	Low	Higher
Operation	Connected	Disconnected
Quality Variability	Low	High
Power and Resources (Computational Ability, Memory, Storage)	High	Low

Network Protocols	Traditional IP	IEEE 802.11, mobileIP, AODV, OLSR, new TCP variations

Table 2.1: Comparison of Wired and Wireless Networks

2.2 Types of Wireless Networks

There are essentially three types of wireless networks: Infrastructured Networks, Infrastructureless/ Ad hoc Networks and Hybrid Wireless Networks.

Infrastructured networks are characterized as those having fixed, wired backbone, in which, devices communicate directly with access points. This type of networking is suitable for locations where access points can be placed.

In case of ad hoc networks, there is no wired backbone. All nodes forming the networks are capable of movement and all nodes serve as routers. Such type of network can be easily deployed as and when needed with very low administrative cost.

The third type of wireless networks combats the limitations of infrastructured wireless networks and provides internet connectivity to ad hoc networks.

Another classification of wireless networks can be in terms of deployment: Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN) and Wireless Wide Area Networks (WWAN), as shown in figure 2.1. Current deployment of ad hoc networks is confined to Wireless Personal Area Networks and Wireless Local Area Networks. Off the-shelf technologies for WPAN and WLAN are enablers of ad hoc networks. In the future, wide area ad hoc networks will be a reality.

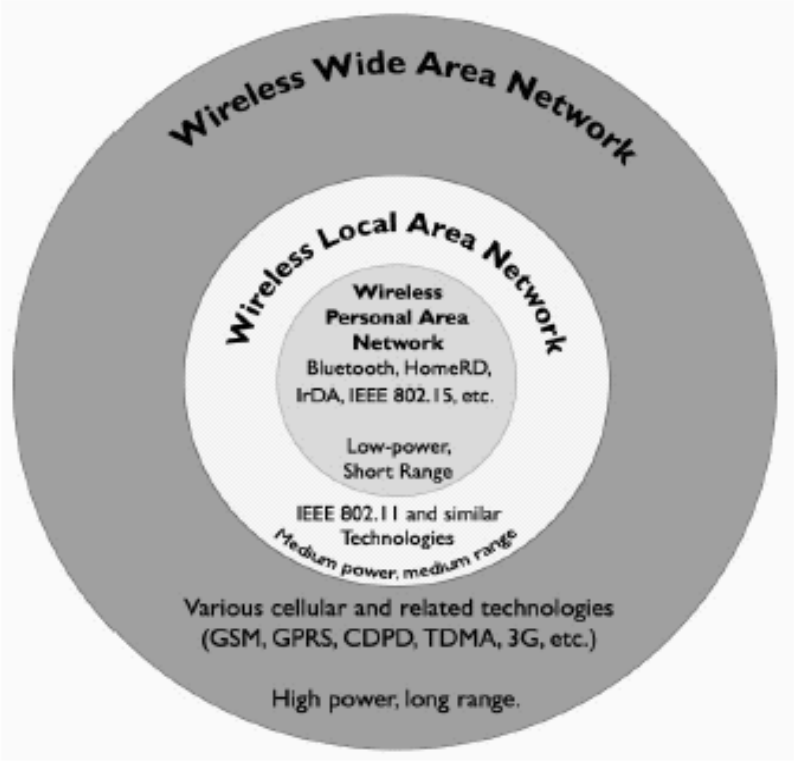

Figure 2.1: The Entire Wireless Landscape

2.3 Open Research Problems for MANETs

Some open research problems for MANETs are: [1]

Scalability: Ad hoc networks suffer from the scalability problems in node capacity due to physical resource limitation.

Quality of Service: QoS in ad hoc networks is the problem inherited from mobile networks. Connections with quality-of-service (QoS) requirements, such as those for multimedia applications with bandwidth constraint, recently have been intensively studied QoS issues in MANETs.

Client Server Model Shift: In ad hoc networks, the issue of locating a requested service and sending of request for the service is a major problem. P2P software model could be suitable for MANETs.

Security: Security issues in MANETS are a composition of those found in traditional networks and those inherent from the mobility problems.

Interoperation with the Internet: IP and MANET are different networks; the process of defining an interface between them is not straightforward. Mobile-IP technology may be a solution.

Power Control: If the nodes are power-constrained embedded device, the power efficiency problem should be considered for the MANETs environment.

Support for Different Routing Protocols: Different routing protocols should be used according to different environments and applications.

Interoperation with Other Wireless Networks: This relates to the scenario when more than one ad-hoc networks are in the same area. It's a joint problem with applications and relates MAC and routing protocols.

2.4 Categories of MANET Issues and Sub-issues

In this section, general observations about the research issues in MANETs are presented. According to different research features, fifteen issues and sub-issues are grouped in Table 2.2. Hundreds of research aspects have been developed and discussed in

this field. Out of these, some fundamental and frequently discussed aspects of MANET are identified and grouped into fifteen categories.

Item #	Issues	Sub-issues
1	Routing	Routing Protocol, Proactive / Reactive / Hybrid Scheme
2	Multicasting/Broadcasting	Source-based / Shared based Schemes, Proactive / Reactive / Hybrid Schemes, Tree / Mesh Schemes, Flat / Hierarchy Schemes, Flooding , Broadcast Storm
3	Location Service	Location service, GPS, geographic position, Graph theory, Grid
4	Clustering	Clusterhead / Gateway, k hop Clustering, Cluster formation / Maintenance
5	Mobility Management	Mobility model, Mobility-aware protocol , Mobility Prediction
6	TCP / UDP	TCP/IP, Acknowledgement
7	IP Addressing	IPv6, IP management, Mobile IP, Address resolution, Addressing Model
8	Multiple Access	Hidden terminal, Collision, FDMA / TDMA / CDMA, CSMA/CA
9	Radio Interface	Omni-directional antennas, Directive antennas, Radiofrequency interference, Radio transmission, Radio channel

10	Bandwidth Management	Load balancing, Traffic control, Virtual backbone
11	Power Management	Power consumption, Power aware, Energy Efficiency
12	Security	Authentication, Encryption/ Decryption
13	Fault Tolerance	Fault recovery, Fault diagnosis, Checkpointing
14	QoS / Multimedia	QoS-based multimedia service, Multimedia QoS Measurement
15	Standards / Products	Bluetooth, IEEE 802.11, HomeRF, IrDA

Table 2.2: MANETs Issues and Sub-Issues

2.4.1 Routing

Routing is a key protocol in this field, because the changes of network topology changes are frequent. An efficient routing protocol is required to cope with high dynamic network conditions.

2.4.2 Multicasting / Broadcasting

There are many applications for MANETs such as disaster recovery or rescue missions. These applications need a multicast service for users who want to communicate with other members in a multicast group.

2.4.3 Location Service

Location information uses the Global Positioning System (GPS) or the network-based geo-location technique to obtain the physical position of destination.

2.4.4 Clustering

Clustering is a method to partition the hosts into several clusters (groups). At each cluster, a clusterhead is selected by a clustering algorithm to be the dominator and manages members in its cluster. Clustering provides a convenient framework for resource management.

2.4.5 Mobility Management

In the environment of MANET, mobile hosts can move unrestricted from place to place. The position information of a mobile host should be identified before other node's call to the mobile host can be established. Mobility management handles with the storage, maintenance, and retrieval of the mobile node position information.

2.4.6 TCP/UDP

TCP and UDP are the standard protocols used in the Internet. TCP can ensure reliable packet delivery and provide efficient bandwidth utilization, but it is not suitable for using in MANETs. UDP is usually used for real-time applications. UDP supplies minimized transmission delay without the connection setup process, flow control and retransmission.

2.4.7 IP Addressing

One of the most important issues is the set of IP addresses that are assigned to the MANET. When a mobile node wants to join the MANET, it has to be assigned an IP

address as part of its initialization. IP addressing and address autoconfiguration have attracted much attention in MANETs.

2.4.8 Multiple Access

The multiple access issue is discussed for the MAC layer in MANETs. The 802.11 MAC layer uses a carrier sensing with a single CTS / RTS handshake to prevent the ‘hidden node’ problem to arise.

2.4.9 Radio Interface

Because the MANET is a wireless environment, the mobile nodes rely on the radio interface or antenna to transmit the packet is needed. In order to investigate the packet forwarding or receiving via radio interface or antenna technique, this topic is also very important in MANETs.

2.4.10 Bandwidth Management

Bandwidth management in MANETs is a typical characterization. Because of the bandwidth limitation, the issue of its effective management and use is a very important issue.

2.4.11 Power Management

Because most ad-hoc mobile devices operate on batteries, power consumption becomes an important issue which includes the issues: maximizing the lifetime of the entire network, evenly distributing the power consumption rate of each node, and minimizing the overall transmission power for each connection request.

2.4.12 Security

The mobile nodes in the MANET are highly vulnerable to malicious damage. The conventional security measures cannot be used in MANETs. In absence of prevention

schemes, the nodes will be a vulnerable point in the network through which intruder can crack.

2.4.13 Fault Tolerance

This issue attempts to ensure that network faults are detected and corrected. Fault-tolerance techniques are brought in for the maintenance when failure occurs during the nodes move, join, or leave the network.

2.4.14 QoS/Multimedia

The Quality of Service (QoS) is concerned with high bandwidth, low delay, and high reliability in this field, especially in relation to multimedia.

2.4.15 Standards/Products

The issues of standards and products that allow the small scale developments are emerging for this field e.g. Bluetooth, which is a low-cost technology for short-range communications technique.

2.5 Routing Protocols Taxonomy

2.5.1 Wired Routing

Traditional wired networks are composed of specified centralized nodes – router – which are only responsible for making routing decision for transmitted packets. Routers are located on backbone network. Each node connects to a router and does not concern the routing problems. The routing procedure is processed in the router, and independent with end users.

For the wired networks, each router usually maintains one or multiple routing tables which store the “distance” information for each neighbor router, or probably “distance” to all routers. The information stored in the routing table could vary and

depends on what protocol is used. Distance Vector and Link State-based protocols are the most accepted approaches for IP network.

Routing table is the fundamental element for wired networks, which indicates each router maintains the whole or part of the network status for a certain period of time. The assumption is that the network topology should be stable so that the routing table synchronization would not impact the whole networks performance. But it is not feasible for fast changing topology of MANETs.

2.5.2 MANETs Routing Category

This section introduces the routing category for MANETs [2]. Table 2.3 summarizes routing protocols for MANETs.

Table-driven protocols are extended from the wired networks routing and each node maintains a routing table independent of the data transmission. On-demand protocols determine the routing decision just when the data is to be transmitted.

Routing Category	Main Features	Examples
Proactive Routing (Table Driven)	Propagates routing information throughout the network at regular time intervals. This routing information is used to determine paths to all possible destinations. This approach generally demands considerable overhead for the message traffic as well as for the routing information maintenance.	Topology Broadcast based on Reverse Path Forwarding (TBRPF)[3], Fisheye State Routing (FSR)[4], Optimized Link State Routing (OLSR) [5], Dynamic Destination-Sequenced Distance-Vector Protocol (DSDV)[6], Source Tree Adaptive Routing (STAR)[7], Cluster Switch Gateway Routing (CSGR) [8], Wireless Routing Protocol (WRP)[9]
Reactive Routing (On-Demand)	Maintains path information on a demand basis by utilizing a query-response technique. The total number of destinations to be maintained for routing information is considerably less	Ad Hoc On-Demand Distance Vector Routing (AODV)[10], Dynamic Source Routing (DSR) [11], Relative Distance Microdiversity Routing (RDMAR)[12], Signal

	than flooding; hence, network traffic is also reduced.	Stability Routing (SSR) [13], Temporally Ordered Routing Algorithm (TORA)[14]
Hierarchical Routing	Provides efficient routing of messages in large dynamic networks. Divides network into interconnected clusters of nodes, which might or might not overlap.	Landmark Ad Hoc Routing Protocol (LANMAR)[15], Hierarchical State Routing (HSR)[16]
Hybrid Routing	Integrates both proactive and reactive routing into a single protocol. Exhibits proactive behavior under a given set of circumstances and reactive behavior under a different set of circumstances.	Zone Routing Protocol (ZRP) [17], Distance Effect Algorithm for Mobility (DREAM)[18]
Secure Routing	Secure routing using intrusion detection and authentication techniques.	Authenticated Routing for Ad Hoc Networks (ARAN) [19], Secure Aware Routing (SAR) [20], Secure Routing Protocol (SRP)[21]

Table 2.3: Summary of Routing Protocols

2.6 Standards for 802.11

As the globally recognized LAN authority, the IEEE 802 committee has established the standards that have driven the LAN industry for the past two decades including 802.11, the first internationally sanctioned standard for wireless LANs.

WLANs come in several different flavors. The three most common types are 802.11a, 802.11b and 802.11g. All of these standards use the Ethernet transport protocol, making them compatible with higher-level protocols like TCP/IP. Where they differ is in the specifics of their transmission characteristics.

802.11a networks are ideal with respect to high performance, for instance, while deploying voice or video applications over WLAN.

802.11b networks are ideal when deploying a WLAN in a large facility with significant range requirements, for instance a warehouse or department store.

802.11g is ideal in the sense that it combines the advantages of both 802.11a and 802.11b.

Table 2.4 compares the three standards.

Characteristics	802.11a	802.11b	802.11g
Frequency	5 GHz	2.4 GHz	2.4 GHz
Data Rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48, 54 Mbps
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	BPSK, QPSK, CCK	BPSK, QPSK, 16 QAM, 64 QAM, CCK
FEC Rate	1/2, 2/3, ¾	NA	1/2, 2/3, ¾
Basic Transmission Mode	BPSK, 6 Mbps, FEC 1/2	BPSK, 1 Mbps	802.11a (6 Mbps) or 802.11b (1 Mbps) basic modes

Table 2.4: Characteristics of the Various Physical Layers in the IEEE 802.11 Standard

2.7 H.323

Networks of computers are built on standards and protocols, selected so that the applications dependent upon the network can exist and operate at their fullest capabilities. The ITU (International Telecommunications Union) is an organization that develops internationally recognized recommendations and standards to enable computers, radios, and other machines to interact with one another.

The ITU H.32x family of standards handles multimedia communications. This family includes H.320 (communication over ISDN [integrated services digital networks]) and H.324 (communication over SCN [switched circuit network], better known as traditional phone services).

The H.323 standard is a cornerstone technology for the transmission of real-time audio, video, and data communications over packet-based networks. It specifies the components, protocols, and procedures providing multimedia communication over packet-based networks as illustrated in figure 2.2.

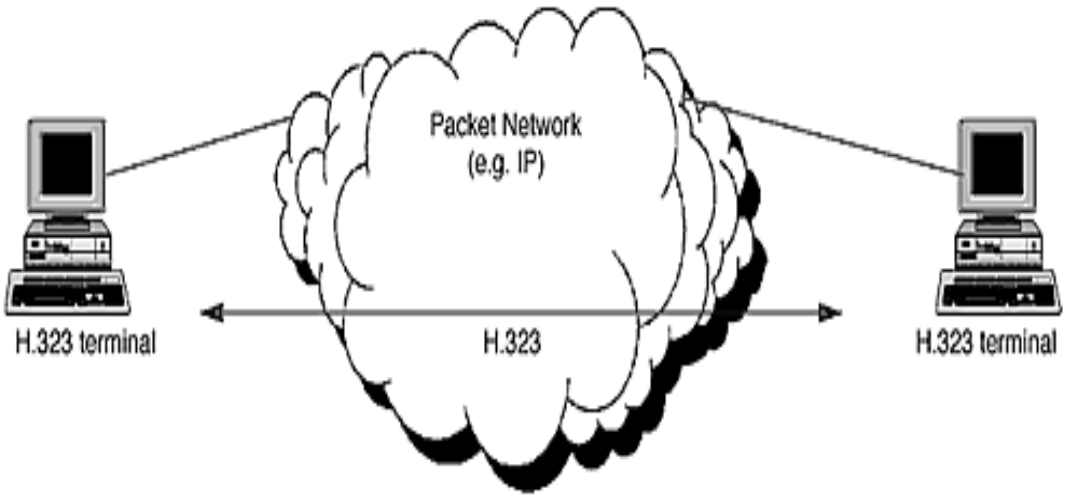

Figure 2.2: H.323 Components and Operation

Packet-based networks include IP based (including the Internet) or Internet packet exchange (IPX) based local-area networks (LANs), enterprise networks (ENs), metropolitan-area networks (MANs), and wide-area networks (WANs).

H.323 can be applied in a variety of mechanisms: audio only (IP telephony); audio and video (video telephony); audio and data; and audio, video and data. H.323 can also be applied to multipoint-multimedia communications.

The H.323 standard specifies the pieces that combine to provide a complete communication service, which are: **terminals**, either PC or stand alone devices, these are the endpoints of the communication lines; **gatekeepers**, the brains of the network; providing services like addressing/identification, authorization, and bandwidth management; **gateways**, which serve as translators when connecting to a dissimilar network (such as an H.324); **MCUs** (multipoint control units) which allow multipoint conferencing, or communication between more than two parties at once.

An H.323 zone is a collection of all terminals, gateways, and MCUs managed by a single gatekeeper as is in figure 2.3. A zone includes at least one terminal and may include gateways or MCUs. A zone has only one gatekeeper. A zone may be independent of network topology and may be comprised of multiple network segments that are connected using routers or other devices.

In addition to component types, H.323 also describes protocol standards, permissible audio and video codecs, RAS (registration, admission, and status), call signaling, and control signaling. H.323 specifies a mandatory level of compliance and support for the above specifications for all terminals on the network.

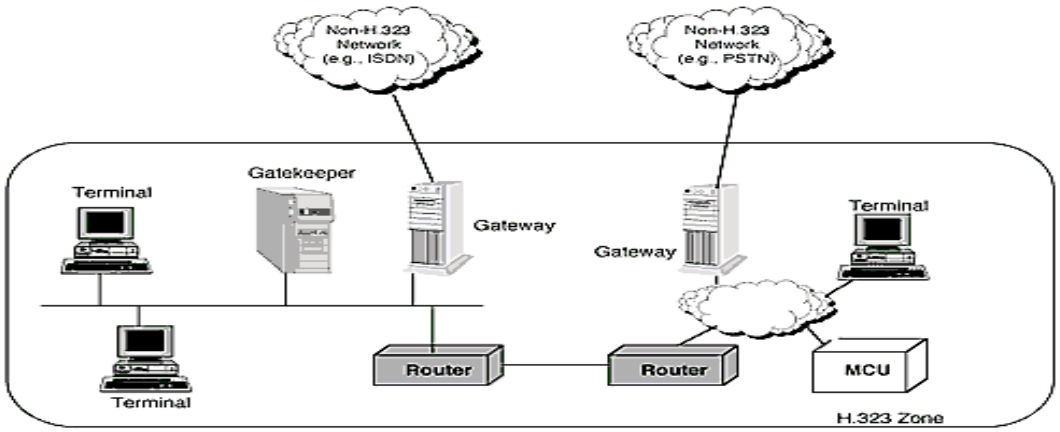

Figure 2.3: Connected H.323 Components

Figure 2.4 illustrates that the H.323 protocol actually comprises of a lot of different standards including Call Signaling and Control, Audio and Video codecs.

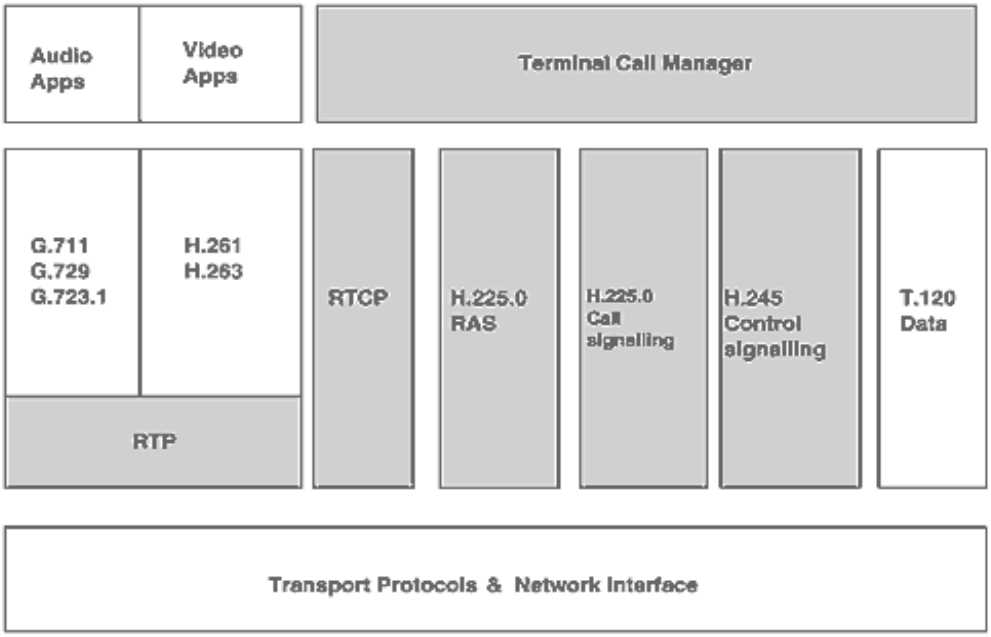

Figure 2.4: H.323 Standards

Registration, admission, and status (RAS) is the protocol between endpoints (terminals and gateways) and gatekeepers. It is used to perform registration, admission control, bandwidth changes, status, and disengage procedures between endpoints and gatekeepers.

The H.225 call signaling is used to establish a connection between two H.323 endpoints. H.245 control signaling is used to exchange end-to-end control messages governing the operation of the H.323 endpoint.

An audio CODEC encodes the audio signal from the microphone for transmission on the transmitting H.323 terminal and decodes the received audio code that is sent to the speaker on the receiving H.323 terminal. Audio codecs include: G.711 - PCM audio

codec 56/64 kbps, G.722 - audio codec for 7 KHz at 48/56/64 kbps, G.723.1 - speech codec for 5.3 and 6.3 kbps, G.728 - speech codec for 16 kbps, G.729 - speech codec for 8/13 kbps.

A video CODEC encodes video from the camera for transmission on the transmitting H.323 terminal and decodes the received video code that is sent to the video display on the receiving H.323 terminal. It includes: H.261 - video codec for >= 64kbps, H.263 - video codec for < 64kbps.

2.8 Summary

This chapter focuses on the knowledge foundation established for the project. This all includes the comparison of wired and wireless networks, the categorization of ad hoc as a type of wireless networks, the major research trends in the emerging field of ad hoc networking, the classification of routing protocols for ad hoc, the three 802.11 IEEE standards, and the H.323 standard, which forms the video conferencing core.

Chapter 3

Mobile Ad hoc Networks

Much of the wireless technology is based upon the principle of direct point-to-point communication. Popular solutions like Group Standard for Mobile communications (GSM) and Wireless Local Area Network (WLAN) both uses an approach where mobile nodes communicate directly with some centralized access point. These types of networks demand centralization for configuration and operation. Contrary to this model is the multi-hop approach. In multi-hop scenarios, nodes can communicate by utilizing other nodes as relays for traffic if the endpoint is out of direct communication range.

Mobile ad-hoc network, MANET [22], uses the multi-hop model. These are networks that can be set up randomly and on-demand. They should be self configuring and all nodes can be mobile resulting in a possibly dynamic network topology.

3.1 Ad-hoc Networks

A mobile ad hoc network (MANET) is a collection of nodes, which are able to connect via a wireless medium forming a dynamic network [23]. These nodes may appear and disappear anytime within the network. This implies that the network topology is constantly changing and the network traffic may be routed between nodes in order for communication to occur.

Centralized networks, such as GSM, cannot be used in all situations. Significant examples of such scenarios include establishing survivable, efficient, dynamic communication for rescue operations, disaster relief efforts and military networks. Such

network scenarios that cannot rely on centralized and organized connectivity can be conceived as applications of MANETs. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks.

To enable multi-hop communication in a distributed manner, all nodes should be able to act as routers for each other as shown in figure 3.1. Routes are set up and maintained by a routing protocol. MANET routing protocol design is a complex issue considering the possible rapidly changing topology of such networks.

For route maintenance, one has two main approaches in MANETs, reactive and proactive. Reactive routing protocols set up traffic routes on-demand, whilst proactive protocols attempts to dynamically maintain a full understanding of the topology.

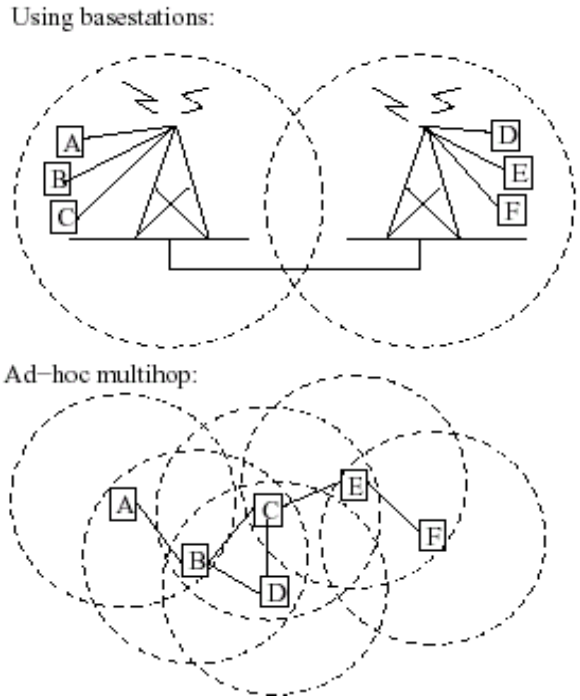

Figure 3.1: A Traditional Base Station Scheme Compared to an Ad-hoc Multi-hop Network

3.2 Classification of Ad-Hoc Networks

There is no standard classification of ad-hoc networks. But a simple classification is to distinguish by formation and communication:

3.2.1 Singlehop

In the singlehop configuration, nodes are in their reach area and can communicate directly. The singlehop configuration is shown in figure 3.2.

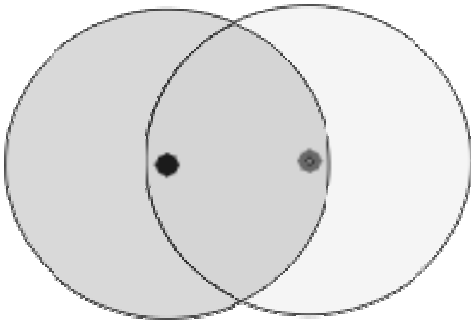

Figure 3.2: Singlehop Configuration

3.2.2 Multihop

Some nodes in an ad hoc network are far and cannot communicate directly. Therefore, the traffic of this communication end-points have to be forwarded by other intermediate nodes. In figure 3.3, the communication path of far nodes is depicted by black lines.

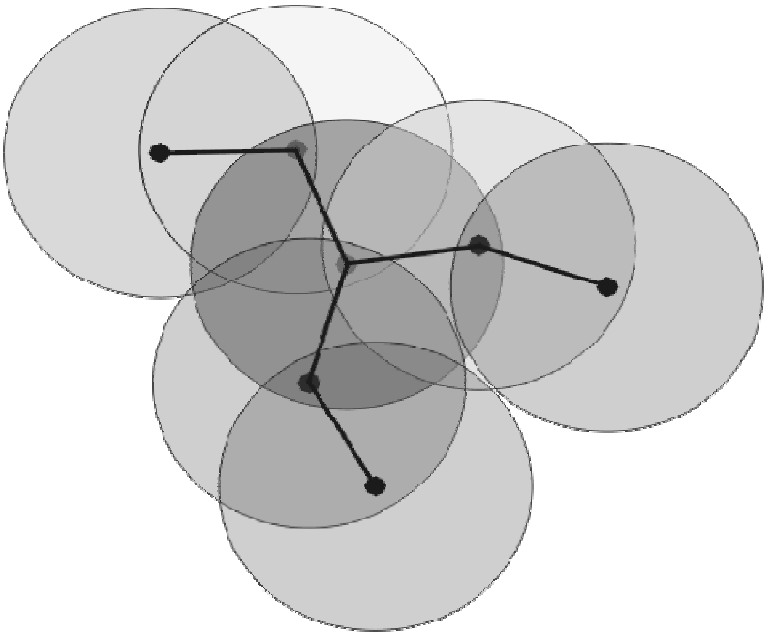

Figure 3.3: Multihop Configuration

3.3 Properties of MANETs

A MANET consists of mobile nodes which are free to move; while there is neither an infrastructured wired network, nor base stations. The nodes connect to each other by wireless transmitters and receivers. Therefore, in the worst case, the network topology changes continuously. This property of MANETs demands that the applied solutions and approaches have to deal with a very different environment than their counterparts in fixed networks. Table 3.1 lists some of the MANET characteristics.

Mobile	The nodes may not be static in space and time resulting in a dynamic network topology. Nodes can move freely and independently. Also some new nodes can join the network, and some nodes may leave the network.
Wireless	MANET uses wireless medium (radio, infrared, etc.) to transmit and receive data. Nodes share the same media.
Self-organizing, distributed, and infrastructure-less	They are self-organizing in nature. There is no centralized control which implies that network management will have to be distributed across various nodes. This makes fault detection and management quite difficult.
Multi-hop	A message from source node to destination node goes through multiple nodes because of limited transmission radius. Every node acts as a router and forwards packets from other nodes to facilitate multi-hop routing.

Scarce resources	The wireless links have limited bandwidth and variable capacity. They are also error prone. In addition, the mobile nodes have limited battery power along with limited processing power. So, energy is a scare resource.
Temporary and rapidly deployable	These networks are temporary in nature. There is no base station. Whenever the nodes are within their transmission radius, they form an ad hoc network. Hence, they are rapidly deployable.
Neighborhood awareness	Host connections in MANET are based on geographical distance.

Table 3.1: Characteristics of MANETs

As illustrated earlier, the network topology in MANETs may change with time depending on nodes' physical positions, their transmitter and receiver coverage, transmission power levels, and co-channel interference levels. These inheritance characteristics from both physical and application determine MANETs have the following technology characteristics: [24]

3.3.1 Dynamic Topology

Nodes are free to move arbitrarily; thus, the network topology – which is typically multi-hop – may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

3.3.2 Bandwidth-Constrained, Variable Capacity Links

Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the throughput of wireless communications is often much less than a radio's maximum transmission rate. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

3.3.3 Energy-Constrained Operation

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

3.3.4 Limited Physical Security

The nodes and the information in MANETs are exposed to the same threats like in other networks. Additionally to these classical threats, in MANETs there are special threats, e.g. denial of service attacks against the energy resource can be performed by using of any of the services a node is offering.

3.4 Ad hoc Communication Using IEEE 802.11 Specifications

Ad-hoc networks are not restricted to any special hardware. But today such networks are most likely to consist of nodes utilizing so-called WLAN interfaces. These are wireless interfaces operating according to IEEE specifications 802.11a [25], 802.11b [26] or 802.11g [27].

IEEE 802.11 [28] does not support multi-hop communication by it self. Two modes are defined for communication using WLAN devices: **Infrastructure mode** and **Ad hoc mode**. In the infrastructure mode, the wireless network consists of at least one access point and a set of wireless nodes. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs (multiple cells). The ad hoc mode is a peer-to-peer mode. This configuration is called Independent Basic Service Set (IBSS), and is useful for establishing a network where nodes must be able to communicate directly and without any centralized access point.

The Ad-hoc mode is obviously the mode to use when setting up a MANET, but it lacks one basic requirement: multi-hop. Traffic is only transmitted to neighbors within radio range when using the ad-hoc mode, therefore there is a need for MANET routing protocols to set up and maintain traffic paths.

3.5 Traditional IP Routing

Routing is the primary function of IP. IP datagrams are processed and forwarded by routers which relay traffic through paths set up by various routing protocols. Routing in today's fixed networks is based on **network aggregation** combined with **best matching**. TCP/IP hosts use a routing table to maintain knowledge about other IP networks and IP hosts. Networks are identified by using an IP address and a subnet mask, and routes to single hosts are rarely set up. When a packet is to be forwarded, the routing table is consulted and the packet is transmitted on the interface registered with a route

containing the **best match** for the destination. If no network matches are found, a default route is used if one exists.

When configuring a network interface with an IP address, a route to the network the address is a member of is usually registered on the interface automatically. This route is not set up with a gateway (the next hop along the path to the host) since hosts with addresses within this network are assumed to be reachable directly from this interface. This shows that the traditional IP routing maintains an idea of all hosts within the same subnet being on the same link. This means that all hosts in a subnet are available on a single one-hop network segment, typically via routers or switches.

When working on wireless multi-hop networks this is not the case. One needs to redefine the idea of nodes being available “on the link”. In MANETs nodes routes traffic by retransmitting packets on the interface it arrived. This approach breaks with the wired “on-link” way of thinking.

MANET requires a different mindset when it comes to routing. Aggregation is not used in MANETs, all routing is host based. This means that for all destinations within the MANET, a sender has a specific route. In a wired network this is not necessary due to the fact that all nodes in the local network are considered available on the link.

3.6 The MANET IETF Working Group

The Internet Engineering Task Force (IETF) has set down a working group for MANET routing [29]. The purpose of this working group is “to standardize IP routing protocol functionality suitable for wireless routing application within both static and

dynamic topologies. The fundamental design issues are that the wireless link interfaces have some unique routing interface characteristics and that node topologies within a wireless routing region may experience increased dynamics, due to motion or other factors."[29].

A wide diversity of protocols have been proposed, but as of this writing, only three protocols are accepted as experimental Request For Comments(RFC), namely Ad hoc On-Demand Distance Vector (AODV)[30], Optimized Link State Routing (OLSR)[31], and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)[32]. The Dynamic Source Routing Protocol (DSR)[33] is expected to be accepted as a RFC in a near future.

3.7 MANET and Mobile IP

In the Internet community, Mobile IP (MIP)[34] is often mentioned when it comes to routing support for mobile hosts. This is technology to support nomadic host roaming, where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility requires address management, protocol interoperability enhancements and the like, but core network functions such as hop-by-hop routing still presently rely upon pre- existing routing protocols operating within the fixed network. In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless

domains, where a set of nodes, which may be combined routers and hosts, themselves form the network routing infrastructure in an ad hoc fashion.

3.8 Summary

Mobile ad-hoc network (MANET) is one of the most vibrant and active research fields today. The ad-hoc networking technology has stimulated substantial research activities in the past ten years. It has stretched to numerous issues. Many scholars are attracted to investigate this domain for further research and learning. There exist a lot of problems and challenges in this field due to the frequent and unpredictable topology changes.

This chapter gives an overview of the mobile ad hoc networks, classifying it as a type of wireless network. It also presents the characteristics of MANETS while taking into account the challenges of deploying ad hoc networks at the same time. In the end, it briefly explains the various routing protocols available for MANETs.

Chapter 4

Multimedia and Visual Applications

Multimedia and voice communication over wireless network have been invented and became popular more than a decade. It makes life becomes more convenient, people can easily attain what they needs by these all-in-one tools. But need for more has always been there. People are no longer satisfied with this monotonic communication method

and the simple functions of nowadays mobile phone. As a result of which, many huge vendors believe that videoconferencing will replace the voice communication method in the near future.

This chapter focuses on the multimedia (SMS and MMS) and visual (Audio and Video) applications developed, to work on wired networks, for the PAPAMANETS project. It gives a brief overview of the design and functioning of the applications.

4.1 Types of Communication

There are essentially two types of communication: Multimedia Communications (word processor files, graphics, images) and Visual Communications (audio, video)

Most components of multimedia require data/file transfer, sometimes isochronous with audio or video information (meaning that the data should arrive in time). This type of communication can be characterized as that demanding lossless information transmission while repeat-requests are possible at the same time and having highly bursty traffic.

Audio-video (visual) information, however, is isochronous by definition and can be characterized as the one in which time constraints are severe, so repeat-request on missing data is not possible. However, the data is, in principle, fairly well scalable. This holds especially for video information (spatial and temporal resolution, compression factor). Also video traffic is, either after rate control or after smoothing of a VBR stream, significantly less bursty than audio.

4.3Architecture of the System

The basic architecture of the audio and video conferencing system is illustrated in figure 4.1.

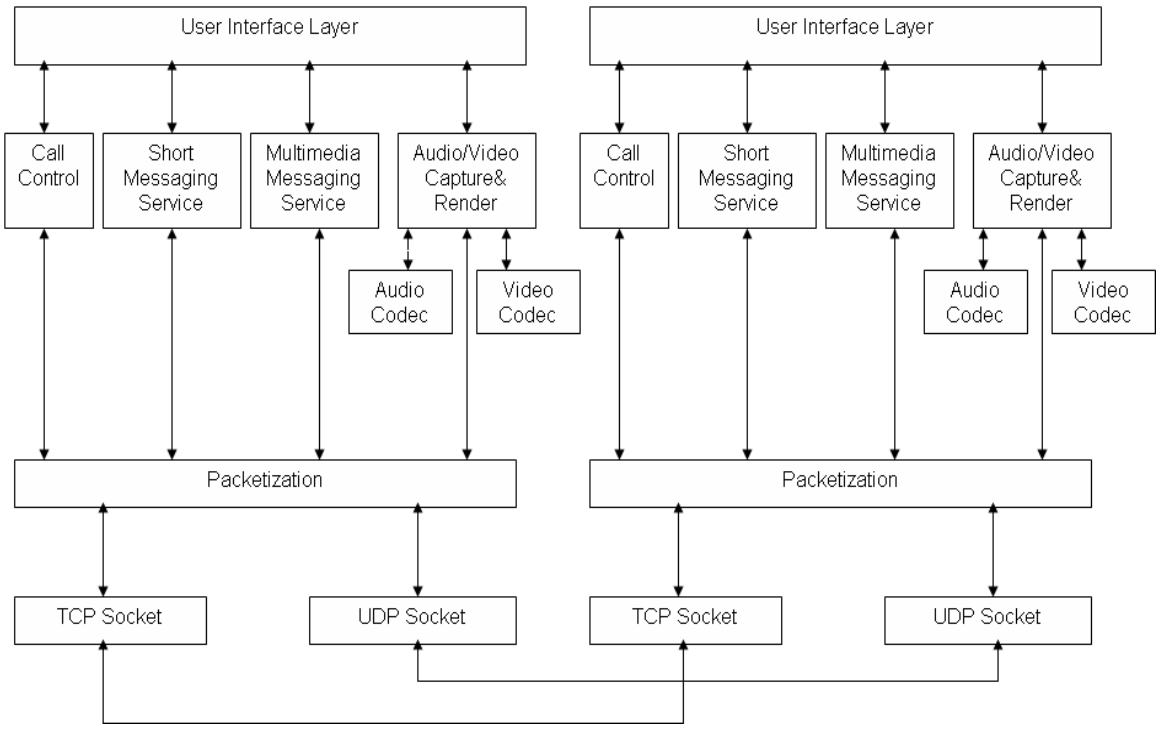

Figure 4.1: Architecture of Multimedia and Visual Applications System

The interface layer interprets user's actions and notifies the corresponding components in the service layer. It also presents various media that are received from the service layer to the user.

The service layer includes four media components and one call control component. The media components are respectively SMS, MMS, audio capturer/renderer and video capturer/renderer. Each of the media components handles a specific media type and its associated devices if any. The media components also perform encoding and

decoding tasks. The call control component sets up the connection between users, supervises the data flow among them, and releases the connection when terminated.

The network layer interacts with the service layer via two buffers, one buffer for reception and one for sending. The TCP socket transmits controlling packets and text packets; the UDP socket transmits the audio/video packets.

4.4Short Message Service (SMS)

SMS is a service for short alphanumeric messages, or in other words, simple text messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender.

In the application developed for the project, the simple text contents of SMS are transferred using socket programming basics which involves connection establishment with the receiver followed by actual transfer of message as bytes. The application is modeled in the project as shown in figure 4.2:

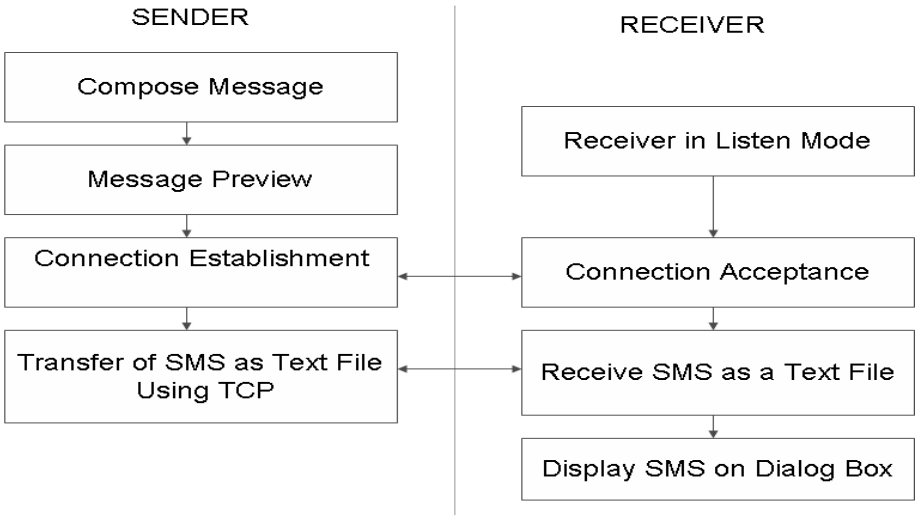

Figure 4.2: Design of SMS Application

4.4 Multimedia Messaging Service (MMS)

Mobile messaging is evolving beyond text by taking a development path from SMS to EMS to MMS. The Multimedia Messaging Service (MMS) allows the sending of messages comprising a combination of text, sounds, images and video to MMS capable handsets.

A multimedia message can be a photo or picture postcard annotated with text and/or an audio clip, a synchronized playback of audio, text, photo or, in the near future, a video emulating a free-running presentation or a video clip. It can also simply be a drawing combined with text.

In the project, the basic strategy followed for the transfer of multiple files at the same time is that all the message contents are sent as one zipped file. The rest details of MMS transfer are the same as that in the case of SMS, involving connection establishment with the receiver, followed by actual message transfer.

The application is modeled in the project as shown in figure 4.3:

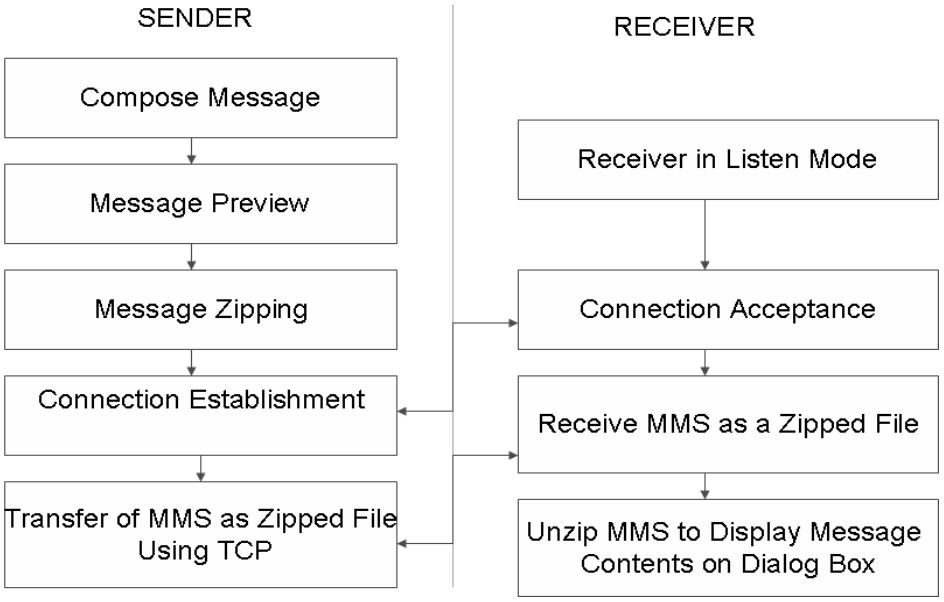

Figure 4.3: Design of MMS Application

4.5 Audio and Video Conferencing

The major problem in video conferencing is that the size of video frames is too big for transmission. Hence the performance is based on the codec used for encoding and decoding the frame. In the project, the h263 Encoder library has been used, which gives better compression rate at high speed.

4.5.1 Recording and Playing Sound

The audio conferencing part has been implemented in the RecordSound and PlaySound classes. A brief overview of how the audio is first recorded and then played on receipt from a remote host is explained in the code snippet in algorithm 4.1.

```
// Create and Start Recorder Thread
```

```
record=new RecordSound(this);
record->CreateThread();
// Create and Start Player Thread
play=new PlaySound1(this);
play->CreateThread();
// Start Recording
record->PostThreadMessage(WM_RECORDSOUND_STARTRECORDING,0,0);
// Start Playing
play->PostThreadMessage(WM_PLAYSOUND_STARTPLAYING,0,0);
// During audio recording , data will be available in OnSoundData callback function
//of RecordSound class.Here you can place your code to send the data to remote host
// To play the data received from the remote host
play>PostThreadMessage(WM_PLAYSOUND_PLAYBLOCK,size,(LPARAM)data);
// Stop Recording
record->PostThreadMessage(WM_RECORDSOUND_STOPRECORDING,0,0);
// Stop Playing
play->PostThreadMessage(WM_PLAYSOUND_STOPPLAYING,0,0);
// At last to Stop the Recording Thread
record->PostThreadMessage(WM_RECORDSOUND_ENDTHREAD,0,0);
// To stop playing thread...
play->PostThreadMessage(WM_PLAYSOUND_ENDTHREAD,0,0);
```

Algorithm 4.1: Algorithm for Audio Recording and Playing

The application is modeled in the project as shown in figure 4.4:

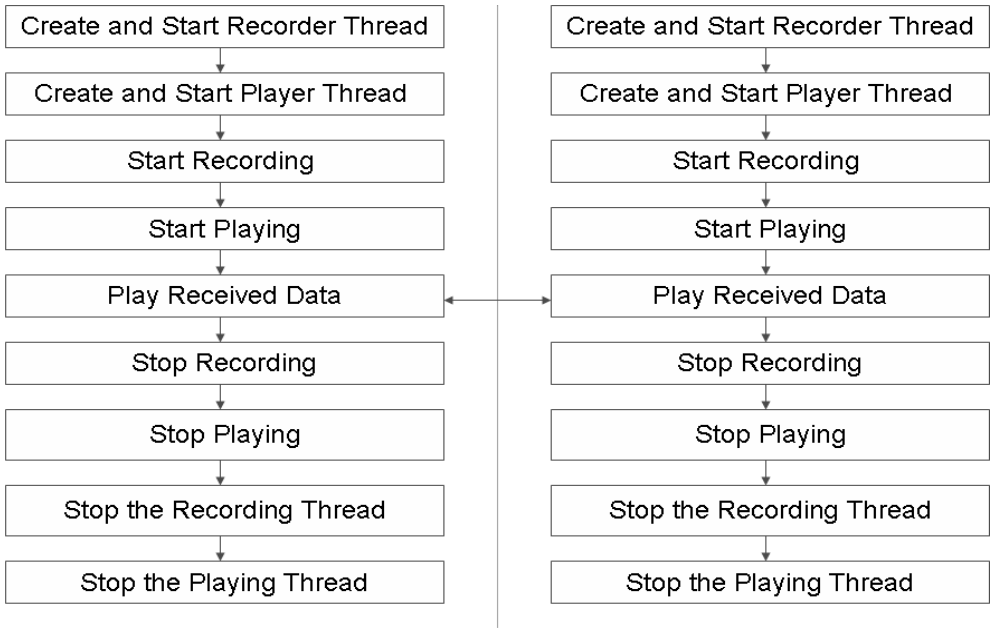

Figure 4.4: Design of Audio Conferencing Application

4.5.2 Video Capture

Video capture is done using VFW (Video for Windows) API. It provides support for capturing the video from web cam. Linking is done through the use of vfw32.lib. VideoCapture.h and VideoCapture.cpp are the files which contain the code for complete video capture process. Figure 4.5 shows the flow chart for video capture.

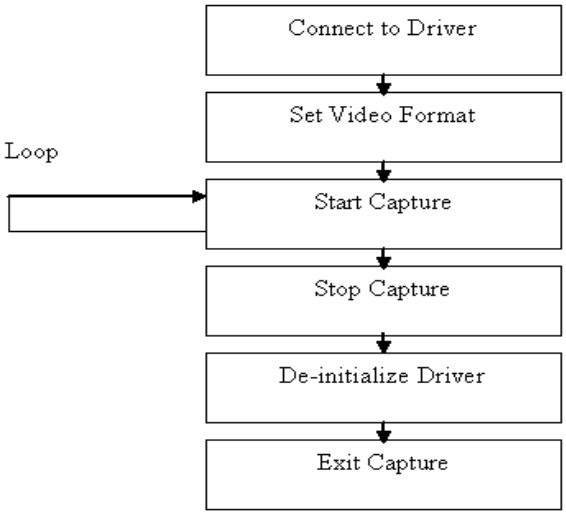

Figure 4.5: Basic steps involved in video capturing

The brief details of the usage of the class in the project are shown in algorithm 4.2.

```
// Create instance of Class
vidcap=new VideoCapture();
// This is used to call display function of main dialog class when frame is captured
vidcap->SetDialog(this);
// This does lot of work including connecting to driver and setting the desired video
//format. Return TRUE if successfully connected to video capture device.
vidcap->Initialize();
// If successfully connected then you can get BITMAPINFO structure associated
//with video format. This is later used for displaying the captured frame...
this->m_bmpinfo=&vidcap->m_bmpinfo;
```

```
// Now start the capture
vidcap->StartCapture();
// Once capture started frames will arrive in callback function "OnCaptureVideo"
//of VideoCapture class.Here you call display function to display the frame.
// To stop the capture
vidcap->StopCapture();
// If your job is over just destroy it
vidcap->Destroy();
```

Algorithm 4.2: Algorithm for Video Capture

4.5.3 Displaying the Captured Video Frame

There are various methods and APIs for displaying the captured frame. The SetDIBitsToDevice() method can be used to directly display the frame. But this is quite slow as it is based on Graphics Device Interface (GDI) functions. The better method is to use DrawDib API to draw the frame. The DrawDib functions provide high performance image-drawing capabilities for device-independent bitmaps (DIBs). DrawDib functions write directly to video memory, hence provide better performance.

A brief view of usage of DrawDib API to display frame is given in algorithm 4.3.

```
// Initialize DIB for drawing
HDRAWDIB hdib=::DrawDibOpen();
// Then call this function will suitable parameters
::DrawDibBegin(hdib,...);
```

```
// Now if you are ready with frame data just invoke this function to displayframe
::DrawDibDraw(hdib,...);
// Finally termination
::DrawDibEnd(hdib);
::DrawDibClose(hdib);
```

Algorithm 4.3: Algorithm for Displaying Captured Video Frames

4.5.4 Encoder Library

H.263 encoder library is used for compression purpose. This library is the modified version of Tmndecoder to make it faster for real time encoding.

A brief view of usage of H263 Encoder library in the video conferencing application is shown in algorithm 4.4.

```
// Initialize the compressor
CParam cparams;
cparams.format = CPARAM_QCIF;
InitH263Encoder(&cparams);
//If you need conversion from RGB24 to YUV420 then call this
InitLookupTable();
// Set up the callback function OwnWriteFunction is the global function called
// during encoding to return the encoded data
WriteByteFunction = OwnWriteFunction;
```

```
// For compression data must be in YUV420 format. Hence before compression
//invoke this method
ConvertRGB2YUV(IMAGE_WIDTH,IMAGE_HEIGHT,data,yuv);
// Compress the frame
cparams.format=CPARAM_QCIF;
cparams.inter = CPARAM_INTRA;
cparams.Q_intra = 8;
cparams.data=yuv; // Data in YUV format
CompressFrame(&cparams, &bits);
// You can get the compressed data from callback function that you have registerd at
//the beginning
// Finally terminate the encoder
ExitH263Encoder();
```

Algorithm 4.4: Algorithm for Compression of Video Frames

4.5.5 Decoder Library

H.263 decoder library is used for decoding the received images. A brief view of H263 decoder library in video conferencing application is given in algorithm 4.5.

```
//Initialize the decoder
InitH263Decoder();
// Decompress the frame. rgbdata must be large enough to hold the output data
```

```
// decoder produces the image data in YUV420 format. After decoding it is
//converted into RGB24 format
DecompressFrame(data,size,rgbdata,buffersize);
// Finaly terminate the decoder
ExitH263Decoder();
```

Algorithm 4.5: Algorithm for Decoding of Compressed Video Frames

The basic design of the application is modeled in figure 4.6:

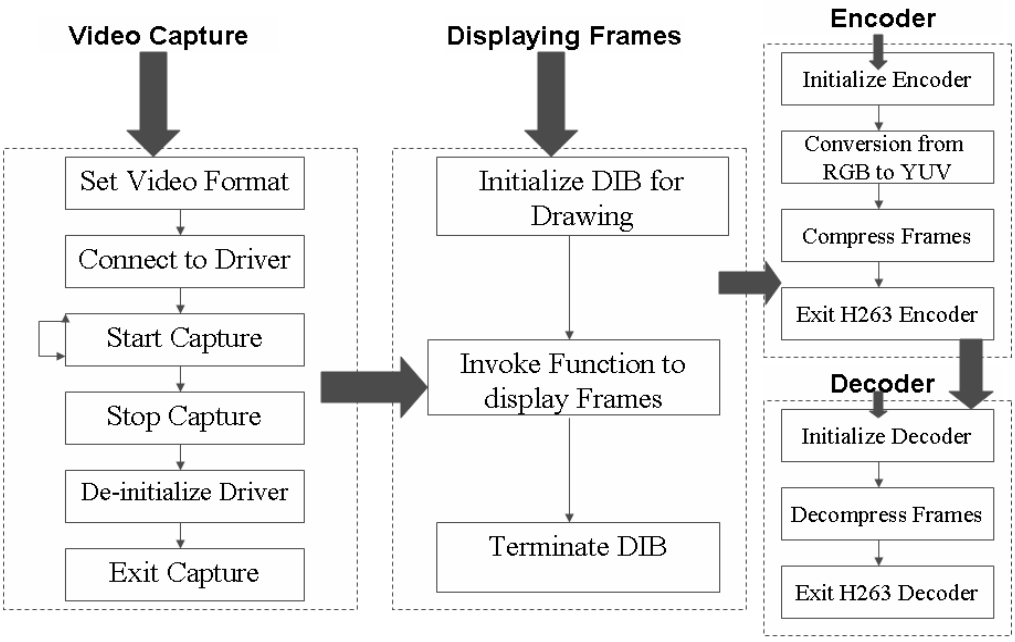

Figure 4.6: Deign of Video Conferencing Application

4.6 Summary

The chapter briefly explains the design of the various multimedia and visual applications used for the project including simple file transfer mechanisms for SMS and MMS and the usage of compression techniques for real time audio and video transfer

Chapter 5

Compression

The H.263 standard, published by the International Telecommunications Union (ITU), supports video compression (coding) for video-conferencing and video-telephony applications.

This chapter describes the concepts and features of H.263 Encoder and Decoder and discusses various issues involved in their implementation.

5.1 Applications

Video conferencing and video telephony have a wide range of applications including: Desktop and Room-based Conferencing, Video over the Internet and over Telephone lines, Surveillance and Monitoring, Telemedicine (medical consultation and diagnosis at a distance), Computer-based Training and Education etc [35].

In each case video information (and perhaps audio as well) is transmitted over telecommunications links, including networks, telephone lines, ISDN and radio. Video has a high "bandwidth" (i.e. many bytes of information per second) and so these applications require **video compression** or **video coding** technology to reduce the bandwidth before transmission.

5.2 Video Coding

Frames of video information are captured at the source and are encoded (compressed) by a video encoder. The compressed "stream" is transmitted across a network or telecommunications link and decoded (decompressed) by a video decoder. The decoded frames can then be displayed [35]. A typical system is shown in the following figure 5.1:

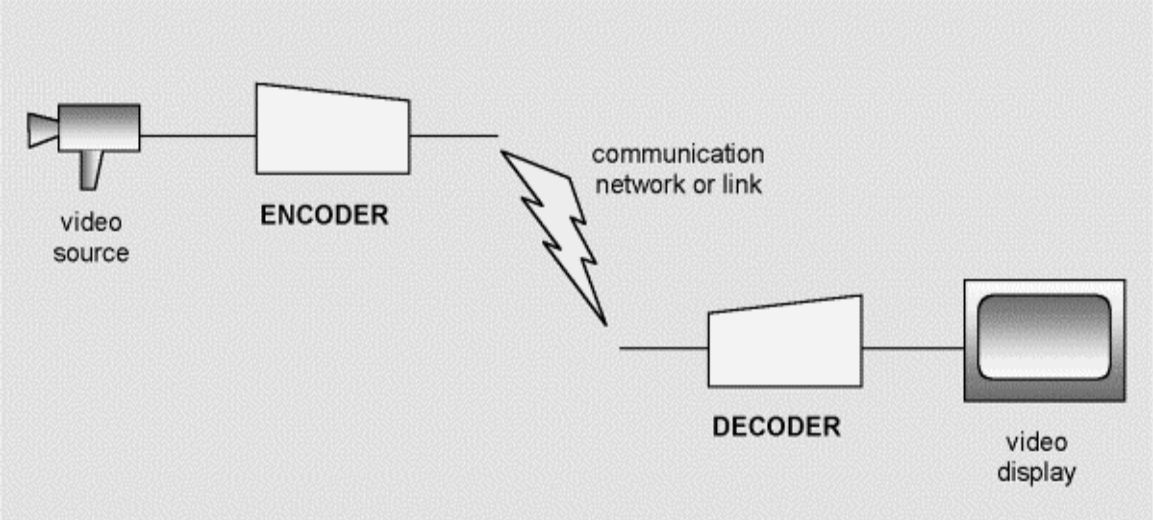

Figure 5.1: A Typical Video Coding System

5.3 The H.263 System

A number of video coding standards exist, each of which is designed for a particular type of application: for example, JPEG for still images, MPEG2 for digital television and H.261 for ISDN video conferencing. H.263 is aimed particularly at video coding for low bit rates (typically 20-30kbps and above).

The H.263 standard specifies the requirements for a video encoder and decoder. It does not describe the encoder or decoder themselves: instead, it specifies the format and

content of the encoded (compressed) stream. A typical encoder and decoder are described here. We have "skipped" many of the details of the H.263 standard such as syntax and coding modes.

5.4 H.263 Encoder

This section gives a brief overview of the various components involved in an H.263 encoder. A typical H.263 Encoder with its various components is represented in figure 5.2 [36].

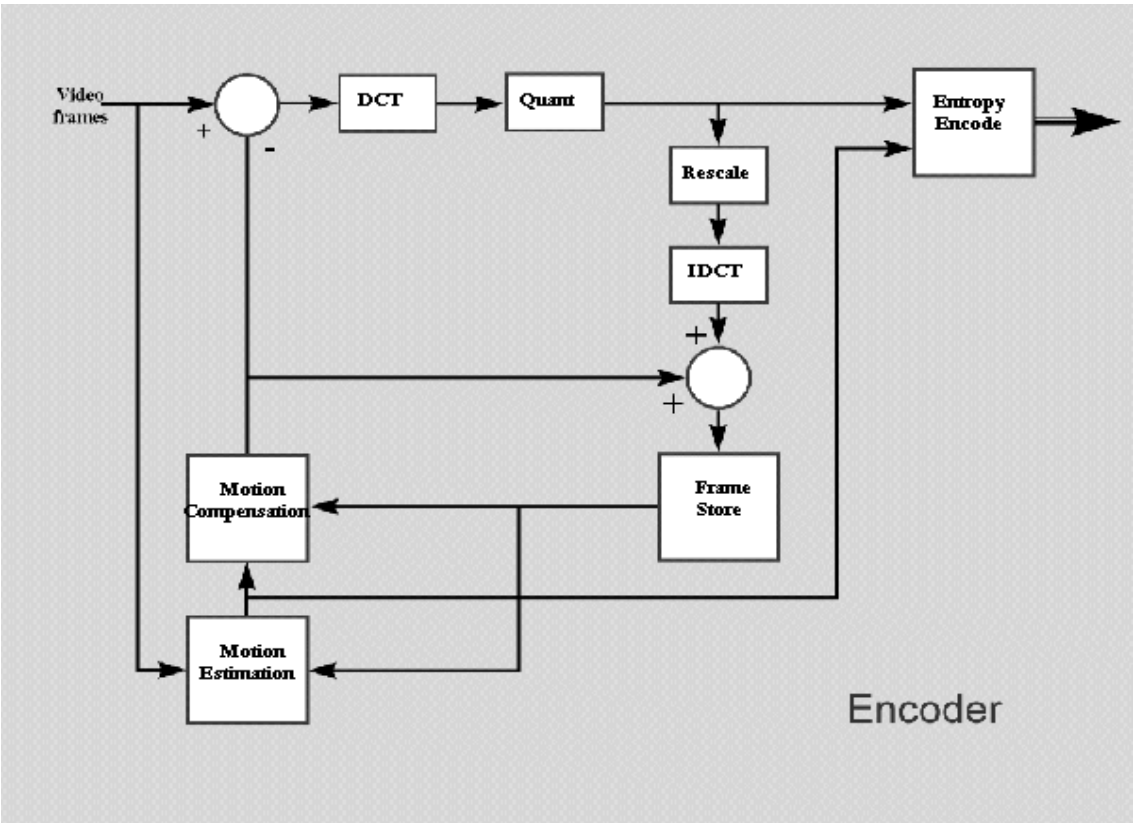

Figure 5.2: H.263 Encoder

5.4.1 Motion Estimation and Compensation

The first step in reducing the bandwidth is to subtract the previous transmitted frame from the current frame so that only the difference or residue needs to be encoded and transmitted. This means that areas of the frame that do not change (for example the background) are not encoded. Further reduction is achieved by attempting to estimate where areas of the previous frame have moved to in the current frame (**motion estimation**) and compensating for this movement (**motion compensation**). The motion estimation module compares each 16x16 pixel block (**macroblock**) in the current frame with its surrounding area in the previous frame and attempts to find a match. The matching area is moved into the current macroblock position by the motion compensator module. The motion compensated macroblock is subtracted from the current macroblock. If the motion estimation and compensation process is efficient, the remaining "residual" macroblock should contain only a small amount of information [36].

5.4.2 Discrete Cosine Transform (DCT)

The DCT transforms a block of pixel values (or residual values) into a set of "spatial frequency" coefficients. This is analogous to transforming a time domain signal into a frequency domain signal using a Fast Fourier Transform. The DCT operates on a 2-dimensional block of pixels (rather than on a 1-dimensional signal) and is particularly good at "compacting" the energy in the block of values into a small number of coefficients. This means that only a few DCT coefficients are required to recreate a recognizable copy of the original block of pixels.

5.4.3 Quantization

For a typical block of pixels, most of the coefficients produced by the DCT are close to zero. The quantizer module reduces the precision of each coefficient so that the near-zero coefficients are set to zero and only a few significant non-zero coefficients are left. This is done in practice by dividing each coefficient by an integer scale factor and truncating the result. It is important to realize that the quantizer "throws away" information.

5.4.4 Entropy Encoding

An entropy encoder (such as a Huffman encoder) replaces frequently occurring values with short binary codes and replaces infrequently occurring values with longer binary codes. The entropy encoding in H.263 is based on this technique and is used to compress the quantized DCT coefficients. The result is a sequence of variable-length binary codes. These codes are combined with synchronization and control information (such as the motion "vectors" required to reconstruct the motion-compensated reference frame) to form the encoded H.263 bitstream.

5.4.5 Frame Store

The current frame must be stored so that it can be used as a reference when the next frame is encoded. Instead of simply copying the current frame into a store, the quantized coefficients are re-scaled; inverse transformed using an Inverse Discrete Cosine Transform and added to the motion-compensated reference block to create a reconstructed frame that is placed in a store (the **frame store**). This ensures that the contents of the frame store in the encoder are identical to the contents of the frame store

in the decoder (figure 5.3). When the next frame is encoded, the motion estimator uses the contents of this frame store to determine the best matching area for motion compensation.

5.5 H.263 Decoder

The figure 5.3 describes a typical H.263 Decoder with various components [37].

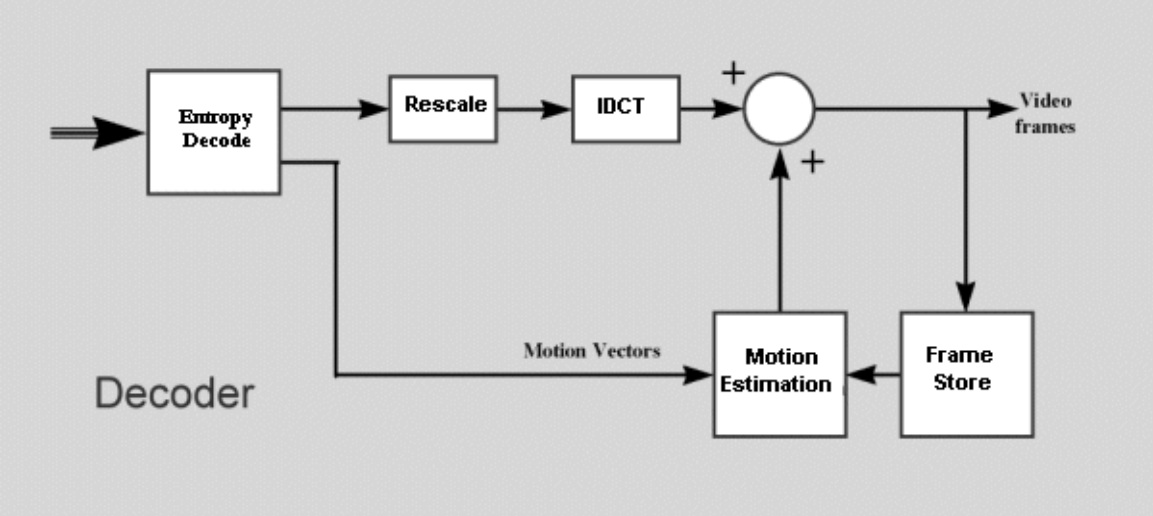

Figure 5.3: H.263 Decoder

5.5.1 Entropy Decode

The variable-length codes that make up the H.263 bitstream are decoded in order to extract the coefficient values and motion vector information.

5.5.2 Rescale

This is the "reverse" of quantization: the coefficients are multiplied by the same scaling factor that was used in the quantizer. However, because the quantizer discarded

the fractional remainder, the rescaled coefficients are not identical to the original coefficients.

5.5.3 Inverse Discrete Cosine Transform

The IDCT reverses the DCT operation to create a block of samples: these (typically) correspond to the difference values that were produced by the motion compensator in the encoder.

5.5.4 Motion Compensation

The difference values are added to a reconstructed area from the previous frame. The motion vector information is used to pick the correct area (the same reference area that was used in the encoder). The result is a reconstruction of the original frame: note that this will not be identical to the original because of the "lossy" quantization stage, i.e. the image quality will be poorer than the original. The reconstructed frame is placed in a frame store and it is used to motion-compensate the next received frame.

5.6 Implementation Issues

Many issues need to be addressed in order to develop a video encoder and decoder that can operate effectively in real time. These include:

5.6.1 Bit Rate Control

Practical communications channels have a limit to the number of bits that they can transmit per second.

In many cases the bit rate is fixed (constant bit rate or CBR, for example POTS, IDSN, etc.).

The basic H.263 encoder generates a variable number of bits for each encoded frame. If the motion estimation/compensation process works well then there will be few remaining non-zero coefficients to encode. However, if the motion estimation does not work well (for example when the video scene contains complex motion), there will be many non-zero coefficients to encode and so the number of bits will increase.

In order to "map" this varying bit rate to (say) a CBR channel, the encoder must carry out **rate control**. The encoder measures the output bit rate of the encoder. If it is too high, it increases the compression by increasing the quantizer scale factor: this leads to more compression (and a lower bit rate) but also gives poorer image quality at the decoder. If the bit rate drops, the encoder reduces the compression by decreasing the quantizer scale factor, leading to a higher bit rate and a better image quality at the decoder.

5.6.2 Synchronization

The encoder and decoder must stay in synchronization, particularly if the video signal has accompanying audio. The H.263 bitstream contains a number of "headers" or markers: these are special codes that indicate to a decoder the position of the current data within a frame and the "time code" of the current frame. If the decoder loses synchronization then it can "scan" forward for the next marker in order to resynchronize and resume decoding. It should be noted that even a brief loss of synchronization can

cause severe disruption in the quality of the decoded image and so special care must be taken when designing a video coding system to operate in a "noisy" transmission environment [37].

5.6.3 Audio and Multiplexing

The H.263 standard describes only video coding. In many practical applications, audio data must also be compressed, transmitted and synchronized with the video signal. Synchronization, multiplexing and protocol issues are covered by "umbrella" standards such as H.320 (ISDN-based videoconferencing), H.324 (POTS-based videotelephony) and H.323 (LAN or IP-based videoconferencing). H.263 (or its predecessor, H.261) provide the video coding part of these standards groups. Audio coding is supported by a range of standards including G.723.1. Other, related standards cover functions such as multiplexing (e.g. H.223) and signaling (e.g. H.245).

5.7 Summary

The chapter briefly explains the design of the H.263 Encoder and Decoder, used in PAPAMANETs, with serves the compression purpose for the efficient transmission of video frames over wireless. The compression issue is particularly important in the case of ad hoc network where the available bandwidth, as compared to fixed networks, is very small.

Chapter 6

Routing

A mobile ad hoc network (MANET) is a collection of nodes, which are able to connect via a wireless medium forming a dynamic network. These nodes may appear and disappear anytime within the network. This implies that the network topology is constantly changing and the network traffic may be routed between nodes in order for communication to occur.

This chapter focuses on the OLSR i.e. Optimized Link State Routing Protocol for MANETS. It gives a brief overview of the design and functioning of the protocol.

6.1 Classification of Routing Protocols

Currently, several types of routing protocols exist. They can be classified generally as table-driven, on-demand or hybrid protocols shown in figure 6.1. [38]

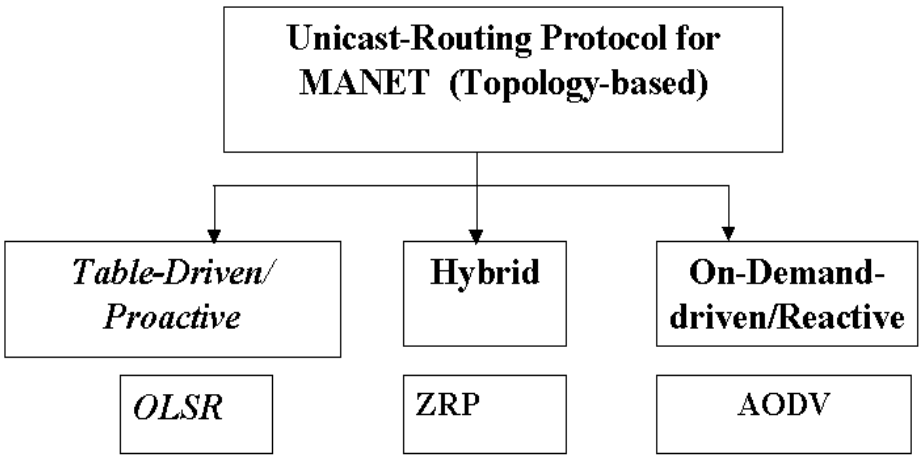

Figure 6.1: Classification of Routing Protocols

Table–driven protocols are characterized by all nodes constantly updating routes to all reachable nodes in their routing tables. On-demand protocols are characterized by nodes seeking routes only when there is data to be transmitted to the destination. Hybrid protocols, as the name implies, attempt to combine the advantages of both table-driven and on-demand protocols. Since we are dealing with time critical applications i.e. real time audio and video conferencing so the delay in on-demand routing protocols is undesirable. Taking this major point into consideration, we have decided to stick to table driven proactive protocol i.e. OLSR.

6.2 Optimized Link State Routing Protocol

6.2.1 Introduction

The Optimized Link State Routing Protocol (OLSR) is developed for mobile ad hoc networks. It operates as a table driven, proactive protocol, i.e., exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR). In OLSR, only nodes, selected as such MPRs, are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required [39].

Nodes, selected as MPRs, also have a special responsibility when declaring link state information in the network. Indeed, the only requirement for OLSR to provide shortest path routes to all destinations is that MPR nodes declare link-state information

for their MPR selectors. Additional available link-state information may be utilized, e.g., for redundancy [39].

Nodes which have been selected as multipoint relays by some neighbor node(s) announce this information periodically in their control messages. Thereby a node announces to the network, that it has reachability to the nodes, which have selected it as an MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. Furthermore, the protocol uses the MPRs to facilitate efficient flooding of control messages in the network.

A node selects MPRs from among its one hop neighbors with "symmetric", i.e., bi-directional, linkages. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over uni-directional links (such as the problem of not getting link-layer acknowledgments for data packets at each hop, for link-layers employing this technique for unicast traffic. OLSR is developed to work independently from other protocols. Likewise, OLSR makes no assumptions about the underlying link-layer.

6.2.2 Applicability

OLSR is a proactive routing protocol for mobile ad-hoc networks (MANETs). It is well suited to large and dense mobile networks, as the optimization achieved using the MPRs works well in this context. The larger and more dense a network, the more optimization can be achieved as compared to the classic link state algorithm. OLSR uses hop-by-hop routing, i.e., each node uses its local information to route packets [40].

OLSR is well suited for networks, where the traffic is random and sporadic between a larger set of nodes rather than being almost exclusively between a small specific set of nodes. As a proactive protocol, OLSR is also suitable for scenarios where the communicating pairs change over time: no additional control traffic is generated in this situation since routes are maintained for all known destinations at all times.

6.2.3 Protocol Overview

OLSR is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks.

OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs, to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes. The minimal set of link state information required is, that all nodes, selected as MPRs, MUST declare the links to their MPR selectors. Additional topological information, if present, MAY be utilized e.g., for redundancy purposes [41].

OLSR may optimize the reactivity to topological changes by reducing the maximum time interval for periodic control message transmission. Furthermore, as OLSR continuously maintains routes to all destinations in the network, the protocol is beneficial for traffic patterns where a large subset of nodes are communicating with another large

subset of nodes, and where the [source, destination] pairs are changing over time. The protocol is particularly suited for large and dense networks, as the optimization done using MPRs works well in this context. The larger and more dense a network, the more optimization can be achieved as compared to the classic link state algorithm.

OLSR is designed to work in a completely distributed manner and does not depend on any central entity. The protocol does NOT REQUIRE reliable transmission of control messages: each node sends control messages periodically, and can therefore sustain a reasonable loss of some such messages. Such losses occur frequently in radio networks due to collisions or other transmission problems.

Also, OLSR does not require sequenced delivery of messages. Each control message contains a sequence number, which is incremented for each message. Thus the recipient of a control message can, if required, easily identify which information is more recent - even if messages have been re-ordered while in transmission [42].

Furthermore, OLSR provides support for protocol extensions such as sleep mode operation, multicast-routing etc. Such extensions may be introduced as additions to the protocol without breaking backwards compatibility with earlier versions.

OLSR does not require any changes to the format of IP packets. Thus any existing IP stack can be used as is: the protocol only interacts with routing table management.

6.2.4 Multipoint Relays

The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same region. Each node in the network selects a set of nodes in its symmetric 1-hop neighborhood which may retransmit its messages. This set of selected neighbor nodes is called the "Multipoint Relay" (MPR) [43].

6.2.5 Functioning

6.2.5.1 Neighbor Sensing (HELLO messages)

In order to understand how OLSR determines the network topology, there are several terminologies that need to be clarified. First and foremost, the term neighbour sensing refers to the process when any node attempts to find out which other nodes are within its neighborhood. By neighborhood, we are referring to the set of nodes which there exists a direct link over which data can be transmitted. A link can be characterized by the direction of the communication. Suppose a node A can only send data to another node B but B cannot send data to A, the link is said to be **asymmetric**. On the other hand, if A can communicate with B and B can also communicate with A, then the link is said to be **symmetric**. Furthermore, if the link between A and B is symmetric, B is said to be the symmetric neighbour of A and vice versa [44].

In OLSR, there is also the concept of the two-hop neighbour. A node C is considered to be a two-hop neighbour of a when C is a symmetric neighbour of B and B is also a symmetric neighbour of A (A not being C). In this case, a symmetric link exists between A and B, B and C but not between A and C (figure 6.2).

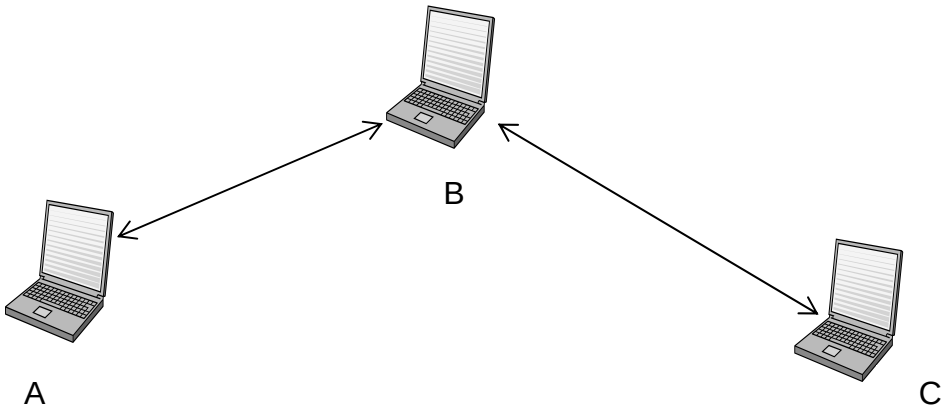

Figure 6.2: C is the two-hop neighbour of A

The neighbour sensing mechanism in OLSR is designed to work in this way: each node broadcasts periodically a HELLO message that contains the list of neighbours which are at that moment known to the node, as well as the status of the link (symmetric or asymmetric) to those nodes. Whenever a node receives a HELLO message, it is able to obtain information about its neighbourhood, two-hop neighbourhood as well as the link status between the neighbouring nodes. In the example above, if node a sees its own address in node B's HELLO message, then it will deduce that the link is symmetric.

Each node maintains a neighbour table storing information about its neighbours and its two-hop neighbours. Each entry in the table has a validity period, during which it is constantly being refreshed to remain valid, or after which it expires and is automatically removed from the table.

6.2.5.2 MPR Selection (Flooding)

After each node has completed its process of neighbour sensing, it still does not have enough to compute routing information to all reachable destinations in the network as the neighbour table only provides information of nodes at most two hops away. Another method is necessary to reliably transmit local topological information, in the form of control traffic messages, to all other nodes [44].

However, as in the case of all wireless communications, the bandwidth resource is limited. Too much control traffic overhead will be very costly and should be kept to a minimum. There is also another problem due to the unreliable nature of wireless communications – packets may be lost when transmissions collide or when routers fail. A method of relaying information to all other nodes with a high probability of success must thus be used.

Any method to diffuse control traffic messages must satisfy certain conditions. Firstly, the message must be able to reach all other nodes. Secondly, duplicated retransmissions must be reduced. A simple flooding mechanism, whereby any control traffic message received on one interface is retransmitted out on all other interfaces, satisfies the first condition but not the second. A node might receive the same message from multiple neighbours (figure 6.3a). Multiple retransmissions also result in higher probability of message loss due to collisions between messages over the wireless medium.

As a result, any method to diffuse control traffic messages must satisfy certain conditions. Firstly, the message must be able to reach all other nodes. Secondly,

duplicated retransmissions must be reduced. A simple flooding mechanism, whereby any control traffic message received by one node is retransmitted out on all other neighbouring nodes, satisfies the first condition but not the second. A node might receive the same message from multiple neighbours (figure 6.3a). Multiple retransmissions also result in higher probability of message loss due to collisions between messages over the wireless medium [45].

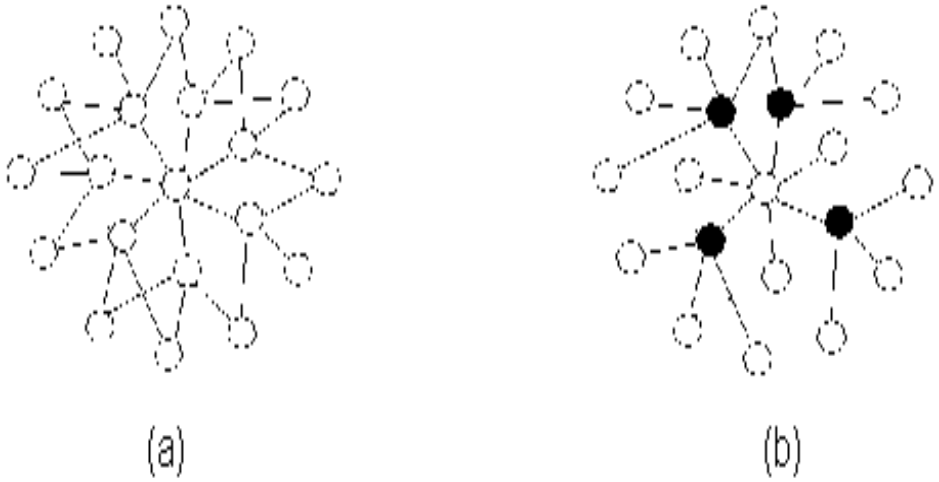

Figure 6.3 – (a) Simple Flooding Mechanism, (b) Flooding Using MPR Mechanism

OLSR introduces another form of flooding mechanism called MPR-flooding that aims to minimize the problems related to duplicate reception of a message within a region. The mechanism works in the following way: first, a set of nodes is selected from a node's symmetric neighbours. These nodes are called multipoint relays (MPRs). The node that selects this set of MPRs is called the MPR Selector. The function of the MPR is to forward the flooded message from its MPR Selector. In the example in figure 6.2, node A's flooded message will only be retransmitted by node B to node C if and only if B is

the MPR of A (or A is the MPR Selector of B). As shown in figure 6.3 (b), by correctly choosing the set of MPRs (nodes that are shaded), the number of retransmissions can be greatly reduced. Furthermore, to reduce the number of control messages flooded into the network, only MPRs generate control messages. Finally, another optimization is done in OLSR – MPRs only declare links with their MPR selectors in their control traffic. The size of the control traffic in OLSR will be smaller than that of pure link state routing protocols.. All nodes will select their individual set of MPRs independently, using probably similar or different heuristics to select a minimal set of MPRs.

The main concept used is: (i) the degree of a symmetric neighbour y of a node x, D(y), is the number of symmetric neighbours y has, excluding the symmetric neighbours of x currently performing the MPR selection and x itself, (ii) any symmetric neighbour of a node is chosen as a MPR if that neighbour is the only neighbour of a two-hop neighbour.

Starting with an empty MPR set, the symmetric neighbours that are the only neighbours of some nodes in the two-hop neighbourhood are chosen as MPR and placed into the MPR set. The two-hop neighbours are then not considered in the later calculations. The degrees, D(y), of all symmetric neighbours are then calculated for the remaining two-hop neighbours that are not covered. While there are still some nodes in the two-hop neighbourhood not covered by nodes in the MPR set, the symmetric neighbour with the highest degree is chosen as MPR. This ensures that the MPR set is optimal, i.e. the resulting number of duplicate message transmission is minimal. The

current node is then the MPR Selector of these MPRs. Figure 6.4 illustrates a step-by-step example of MPR selection.

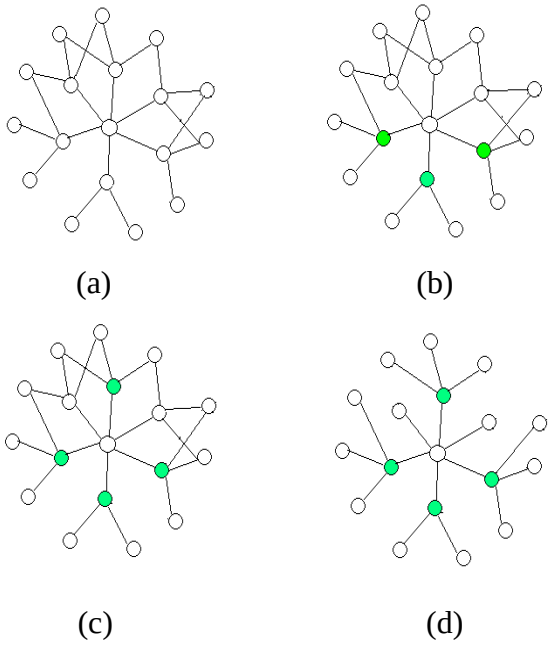

Figure 6.4 – (a) Before MPR Selection (b) Symmetric Neighbour that is the only neighbour of some nodes in the two-hop neighbourhood is chosen (c) Select Symmetric Neighbour with the highest degree (d) After MPR Selection

The purpose of the second step selection of symmetric neighbours that are the only neighbours of some nodes in the two-hop neighbourhood as MPR) is to optimize the MPR set. Without this step, the MPR set can still be calculated with success, i.e. all two-hop neighbours will be eventually covered. However, this step helps to reduce the number of recursive calls for the third step by removing those covered two-hop neighbours from consideration before the third step is performed.

6.2.5.3 Topology Control (TC) Message Broadcast and Processing

During the topology discovery phase, multipoint relays (MPRs) are used to disseminate topology information through the network. This topology information will allow each node to evaluate routes to destinations in the network. Each node that has been selected as an MPR by its neighbour node will create and broadcast Topology Control (TC) messages to all its 1-hop neighbour nodes. MPRs also retransmit to its 1-hop neighbours the TC messages it received that were created by nodes within its MPR Selector Set [46]. A TC message contains the list of neighbours that have selected the sender node as a MPR and a MPR Selector Sequence Number (MSSN). MSSN is a sequence number that allows nodes to keep track of the most recent topological information. For every new TC message created, this number is incremented to indicate a change in the MPR Selector Set (i.e. list of neighbors that have selected the sender node as an MPR). The format of a TC message is shown in figure 6.5.

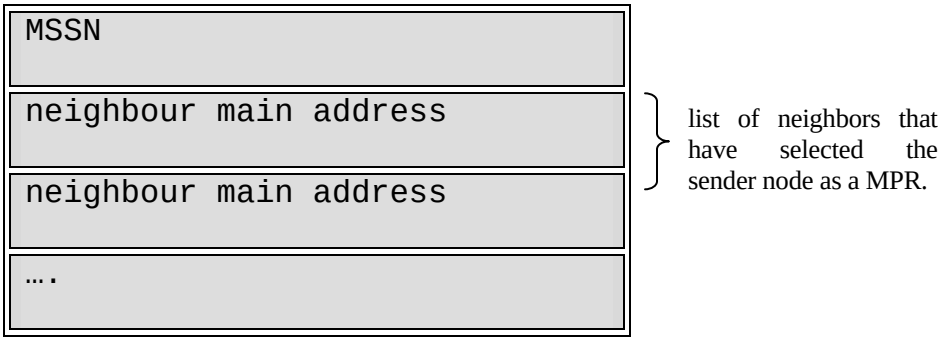

Figure 6.5: Format of TC Message

Each node in the network maintains a topology table, in which it records the topological information about the network retrieved from the TC messages received.

6.2.5.4 Routing Table Calculation

Each node in the network maintains a routing table, in which it records the routing information that allows it to route data destined for other nodes in the network. The routing table is calculated using the information in the neighbour table of the node that has been determined through the flooding of HELLO messages and the topological information recorded in the topology table that has been determined through the flooding of TC messages [47].

The routing table is constantly updated to reflect changes in the topology table and the neighbour table. That is, the routing table will be updated when a neighbour appear or disappear or when new topology table entries are added or existing topology table entries removed. All destinations in the network with a known route will be recorded in the routing table.

Each routing table entry consists of the destination (R_dest), the next hop to the destination (R_next) and number of hops to the destination (R_dist). Sample routing table at a node is shown in figure 6.6.

1.	R_dest	R_next	R_dist
2.	R_dest	R_next	R_dist
.	…	..	..

Figure 6.6: Sample Routing Table

Shortest path algorithm is adopted during route evaluation. Whenever the routing table is recalculated, all the routing table entries are initially removed. New routing table entries are recorded in the table starting with one-hop neighbors as destination nodes

(R_dest). Next, the following process is executed beginning with number of hops, h =1 and each time incrementing the value of h by 1. For each topology table entry, if its destination address (T_dest) does not correspond to R_dest of any routing table entry and its address of the last hop to the destination (T_last) corresponds to R_dest of a routing table entry whose R_dist is equal to h, then a new routing table entry is inserted with: R_dest set to T_dest, R_next set to R_next of the routing table entry whose R_dest is equal to T_last of the topology table entry; and R_dist is set to h+1. The execution stops when no new entry is inserted within an iteration of the process [48].

6.2.6 Structure of OLSR Network

MPRs form **routing backbone** in the network while other nodes act as “hosts”. The information is transferred from the source to the destination with the help of MPRs in between. The figure below depicts this scenario that whenever a node wants to send some piece on information to the other node it will be either directly (if that node comes in its direct range) or indirectly with the help of MPRs that come in between them [49].

As nodes move, since all nodes are mobile and they can move quite often, so topological relationships change, Routes change Backbone shape and composition changes. The same node (fig 6.7) will then send the required information with the help of other routers i.e. MPRs forming another route in the network, shown in fig 6.8, so the network of MANET should be densely populated with nodes for reliable and successful communication.

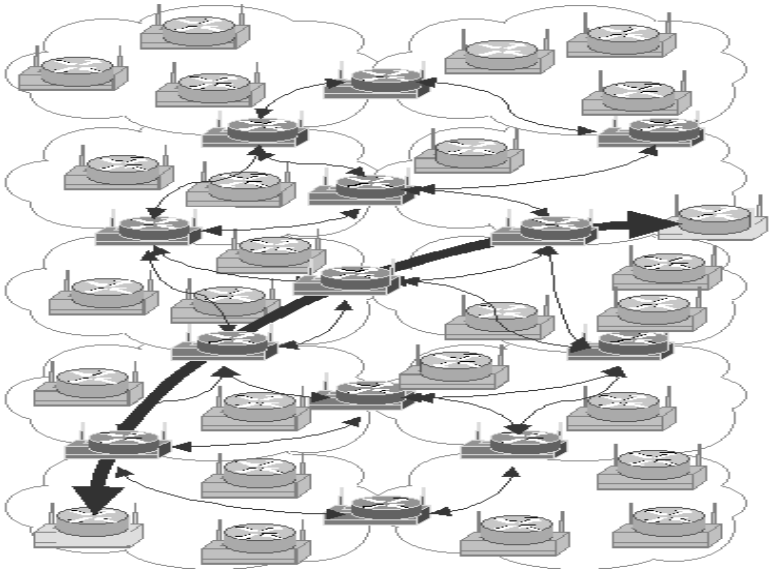

Figure 6.7: MPRs as Routing Backbone

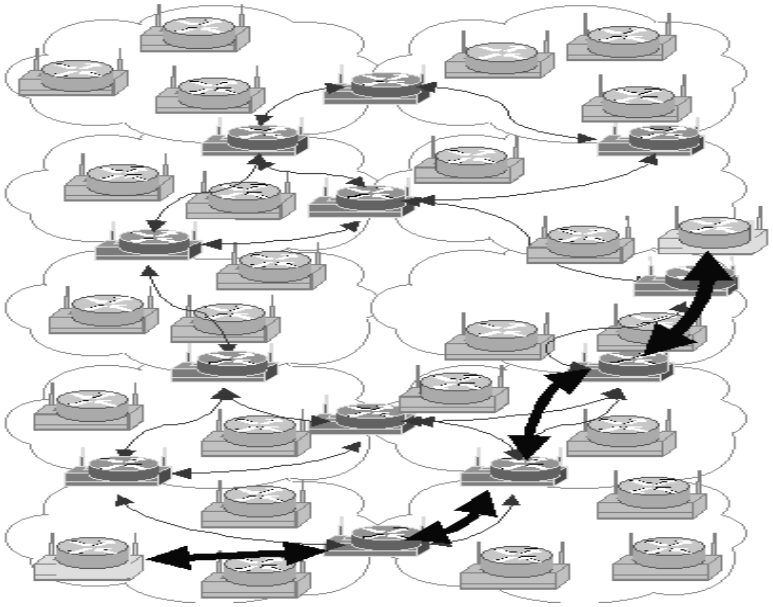

Figure 6.8: New Route as Nodes Move

6.3 Summary

This chapter clearly explains the Optimized Link State Routing Protocol, which is a table-driven proactive protocol used for routing in PAPAMANET. OLSR is discussed in detail with a focus on its working and its structure.

Chapter 7

PAPAMANETS Plugins

As MANETs are an area for research and development, the ability to add extensions or change normal operation in implementations of routing protocols for such networks, provides a great way of testing new solutions.

The MPR flooding and default forwarding algorithm used in OLSR makes this protocol very interesting to extend. Normal MANET routing suffers from lack of broadcast and multicast solutions. By letting OLSR carry traffic, one can provide a broadcast solution that is optimized. The OLSR daemon will then work as a flooding

relay agent for local applications. Already existing services that require a broadcast mechanism can be used in a MANET routed by OLSR if using an OLSR plugin to flood broadcasted traffic. Such services include domain name service (DNS), service discovery mechanisms and key distribution schemes. Other interesting extensions can be updating OLSR parameters at runtime, based on traffic analysis, or creating visualizations of the network topology.

As modularity was one of the main goals when designing and implementing OLSR, the idea of easily extending the protocol led to the design of a plugin interface. In this chapter this interface, areas of usage and the plugin implementations for PAPAMANETS are covered.

7.1 Plugins

OLSR supports loading of dynamically linked libraries, called *plugins*, for generation and processing of private package-types and any other custom functionality. A dynamically loadable library (DLL) is a piece of executable code that contains functions and data. Unlike normal executables, DLLs are not “fully” linked after compilation. They are set up in a way that allows the actual linking to take place at runtime. An application can load and run functions from a DLL dynamically, therefore the library is said to be dynamically linked.

One of the big advantages of DLLs is that they can be used simultaneously by multiple processes; still only one instance of the library will be maintained in memory. These type of DLLs are typically libraries of functions shared by many processes. An

example would be a Graphical User Interface (GUI) library. This is however not something taken advantage of when using DLLs as *plugins*. Plugins provide new functions to an existing application without altering the original application. An illustration of this is shown in figure 7.1. OLSR uses DLLs in this fashion.

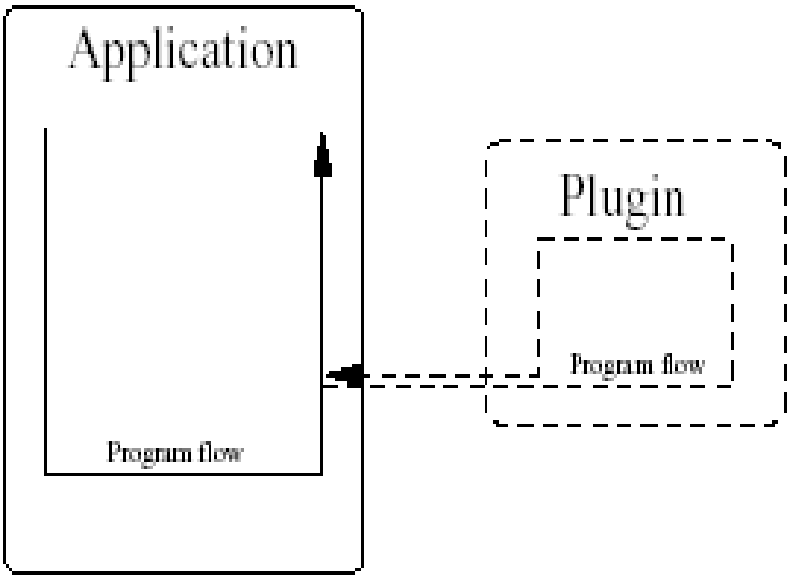

Figure 7.1: A Plugin intercepts an Application and adds its own Program Flow

DLL functionality exists for all common operating systems. In Linux they are known as *.so* files while in Microsoft Windows they are known as *.DLL* files.

7.1.1 OLSR Plugins

The plugin design was chosen for amongst others for a number of reasons. Primarily because there is no need to change any code in the OLSR daemon to add custom packages or functionality. Secondly, users are free to implement OLSR plugins

and license them under whatever terms they like. Plugins can be written in any language that can be compiled as a dynamic library. No need for people using extended OLSR functionality to rely on heavy patching to maintain functionality when new OLSR versions are released. The plugin interface will always be backwards compatible.

OLSR provides a default forwarding algorithm that allows for forwarding of OLSR messages of unknown types. This means that even if only a subset of the nodes in the network actually knows how to interpret a certain message-type, all nodes will forward them according to the MPR scheme. A wide variety of services designed for wired network environments rely on net-wide broadcasts. Services that needs to broadcast/multicast data can encapsulate data in a private OLSR message-type using an OLSR plug-in as illustrated in figure 7.2.

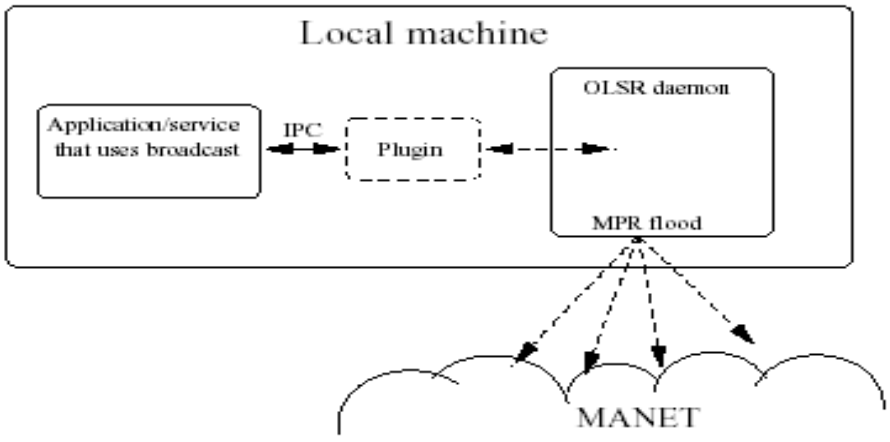

Figure 7.2: A Plugin uses OLSR Daemon to work as a Relay for Broadcasting

The design of the various entities of OLSR allows one to easily add special functionality into most aspects of the program. One can both register and unregister

functions with the socket parser, packet parser and scheduler, and one can update many variables; manipulate incoming and outgoing traffic and more. This opens up for possibilities like intercepting current operation and replacing it with custom actions. As an example, a plugin can provide its own HELLO message generation and parser functions. The plugin can unregister the default functions used by OLSR and replace them with its own. This relationship is illustrated in figure 7.3.

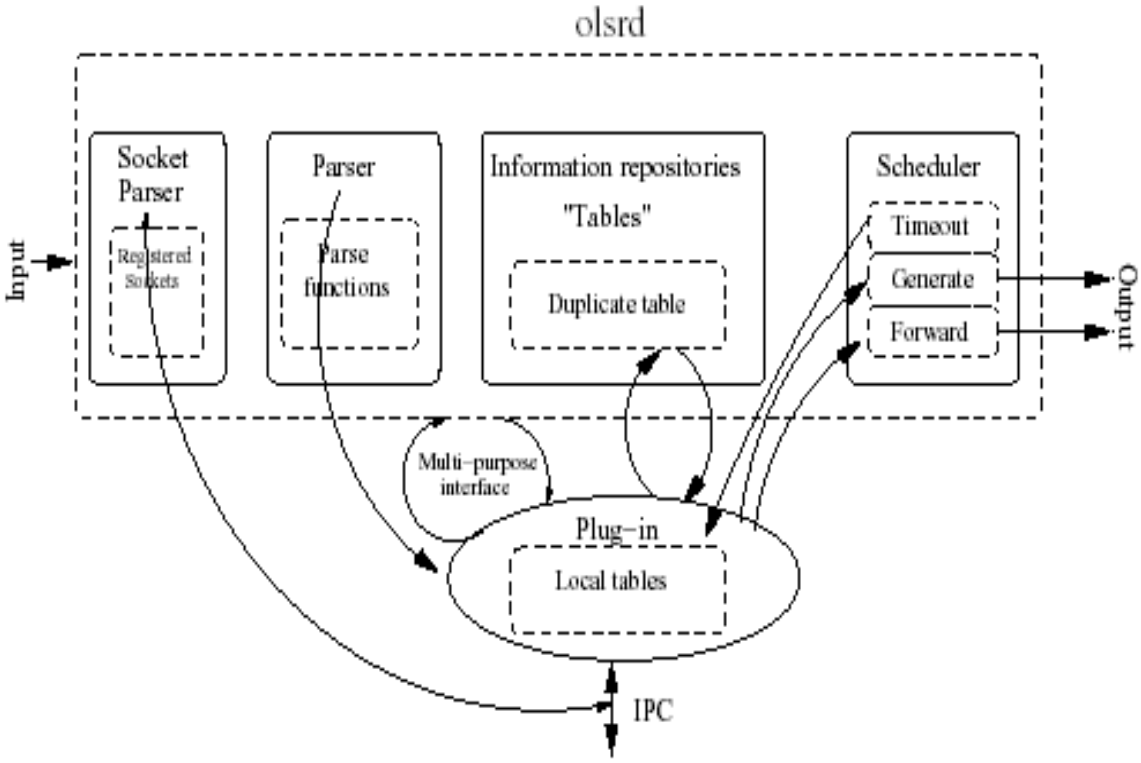

Figure 7.3: A Plugin can manipulate virtually every part of the OLSR Daemon

The modular design of OLSR really shows its strengths when dealing with plugins. A plugin can do things like establishing blocking sockets for communication of

its own, without blocking OLSR operation. This is because the plugin can register its sockets with the socket parser in OLSR.

7.2 The Plugin Interface

For a plugin scheme like this to work, one needs a well defined and easy-to-expand interface for communication between the OLSR daemon and the plugin. The interface should be well defined so that a plugin always knows what to expect from the daemon, and the daemon always knows what to expect from the plugin within some given set of functions. Still, the design should be flexible enough to allow for extending the functionality while keeping backwards compatibility.

The actual data that must be set up between the application and the plugin are pointers to variables and functions. The OLSR plugin interface is mainly based upon the function:

```
int
plugin_io(int cmd, void *data, size_t size);
```

In this function, one passes a command and a pointer to some allocated memory and the size of the allocated memory area. The return value indicates success or error, while actual data is put or read from the memory buffer pointed to by **data*. This function is implemented in src/plugin.c. The function is in reality just a big *switch* statement. All defined commands must be implemented as a *case* statement in this switch. The command **GETF__OLSR_REGISTER_SCHEDULER_EVENT,** for

example, retrieves a pointer to the **olsr_register_scheduler_event** which is used to register an event with the OLSR scheduler. The case statement, implemented in plugin.c, takes care of setting up the pointer to the function, as shown in algorithm 7.1.

```
case(GETF__OLSR_REGISTER_SCHEDULER_EVENT):
    ptr = &olsr_register_scheduler_event;
    memcpy(data, &ptr, size);
    break;
```

Algorithm 7.1: Example Case Statement for plugin_io Function

Here data is the pointer provided by the caller of the function. Now an example of how a plugin can use a function implemented in OLSR. The function **get_msg_seqno()** returns the next message sequence-number for OLSR to use when transmitting an OLSR packet. In order to use this function in a plugin something like that shown in algorithm 7.2, needs to be executed:

```
/*Define this function-pointer somewhere*/
olsr_u16_t (*get_msg_seqno) ();

/* Messageseqno fetch function */
if(!olsr_plugin_io(GETF__GET_MSG_SEQNO, &get_msg_seqno, sizeof(get_msg_seqno)))
{
        get_msg_seqno = NULL;
        retval = 0;
}
```

Algorithm 7.2: Example Usage of OLSR Standard Functions

The available commands (like **GETF__GET_MSG_SEQNO**) are defined in src/olsr_plugin_io.h in OLSR codebase. All commands that fetch function pointers start with GETF_ while all commands that fetches data-pointers starts with GETD_. No commands are to be removed from this header-file, but new ones can be added. One

should therefore always use the most recent version of this file to have access to as many functions and variables as possible when implementing a plugin.

To be able to access the olsr_plugin_io function, the plugin needs to be initialized from OLSR. The file src/plugin_loader.c implements the plugin loader code. For the plugin loader to be able to set up the needed pointers, the plugin must provide the function (in addition to some variables and other functions):

```
int
register_olsr_data(struct olsr_plugin_data *data);
```

This function is called from the OLSR plugin loader passing a pointer to a struct olsr_plugin_data which contains the pointers to OLSR functions that the plugin needs to use to be able to set up all needed data pointers. After this, the plugin is responsible for fetching all needed pointers from the OLSR daemon. The process of initializing a plugin is illustrated in figure 7.4.

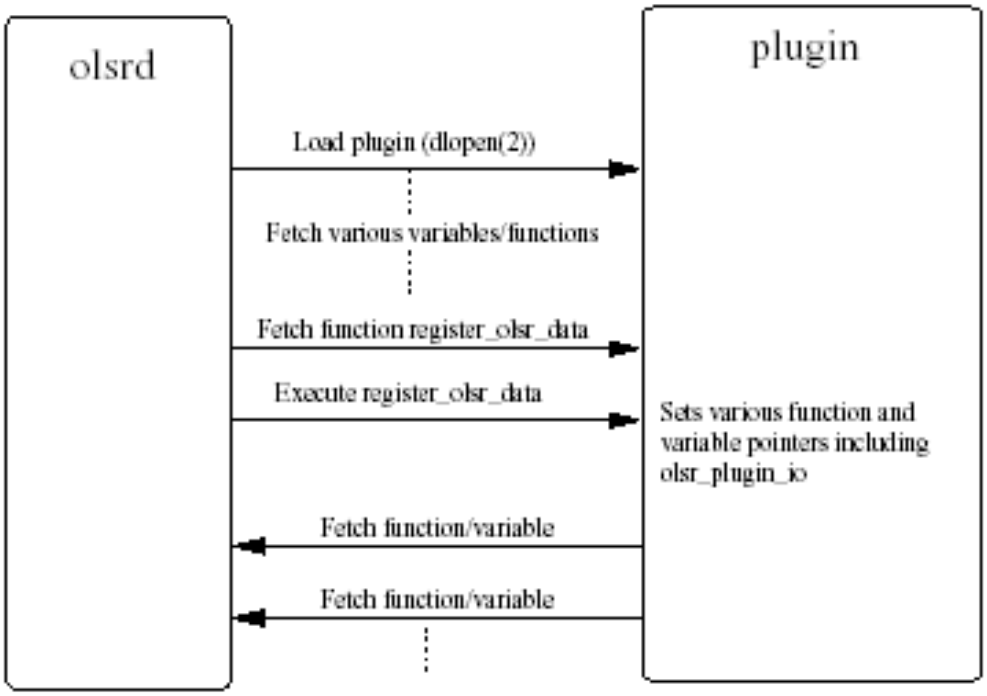

Figure 7.4: The Plugin Initialization Process

To make OLSR load a plugin at startup, the LOAD_PLUGIN directive is used in the configuration file.

7.3 PAPAMANETS Plugins

For the PAPAMANETS project, the basic need is to use the routing information provided by OLSR to transfer both unidirectional (SMS and MMS) and bidirectional (Audio and Video Conferencing) communications. For this reason, a plugin has to be developed for each of the multimedia applications. The section 7.3.1 explains how the OLSR plugins can be compiled using Cygwin. The sections 7.3.2 and 7.3.3 deal with the explanation of what the multimedia plugins do and how they are designed.

7.3.1 Plugin Compilation Using Cygwin

For Windows platform, the OLSR plugins can only be compiled as a DLL using a Cygwin installation with a current version of GCC and Mingw32. Each of the corresponding subdirectory for each plugin contains a shell script named "mkmf.sh" that takes "Makefile.win32.in" as its input, appends the dependencies, and outputs "Makefile.win32".

Any compiled files can be removed using the command:

```
make -f Makefile.win32 clean
```

The compiled files and the generated makefile can also be removed using the command:

```
make -f Makefile.win32 mclean
```

The plugin source code is compiled using the command:

```
make -f Makefile.win32
```

7.3.2 SMS and MMS Plugin

The plugin is to provide a solution where one of the nodes, running the plugin, in the MANET needs to send to another node, running the plugin, a text message or SMS.

This information is made available to the user and other processes through IPC using a TCP socket. The plugin should not affect nodes running without this functionality.

A node is to flood the network with a custom packet of SMS containing the information: The information about the destination, the size of the message and the message itself.

This should result in a scenario where only the node, whose IP is the same as that in the destination part of the packet, will process the message and others would forward it using the default forwarding algorithm.

To take advantage of OLSR's default forwarding scheme, the SMS has to be transmitted as an OLSR message. The message is encapsulated in a regular OLSR message header with a message type from the private message types (128-255). An OLSR message containing our SMS or MMS is shown in Figure 7.5.

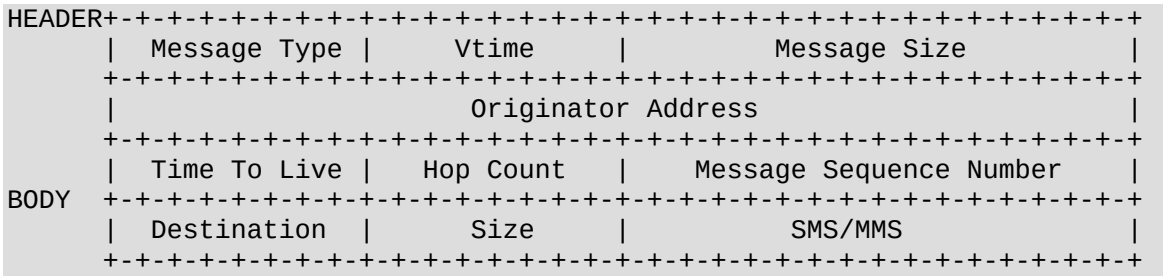

Figure 7.5: OLSR Message with SMS or MMS

To transmit the message, a message generation function is implemented. This function is registered with the OLSR scheduler at plugin initialization. The function polls a text file "IP.txt" to get hold of the receiver's ID. Then the function polls another text file "SMS.txt" to fill in the size information of the message and at the same time, writes

the actual message contents into a buffer thus building the message based on the information. This message is then flooded through OLSR.

A message parse function is registered with the OLSR message parser at plugin initialization to receive all incoming SMS messages. This function compares the destination component of the message with own address. In case the destination address matches with the node's own address, it further processes the message, reading the contents of the buffer into a text file "ReceiverSMS.txt". The function is also responsible for forwarding the message as well as checking for duplicate messages.

The plugin design for the SMS application and its working is illustrated in figure 7.6.

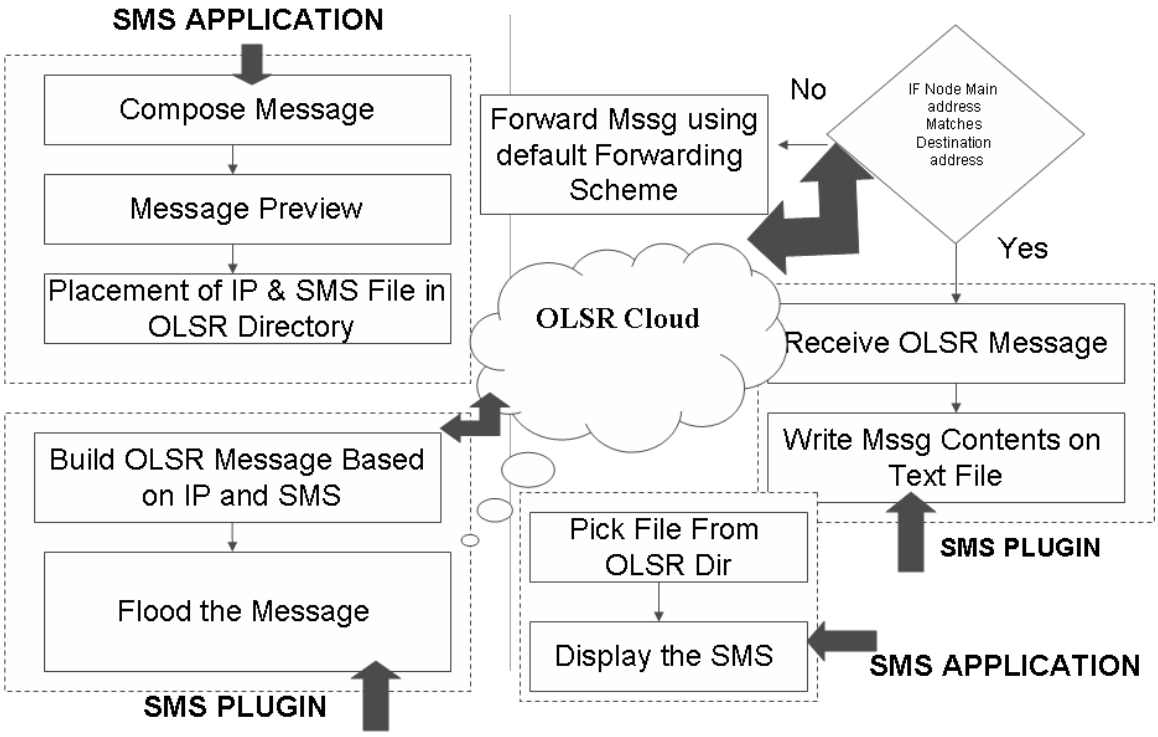

Figure 7.6: Design and Working of SMS Plugin

MMS plugin is implemented in a similar way. The only difference is that instead of polling to a text file, the message generation function polls to a zipped file “MMS.zip” which can comprise of image, audio, text or video, text or image, text etc. Also the message parser function, in case of a match in destination address and own address, reads the contents of the buffer into a zipped file “ReceivedMMS.zip”.

The plugin design for the MMS application and its working is illustrated in Figure 7.7.

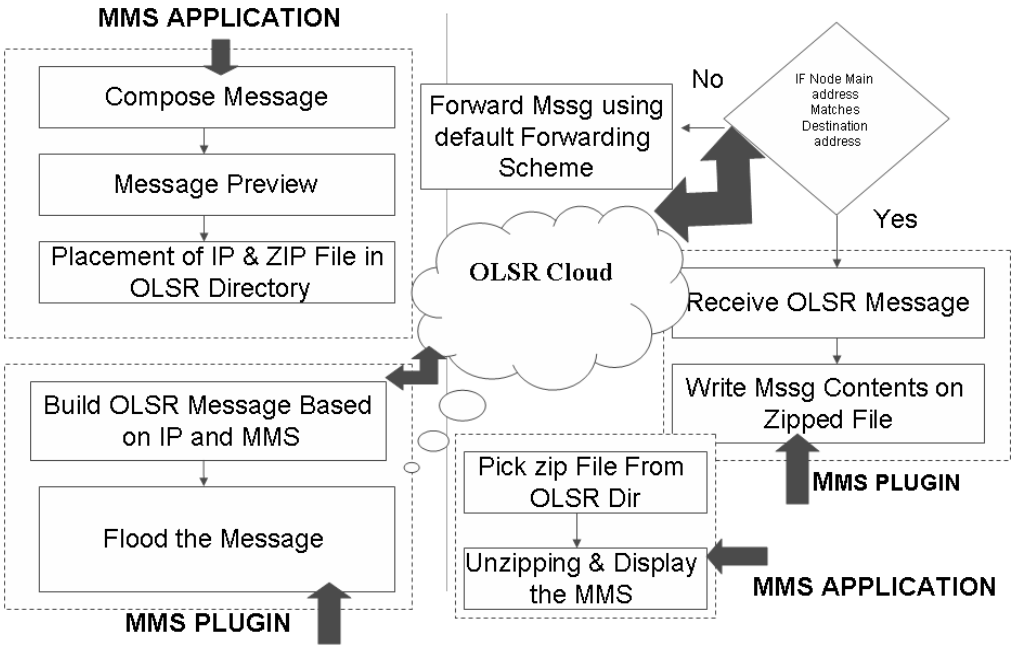

Figure 7.7: Design and Working of MMS Plugin

7.3.3 Audio and Video Conferencing Plugin

A similar strategy is followed in the case of audio and video conferencing plugin. The only difference is that instead of polling to a single file, the message generation function polls to two different files, meant for carrying the audio and video frames. The message is then composed in a similar way and is flooded throughout the network. In case of a match in destination address and own address, the receiving node reads the contents of the two buffers into wav file and bmp respectively. These are then used by the audio/video conferencing application to enable real time conferencing.

The design and working of audio and video conferencing plugin is illustrated in Figure 7.8.

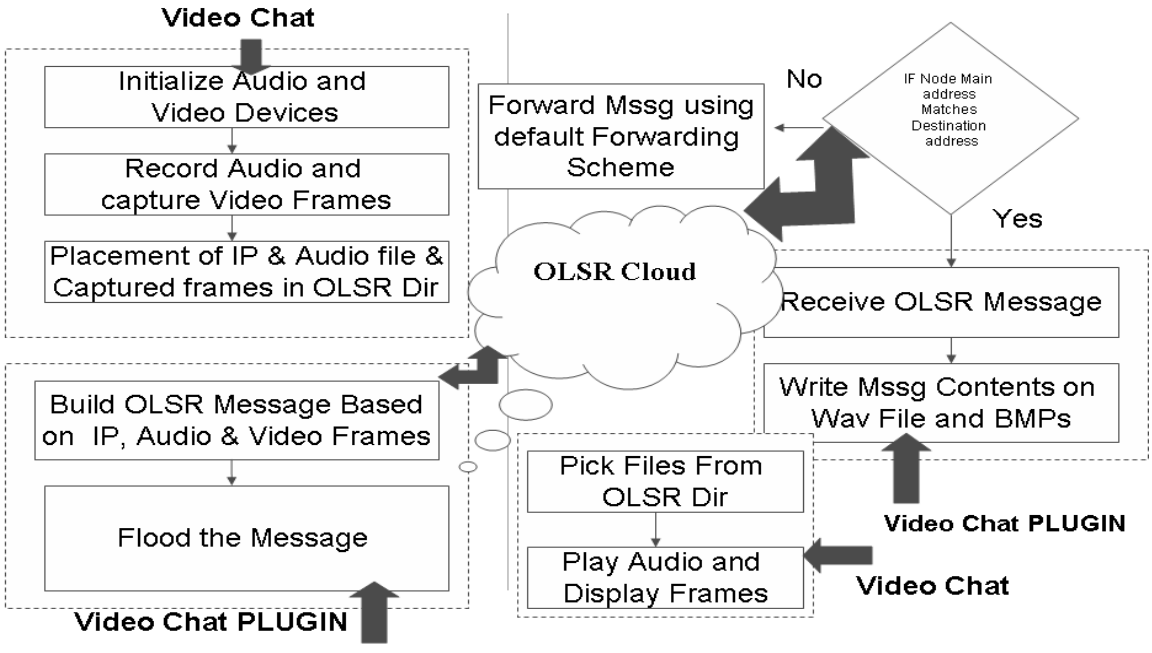

Figure 7.8: Design and Working of Audio and Video Conferencing Plugin

7.4 Summary

The chapter described the working of OLSR plugins, with an emphasis on the plugins designed for the PAPAMANETS project. The basic strategy followed for all the plugins is that information contained in a text file, zipped file, wav file, is picked up by OLSR which is then flooded through the network. The destination node identifies its own address in the message and receives the message, while all the remaining nodes serve to flood the message using the default forwarding algorithm.

Chapter 8

Ad hoc Wireless Configuration

The simplest way to create an Ad hoc Wireless network is with laptops or PCs equipped with 802.11 wireless transmission. A wireless peer-to-peer network with minimal configuration is set very quickly. No hubs, no routers, no cables, no worries.

This chapter focuses on the configuration of 802.11g Wireless Cards on Ad hoc mode. It gives a brief overview of various steps involved in the configuration.

8.1 Ad hoc Vs Infrastructure

Most installed wireless LANs today utilize "infrastructure" mode that requires the use of one or more access points. With this configuration, the access point provides an interface to a distribution system (e.g., Ethernet), which enables wireless users to utilize corporate servers and Internet applications (figure 8.1).

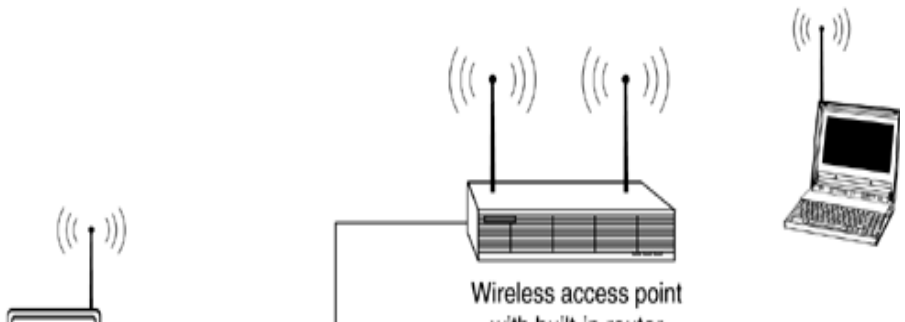

Figure 8.1: Infrastructure Network

As an optional feature, however, the 802.11 standard specifies "ad hoc" mode, which allows the radio network interface card (NIC) to operate in what the standard refers to as an independent basic service set (IBSS) network configuration. With an IBSS, there are no access points. User devices communicate directly with each other in a peer-to-peer manner.

Ad-hoc mode essentially eliminates the need for an access point by simply working off a 'peer-to-peer' style of communication. An Ad-Hoc network only requires wireless adapters to communicate (figure 8.2) hence significantly reducing the cost and maintenance compared to a network structured around an access point.

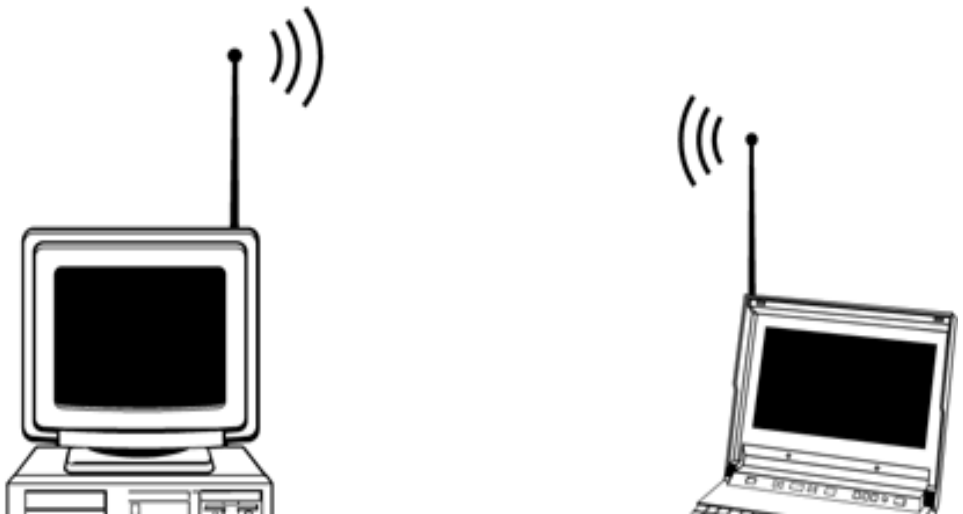

Figure 8.2: Ad hoc Network

8.2 Ad hoc Applications

Ad hoc mode allows users to spontaneously form a wireless LAN. For example, a group of people with 802.11-equipped laptops may gather for a business meeting at their corporate headquarters. In order to share documents such as presentation charts and spreadsheets, they could easily switch their NICs to ad hoc mode to form a small wireless LAN within their meeting room. Another example is when associates are waiting for a flight at the airport, and there is a need to share a relatively large PDF file. Through ad hoc mode, a file can easily be transferred from one laptop to another. With any of these applications, there's no need to install an access point and run cables.

The ad hoc form of communications is especially useful in public-safety and search-and-rescue applications. Medical teams require fast, effective communications when they rush to a disaster to treat victims. They can't afford the time to run cabling and install networking hardware. The medical team can utilize 802.11 radio NICs in their

laptops and PDAs and enable broadband wireless data communications as soon as they arrive on the scene.

Some product vendors are beginning to base their solutions on ad hoc mode. As an example, **MeshNetworks** offers a wireless broadband network system based on 802.11 ad hoc mode and a patented peer-to-peer routing technology. This results in a wireless mesh topology where mobile devices provide the routing mechanisms in order to extend the range of the system. For example, a user on one side of the building can send a packet destined to another user on the far side of the facility, well beyond the point-to-point range of 802.11, by having the signal hope from client device to client device until it gets to its destination. This can extend the range of the wireless LAN from hundreds of feet to miles, depending on the concentration of wireless users.

8.3 Pros and Cons of Ad hoc Scheme

Ad hoc mode is efficient in its own way. Some of the major advantages and disadvantages of the ad hoc scheme are addressed in this section.

8.3.1 Cost Savings

Without the need to purchase or install access points, considerable amount of money is saved when deploying ad hoc wireless LANs. Of course this makes the bean counters happy, but be sure to think about all of the pros and cons before making a final decision on which way to go.

8.3.2 Rapid Setup Time

Ad hoc mode only requires the installation of radio NICs in the user devices. As a result, the time to setup the wireless LAN is much less than installing an infrastructure wireless LAN. Obviously this timesaving only applies if the facility to support wireless LAN connectivity doesn't already have a wireless LAN installed.

8.3.3 Better Performance Possible

The question of performance with ad hoc mode is certainly debatable. For example, performance can be higher with ad hoc mode because of no need for packets to travel through an access point. This assumes a relatively small number of users, however. If there are lots of users, then better performance is by using multiple access points to separate users onto non-overlapping channels to reduce medium access contention and collisions. Also because of a need for sleeping stations to wake up during each beacon interval, performance can be lower with ad hoc mode due to additional packet transmissions if power management is implemented.

8.3.4 Limited Network Access

Because there is no distribution system with ad hoc wireless LANs, users don't have effective access to the Internet and other wired network services. Of course setting up a PC with a radio NIC is easy and configuring the PC with a shared connection to the Internet can be easily done. This won't satisfy a larger group of users very well, though. As a result, ad hoc is not a good way to go for larger enterprise wireless LANs where there's a strong need to access applications and servers on a wired network.

8.3.5 Difficult Network Management

Network management becomes a headache with ad hoc networks because of the fluidity of the network topology and lack of a centralized device. Without an access point, network managers can't easily monitor performance, perform security audits, etc. Effective network management with ad hoc wireless LANs requires network management at the user device level, which requires a significant amount of overhead packet transmission over the wireless LAN. This again leans ad hoc mode away from larger, enterprise wireless LAN applications.

8.4 802.11g Configuration in Ad-Hoc Mode

The Ad-Hoc standard is featured in almost every 802.11x Wireless LAN Card or Adaptor Model. Now successfully install wireless adapter i.e. 802.11g Wireless Card (figure 8.3) and the appropriate protocols, which will usually be explained in the product's manual.

Figure 8.3: 802.11g Wireless Cards

First off the bat, make sure that all the adapters installed on the computers waiting to be networked are ready to talk to each other. This will require the TCP/IP protocol to be installed for all the adapters on every computer. After this is completed, to configure TCP/IP by allocating an IP address and subnet mask to every adapter, which can be done by accessing the TCP/IP properties for the adapter. Since this depends on the Windows versions there is no universal method of doing this, but by snooping around the properties of the network connection it can be easily find out.

Once inside the TCP/IP properties of the adapters shown in figure 6.4, give every adapter a unique IP address. As an easy choice, use the 192.168.0.x IP range, which automatically configures itself to use the 255.255.255.0 subnet mask. In other words, or three computers, give the first an IP address of 192.168.0.1 and a subnet of 255.255.255.0, the second an IP of 192.168.0.2 with the **same** subnet and the third with an IP of 192.168.0.3 with the same subnet again, and so on for each computer, incrementing the x in 192.168.0.x by 1 for every new computer. On some network setups, a server allocate each other computer an automatic IP address, however manual allocation is by far the simplest way.

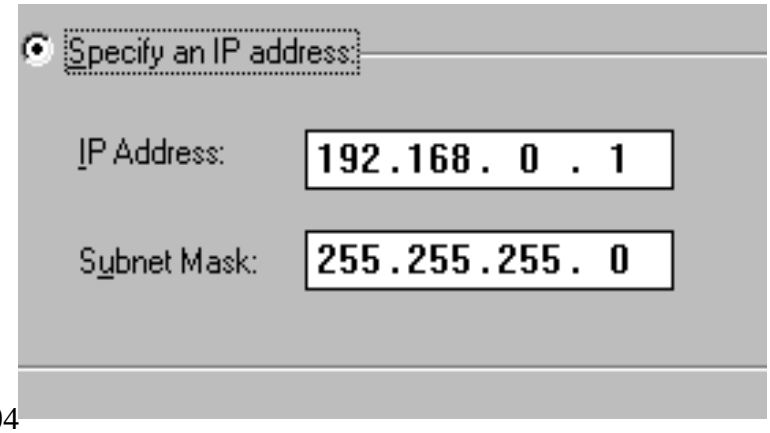

Figure 8.4: TCP/IP Settings

8.5 Ad-Hoc Settings

Even if all the Windows network settings are complete, the simple task of pinging another computer on the network just created will be impossible. As is the nature of Ad-Hoc wireless networks, there are a few settings to correct before any data can be sent to and from the network, mainly acting as security measures to render the network next to impossible to breach.

To begin with, enable Ad-Hoc mode in adapter's settings. Depending on the make and model the location of this setting will vary, with the adapter change to Ad-Hoc by simply selecting it from the "mode" drop down menu from the included utility (figure 8.5). Every adapter should come with its own software with every option available, so it is only a matter of looking for it.

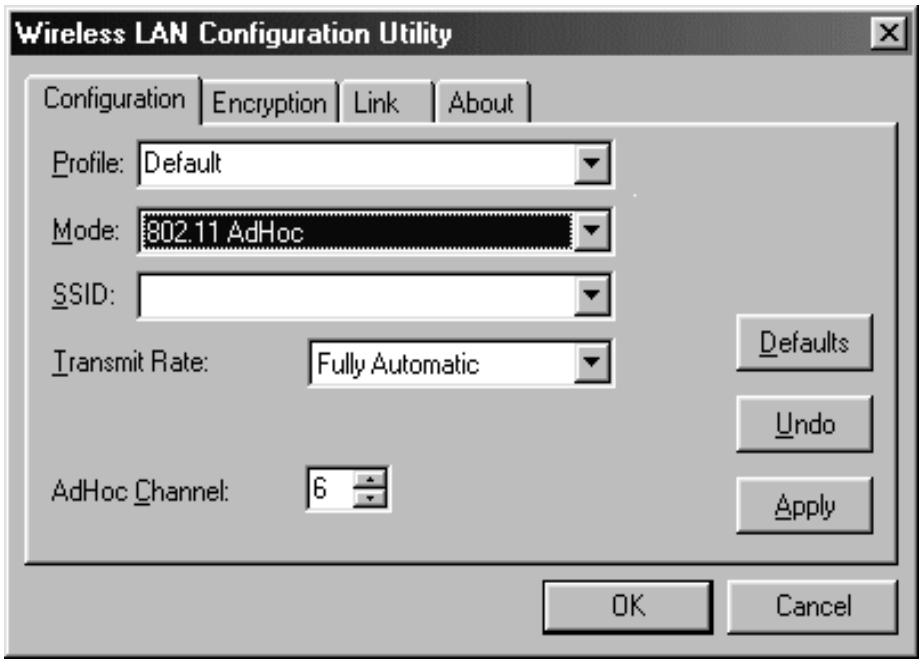

Figure 8.5: Wireless LAN Configuration Utility

Selecting Ad-Hoc is obviously the first important step, which has to be done on every adapter otherwise it will probably default in looking for an access point, which doesn't exist.

The next step is to create unique characteristics to the network to prevent any intrusions. Despite the remote chance someone will attempt to hack the home wireless network, they are important, not to mention necessary, to attend to. The first of these is the channel.

Like most wireless communication devices, a channel to send and receive data from will need to be selected. This is a number that has no direct influence on the

network, so select any number in the list but make sure to keep it consistent within the network. In other words, each adapter has to be set to the same channel otherwise it will completely decline to even recognize the other computers (figure 8.5).

The final task that needs to be set for bare minimal communication in an Ad-Hoc network is the SSID (figure 8.5), which is an acronym for Service Set Identifier. The SSID is a unique identifier, which acts like a password for the network, if an identical SSID is not set on any given adapter, access will be denied. This can be a 32-character variant, so treating it like any other password is a good idea, try to keep it hard to guess.

Once all these settings are out of the way, click apply and leave the utility. To test if data can successfully travel through the network open a command window, or MS Dos window, and type "ping 192.168.0.1" and press enter. A reply will be received with the time taken to receive the data, which should be under 10ms for the basic ping command but that depends on the signal strength and quality. If requests timed out errors are received, something has not been set correctly, so make sure everything is in order and perhaps follow the Ad-Hoc setup again. Make sure to ping every address from every computer, if the 1st computer can ping the 2nd, and the 2nd can ping the 3rd, it doesn't mean the 1st and 3rd can talk to each other so confirm every combination.

8.6 Data Security

This is a question that has riddled the 802.11 standard since day one. In a nutshell, data is not 100%, completely safe from outside access. Due to the nature of wireless

technology, for someone to hack a cabled LAN, they would have to physically connect the network, however there is no direct control on where the wireless signal travels.

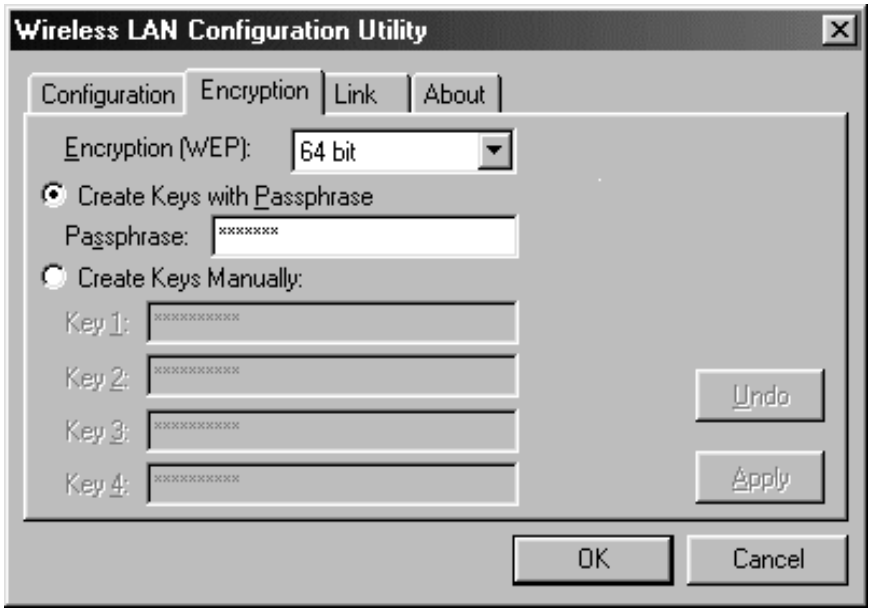

Figure 8.6: Encryption option

It is time to select another word to use as another password like filter for the network (figure 8.6). Try not to use the same one as the SSID; otherwise it will make encryption somewhat pointless. Choose 4 unique keys to use, which will make hacking that extra bit more difficult, but using just one should do it.

Although it is true a 802.11x wireless network is never 100% safe, having a unique channel, a unique SSID and the capability to have 4 unique encryption keywords practically makes a wireless network a completely safe solution.

8.7 Summary

The chapter briefly explained the various steps involved in the configuration of 802.11g Wireless Cards to be used for the establishment of Mobile Ad hoc Wireless Network that forms the basis of the practical deployment of PAPAMANETs.

Chapter 9

Conclusions

The field of ad hoc mobile networks is rapidly growing and changing. There are still many challenges that need to be met and that may be worth examining but not addressed in this report.

The work on this report has been very interesting and many lessons have been learned along the way. In this chapter, the major challenges in the practical deployment of ad hoc networks on wider scale are explained. Some of the things learned in the implementation process are described as possible updates to the project. The future of the PAPAMANETs and extensions to the project are also discussed, and some final conclusions are drawn. Some possible applications of the project are also conversed.

9.1 Challenges in Ad hoc Network Deployment

The ad hoc networking technology has stimulated substantial research activity in the past 10 years or so. The rather interesting fact is that although the military has been experimenting and even using this technology for the last three decades, the research community has been coping with the rather frustrating task of finding a "killer" non-military application for ad hoc networks.

A major challenge that has been perceived as a possible "show stopper" for technology transfer is the fact that commercial applications do not necessarily conform to the "collaborative" environment that the military communication environment does. In other words, why should a user forward someone else's transmission, depleting his or her own battery power and, thus, possibly restricting his or her use of the network in the future? This question may relate to the issue of billing - if billing is possible (and, in fact,

desirable), then nodes that serve as "good citizens" could be rewarded. But billing is, by itself, a significant challenge in ad hoc networks.

Other challenges in deployment of ad hoc networks relate to the issues of manageability, security, and availability of communication through this type of technology.

Another challenge in MANETs is related to the issue of location management. Since there is no fixed infrastructure available for MANET with nodes being mobile in the three-dimensional space, location management becomes a very important issue. For example, *route discovery* and *route maintenance* are some of the challenges in designing routing protocols. In addition, finding the position of a node at a given time is an important problem. This led to the development of *location-aware* routing, which means that a node will be able to know its current position. A great deal of work has been done using GPS to determine the position of a node at a particular instance of time but much is remaining in this field.

9.2 Applications of MANETS

According to the analysis carried out during the course of the project, the project “Multimedia over PAPAMANETS” may find its utility in one of the possible areas mentioned in this section.

9.2.1 Mobile Conferencing

Ad hoc networks enable mobile conferencing for business users who need to collaborate outside their office where no network infrastructure is available. There is a

growing need for mobile computing environments where different members of a project need to collaborate on design and development. The users need to share documents, upload and download files, and exchange ideas using any one of the multimedia applications.

9.2.2 Personal Area and Home Networking

Ad hoc networks are quite suitable for home as well as personal area networking applications. Mobile devices with Bluetooth or WLAN cards can be easily configured to form an ad hoc network. With the Internet connectivity at home, these devices can easily be connected to the Internet. Hence, the use of these kinds of ad hoc networks has practical applications and usability.

9.2.3 Emergency Services

When the existing network infrastructure has ceased to operate or is damaged due to some kind of disaster like earthquakes, hurricanes, fire, and so forth, ad hoc networks can be easily deployed to provide solutions to emergency services. These networks can also be used for search and rescue operations, retrieval of patient data remotely from hospitals and many other useful services.

9.2.4 Public Hotspots

In places like airports, train stations, coffee shops, football grounds, and malls, the ad hoc networks provide users the ability to create their own network and communicate with each other instantly. Ad hoc networks can also be used for entertainment purposes

like providing instant connectivity for multi-user games. In addition, household Internet connectivity can be provided by a community hotspot.

9.2.5 Military Applications

In battlefield, MANET can be deployed for communications among the soldiers in the field. Different military units are expected to communicate and cooperate with each other within a specified area. In these kinds of low mobility environments, MANET is used for communications where virtually no network infrastructure is available. The idea can be that every soldier is equipped with a mobile PC with headset and microphone to handle voice communications while mapping whereabouts of soldiers and their companions.

9.2.6 Ubiquitous and Embedded Computing Applications

With the emergence of new generations of intelligent portable mobile devices, ubiquitous computing is becoming a reality. As predicted by some researchers, ubiquitous computers will be around us, always doing some tasks for us without our conscious effort. These machines will also react to changing environments and work accordingly. These mobile devices will form an ad hoc network and gather various localized information and sometimes inform the users automatically.

9.2.7 Mobile Commerce

Ad hoc networks can be used to make electronic payments anytime, anywhere. Business users can retrieve customer/sales-related information dynamically and can build reports on the fly.

9.2.8 Location-based Services

MANET when integrated with location-based information provides useful services. GPS (Global Positioning System), a satellite-based radio navigation system, is a very effective tool to determine the physical location of a device. A mobile host in a MANET when connected to a GPS receiver will be able to determine its current physical location. For example, a group of tourists using PDAs with wireless LAN cards installed in them along with GPS connectivity can form a MANET. These tourists can then exchange messages and locate each other using this MANET. Vehicles on a highway can form an ad hoc network to exchange traffic information. In addition, location-based information services can be delivered by MANETs. For example, one can advertise location-specific information like restaurants and shopping malls and retrieve location-dependant information like travel guides, movie theatres, drug stores, and so forth.

9.2.9 Sensor Networks

It is a special kind of hybrid ad hoc network. There are a growing number of practical applications for tiny sensors in various situations. These inexpensive devices, once deployed, can offer accurate information about temperature, chemicals, critical environmental conditions (e.g., generate wild fire alarms), and behavior patterns like movements of some animals, and so forth. In addition, these devices can also be used for security applications. However, these sensors once deployed have limited battery power, and lifetime of the battery may determine the sensor's lifetime.

9.2.10 Geocasting

Another important application area is geocast, which means sending messages to all the hosts in a particular geographic region. Geocasting will be a very useful application when someone wants to send some messages to people in a particular region. This is particularly important in situations when there is a disaster or emergency.

9.3 Security Issues

The Wired Equivalent Privacy protocol was supposed to provide wireless IEEE 802.11 based networks with the same amount of security as their wired counterparts. But WEP has several proved flaws in its architecture. Because of the weak security provided by WEP and due to the fact that parts of MANETs might run on wired links where no encryption is used, some security mechanism should be provided by the routing protocol itself.

The provision of security services in the MANET context faces a set of challenges specific to this new technology. The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified. Nevertheless, the single most important feature that differentiates MANET is the absence of a fixed infrastructure. No part of the network is dedicated to support individually any specific network functionality, with routing (topology discovery, data forwarding) being the most prominent example. Additional examples of functions that cannot rely on a central service, and which are also of high relevance to this work, are naming services, certification authorities, directory and other administrative services.

Even if such services were assumed, their availability would not be guaranteed, either due to the dynamically changing topology that could easily result in a partitioned network, or due to congested links close to the node acting as a server. Furthermore, performance issues such as delay constraints on acquiring responses from the assumed infrastructure would pose an additional challenge.

The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and nontrusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials and the ability for nodes to validate them. In the MANET context, there may be no ground for an *a priori* classification, since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Additionally, in MANET freely roaming nodes form transient associations with their neighbors; join and leave MANET sub-domains independently and without notice. Thus it may be difficult in most cases to have a clear picture of the ad hoc network membership. Consequently, especially in the case of a large-size network, no form of established trust relationships among the majority of nodes could be assumed.

In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. The mechanisms currently incorporated in MANET routing protocols cannot cope with disruptions due to malicious behavior. For

example, any node could claim that is one hop away from the sought destination, causing all routes to the destination to pass through itself. Alternatively, a malicious node could corrupt any in-transit route request (reply) packet and cause data to be misrouted.

The presence of even a small number of adversarial nodes could result in repeatedly compromised routes, and, as a result, the network nodes would have to rely on cycles of timeout and new route discoveries to communicate. This would incur arbitrary delays before the establishment of a non-corrupted path, while successive broadcasts of route requests would impose excessive transmission overhead. In particular, intentionally falsified routing messages would result in a *denial-of-service (DoS)* experienced by the end nodes.

Thus the security of MANET routing protocols is envisioned to be a major "roadblock" in commercial application of this technology and much needs to be done in this regard before MANETs find their practical deployment.

9.4 Self-configuring Networks

Mobile ad-hoc networks should be *self-configuring*. This means that nodes that are to participate in a MANET should not need extensive knowledge of network parameters prior to joining the network. This should include automatic configuration of IP addresses. Although IP address auto-configuration is not explicitly a part of MANETs, many ad-hoc networks should benefit from some generic auto configuration scheme. This should not only include automatic IP address allocation, but also the detection of some basic abilities of the MANET such as the routing protocol utilized.

9.5 Energy Efficiency in MANETs

Wireless devices are often powered by batteries that have a finite amount of energy. In some ad hoc networks, such as sensor networks deployed in a hostile zone, it may not be possible to change a battery once it runs out of energy. As a consequence, the conservation of energy is of foremost concern for those networks. A good ad hoc routing protocol should therefore be *energy efficient.*

Lack of infrastructure, cost of using a shared wireless medium, and the dynamic nature of ad hoc networks also entail a significant amount of overhead when routing data in ad hoc networks and maintaining the route information. A good ad hoc routing protocol should contain *minimal overhead*. For large networks, minimizing the overhead is closely related to the scalability requirement, as the communication overhead often grows significantly with increasing number of nodes in a network.

The table-driven routing protocols, such as OLSR, attempt to maintain up-to-date routing information stored in one or more tables. Paths toward all destinations are periodically refreshed even if not used. Normally, these protocols require nodes to broadcast information about their neighbors, and based on this information, each node in the network computes the minimum path to every possible destination. The main objective of these protocols is to maximize the *throughput* and minimize the *response time*. For a large ad hoc network consisting of hundreds or thousands of nodes, the amount of routing information stored in each node grows proportionally. Periodical update messages will eventually consume all the resources leaving the network unusable.

To improve the *scalability* of ad hoc routing protocols, the need is to use energy efficient protocols, which are based on the amount of energy that is spent in correctly delivering a packet to its final destination. Their target is to maximize energy efficiency (e.g., by finding the lowest energy routing path) and/or the lifetime of the whole network (e.g., by balancing traffic).

9.6 QoS Based Multimedia Service

In the recent years, there has been a tremendous growth in the multimedia applications, hence, multimedia traffic over wired and wireless networks. With the growing demand for services that support multimedia traffic, the ad hoc networks should have the capability to deliver multimedia traffic with reasonable quality. However, due to the very nature of ad hoc networks and the constraints described earlier, it is a difficult task.

The need for more bandwidth, less delay, and minimum packet loss are some of the criteria for high quality transmission for delivering real-time multimedia. However, the current best-effort network architecture does not offer any quality of service (QoS).

It is well known that TCP is mainly designed for reliable data traffic. It is not suitable for real-time multimedia traffic as the delay and jitter caused by TCP retransmissions may be intolerable; the slow-start and congestion avoidance are not suitable for real-time multimedia transport. In addition, TCP does not support multicast.

The UDP is typically used in almost all real-time multimedia applications. When congestion occurs, an unlimited amount of UDP datagrams may be dropped since UDP is

non-adaptive. Hence, real-time multimedia applications must implement additional rate control and error control techniques in order to cope with network congestion.

In ad hoc networks, wireless links have high transmission error rate because of fading, path loss, and interference. An end-to-end path found in ad hoc networks has an even higher error rate since it is composed of multiple links. The frequent link failures (some nodes move away out of the transmission range due to mobility) and route changes cause packet losses and reduce the received video quality. In order to maintain a good quality of video in ad hoc networks, there should be effective error control to reduce packet losses to a certain level.

9.7 Final Thoughts

Lot can be predicted about the future of wireless communication, but one thing is for sure, wireless technology is here to stay. As more and more of the services currently operated over wired, centralized networks are migrated to wireless communication solutions, more focus will be put on the possibilities of moving beyond the centralized access point paradigm. The MANET working group has laid down some important initial work on mobile ad-hoc routing. However, MANET routing needs to take other constraints than just take hop count into consideration when calculating routes. Issues like bandwidth, delay and stability should all be taken into consideration.

BIBLIOGRAPHY

[1] A. Penttinen, “Research on ad hoc networking: Current activity and future directions.”

[2] E. Royer and C. Toh, “A review of current routing protocols for ad-hoc mobile wireless networks,” *IEEE Personal Communications*, apr 1999.

[3] Ogier, R.G., Templin, F.L., Bellur, B., & Lewis, M.G. (2002, March). Topology broadcast based on reverse-path forwarding (TBRPF). draft-ietf-manettbrpf- 05.txt, Internet Draft, MANET Working Group.

[4] G., Gerla, M., & Chen, T.-W. (2000).*Fisheye state routing: A routing scheme for ad - hoc wireless networks.*Proceedings of the ICC 2000, New Orleans, Louisiana.

[5] Jacquet, P., Muhlethaler, P., Qayyum, A.,Laouiti, A., Viennot, L., & Clausen, T.(2000, November). Optimized link state routing protocol. draft-ietf-manet-olsr-05.txt, Internet Draft, IETF MANET Working Group.

[6] Johnson, D.B., & Maltz, D.A. (1999). The dynamic source routing protocol for mobile ad hoc networks. Retrieved December 30, 2004, from *http://www.ietf.org/internet-drafts/draftietf-manet-dsr-03.txt*

[7] Garcia-Luna-Aceves, J.J., & Spohn, M.(1999). Source tree adaptive routing in wireless networks. *Proceedings of IEEE ICNP*.

[8] Chiang, C.-C., Wu, H.K., & Gerla, M. (1997). Routing in clustered Multihop mobile wireless networks with fading channel. *Proceedings of the IEEE Singapore International Conference on Networks.*

[9] Murthy, S., & Garcia-Luna-Aceves, J.J.(1996). An efficient routing protocol for wireless networks. *ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks*, 183-97.

[10] Perkins, C.E., & Belding-Royer, E.M.(1999). Multicast operation of the adhoc on-demand distance vector routing protocol. *Proceedings of the MobiCom*, Seattle, Washington, 207-218.

[11] Broch, J., Johnson, D., & Maltz, D. (1999). The dynamic source routing protocol for mobile ad hoc networks. *IETF, MANET Working Group*. Internet draft 03.

[12] Aggelou, G., & Tafazolli, R. (1999). *RDMAR: A bandwidth-efficient routing protocol for mobile ad hoc networks.* Proceedings of the 2nd ACM International Workshop on Wireless Mobile Multimedia (WoWMoM), Seattle, Washington.

[13] Ramanathan, R., & Streenstrup, M. (1998). Hierarchically organized, multi-hop mobile wireless networks for quality-of-service support. *Mobile Networks and Applications, 3*, 101-119.

[14] Park, V.D., & Corson, M.S. (1997). A highly adaptive distributed routing algorithm for mobile wireless networks. *Proceedings of the INFOCOM.*

[15] Pei, G., Gerla, M., & Hong, X. (2000). LANMAR: Landmark routing for large scale wireless ad hoc networks with group mobility. *Proceedings of IEEE/ACM MobiHOC 2000*, 11-18.

[16] Pei, G., Gerla, M., Hong, X., & Chiang, C.- C. (1999). *A wireless hierarchical routing protocol with group mobility*. Proceedings of IEEE ICCCN'99, Boston, Massachusetts.

[17] Haas, Z., & Pearlman, M. (2000). *The zone routing protocol (ZRP) for ad hoc network.* IETF, MANET Working Group. Internet draft 03.

[18] Basagni, S., Chlamtac, I., Syrotiuk, V., & Woodword, B. (1998, October). *A distace routing effect algorithm for mobility (DREAM).* Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Dallas, Texas.

[19] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. & Belding-Royer, E.M. (2002, November). *A secure routing protocol for ad hoc networks.* Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), Paris, France.

[20] Yi, S., Naldurg, P., & Kravets, R. (2002, July) *A security aware routing protocol for wireless ad hoc networks.* Proceedings of the 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI), Orlando, Florida.

[21] Papadimitratos, P., & Haas, Z. (2000, January). *Secure routing for mobile ad hoc networks.* Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, Texas.

[22] S. Corson and J. Macker. *MANET RFC 2501*, informational edition, January 1999.

[23] T. Clausen, P. Jacquet et L. Viennot, *Comparative Study of Routing Protocols for Mobile Ad Hoc Networks*, Med-hoc-Net, 2002 Available at: http://hipercom.inria.fr/~viennot/postscripts/medhocnet2002sim.ps.gz

[24] S. Corson and J. Macker, " Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," *Network Working Group RFC 2501*, pp. 2–3, Jan. 1999.

[25] The IEEE 802.11a standard. Technical report.

[26] The IEEE 802.11b standard. Technical report.

[27] The IEEE 802.11g standard. Technical report.

[28] *ANSI/IEEE 802.11 Std 802.11, 1999 Edition*, ieee standards document edition, February 1999.

[29] Internet Engineering Task Force. *Mobile Ad-hoc Networks (MANET) - WORKGROUP*. http://www.ietf.org/html.charters/manet-charter.html.

[30] C. Perkins, E. Belding-Royer, and S. Das. *AODV RFC3561*, experimental edition, July 2003.

[31] Clausen, Jacquet, Laouiti, Minet, Muhlethale, Qayyum, and Viennot. *OLSR RFC3626*, experimental edition, October 2003.

[32] F. Templin R. Ogier and M. Lewis. *TBRPF RFC3684*, experimental edition, February 2004.

[33] David A. Maltz David B. Johnson and Yih-Chun Hu. *The Dynamic Source Routing Protocol*, experimental edition, April 2003. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.

[34] C. Perkins. *IP Mobility Support RFC2002*, standards track edition, October 1996.

[35] ITU-T Recommendation H.263, "Video coding for low bit rate communication"

[36] Riley and Richardson, "Digital Video Communications", Artech House 1997 (available from http://www.artech-house.com/)

[37] http://www.4i2i.com/ , software and hardware implementations of H.263

[38] Tracy Camp Jeff Boleng Vanessa Davies, *A Survey of Mobility Models for Ad Hoc Network Research*, Dept. of Math. and Computer Sciences, Colorado School of Mines, Golden, CO, 12 April, 2002. Available at: http://toilers.mines.edu/papers/psgz/models.ps.gz

[39] T.H. Clausen, G. Hansen, L. Christensen and G. Behrmann, *The Optimized Link State Routing Protocol, Evaluation through Experiments and Simulation*, IEEE Symposium on "Wireless Personal Mobile Communications", September 2001. Available at: http://menetou.inria.fr/olsr/wpmc01.ps

[40] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, a. Qayyum et L. Viennot, *Optimized Link State Routing Protocol*, IEEE INMIC Pakistan, 2001. Available at: http://hipercom.inria.fr/~viennot/postscripts/inmic2001.ps.gz

[41] Thomas Clausen, Philippe Jacquet, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, Laurent Viennot, *Optimized Link State Routing Protocol (OLSR)*.

Internet Draft, Internet Engineering Task Force, 10 December 2002. Work In Progress. Available at: http://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-08.txt

[42] T. Clausen, P. Jacquet et L. Viennot, *Comparative Study of Routing Protocols for Mobile Ad Hoc Networks*, Med-hoc-Net, 2002 Available at: http://hipercom.inria.fr/~viennot/postscripts/medhocnet2002sim.ps.gz

[43] V.Davies. *Evaluating mobility models within an ad hoc network*. Master's thesis, Colorado School of Mines, 2000. Available at: http://toilers.mines.edu/papers/pdf/vanessa-thesis.pdf

[44] P.Jacquet, A. Laouiti, P. Minet and L. Viennot, *Performance Analysis of OLSR Multipoint Relay Flooding in Two Ad Hoc Wireless Network Models*, Research Report-4260, INRIA, September 2001 Available at: ftp://ftp.inria.fr/INRIA/publication/publi-ps-gz/RR/RR-4260.ps.gz

[45] P. Jacquet, A. Laouiti, P. Minet, L. Viennot, *Performance of multipoint relaying in ad hoc mobile routing protocols*, Networking 2002, Pise (Italy) 2002. Available at: http://hipercom.inria.fr/olsr/networking2002.ps

[46] P. Jacquet and L.Viennot, *Overhead in Mobile Ad hoc Network Protocols*, Research Report-3965, INRIA, June 2000 Available at: ftp://ftp.inria.fr/INRIA/publication/publi-ps-gz/RR/RR-3965.ps.gz

[47] A. Laouiti, P. Muhlethaler, A. Najid, E. Plakoo, *Simulation Results of the OLSR Routing Protocol for Wireless Network*, Med-Hoc-Net 2002. Available at: http://hipercom.inria.fr/olsr/medhoc.ps

[48] A. Laouiti, A. Qayyum et L. Viennot, *Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks*, 35th Annual Hawaii International Conference on System Sciences 2002. Available at: http://hipercom.inria.fr/olsr/hicss2001.ps

[49] Laurent Viennot, Philippe Jacquet and Thomas Heide Clausen T. Clausen, P. Jacquet et L. Viennot, *Ad-hoc Network Protocols versus Mobility and Data Traffic Activity*, INRIA Rocquencourt, Projet Hipercom, Med-hoc-Net, 2002Available at: http://hipercom.inria.fr/~viennot/postscripts/medhocnet2002ctrl.ps.gz