Chapter 2 – AD-HOC NETWORKING

2.1 MANET OPERATIONAL EMPLOYMENT

MANET protocols can be implemented on various radio subnetworks: "classical" military VHF/UHF networks, militarized WLAN.

The need for Wireless LAN has been identified at the Brigade, Battalion and Platoon levels. In the future, wireless LAN could also be used inside a group of mobile entities relatively closed one from the others, such as in a tank squadron on the move.

The mobile ad-hoc network is especially useful in rapid deployment. Military teams require fast, effective communications when they rush to an operational scenario.

MANET networks has to meet C3I system requirements, according to the NATO definition. On a C3I tactical level, MANET network has to gather information about enemy and own forces and the environment in which they are deployed, disseminate orders to execute decisions, acquire reports from lower level units.

MANET Protocols has to solve the main problems due to tactical behavior:

- Range of the radio networks: a mobile or a group of mobile may be temporarily isolated from a network (for many reasons including distance and relief): relaying capacities, back-up networks and reconfiguration are important functions to keep a maximum connectivity with acceptable data rate and quality of service;
- Moves of users from one network to another or from on access interface to another that need adaptation of the routing and may be of the addressing;
- Moves of assets and LANs (Aircraft, Navy ships) that may imply other routing functions; and
- EMCON communication restrictions: When a mobile platform, due to operational security, is operating under EMCON directives it can't be capable of transmitting any information and it is unable to respond any received signals. Therefore co-operative communications are not possible; tactical units are committed solely to a "receive only" communication network or unidirectional link. Solutions to the EMCON communication restrictions can be envisaged at different level and require both doctrinal aspects as well as protocol implications.

2.2 MANET ROUTING

2.2.1 Overview

Mobile ad-hoc networking is to extend mobility ("Mobile IP" technology is to support a mobile host connected through various means to the Internet other than its well-known fixed-address domain space), into the field of autonomous, mobile, wireless domains, where a set of nodes, which may be routers and hosts, themselves form the network routing infrastructure in an ad-hoc mode.

MANET concerns with the autonomous system of mobile routers, connectedly wireless links.

Because of the different nature of wireless networks as compared to the fixed wired networks, the existing solutions are not suitable for this environment. This situation opens a wide variety of issues and challenges the designers of routing protocols with a complex combination of conflicting problems. The main challenges include the dynamic and rapidly changing topology, low available bandwidth, lack of a

centralised entity, large network diameters, existence of unidirectional links, scaling up problems, and the security considerations for these shared medium access networks.

In an encumbered mobile network, to quickly discover the various options of routing, is preferable to calculate the single shortest road.

These issues require that a routing protocol for a mobile ad-hoc network should be self starting and self organising, which provides the multi-hop, loop free paths to the required destinations in the network. Because of the mobility of the nodes, there should be a mechanism of dynamic topology maintenance, and rapid convergence of the protocol should be assured to stabilise the system. But the daunting task is to make it all possible using the minimum memory and bandwidth resources, and minimal overhead for data transmission. It is also required from these protocols to be scaleable to large networks.

In IETF WG, MANET is now focus on unicast and broadcast issues, but no more on multicast.

2.2.2 Concepts Developed by MANET

Architectural and protocol issues are here discussed.

2.2.2.1 Hierarchy of MANET Routing Protocols

MANET routing protocols work at the Network Layer level. The general MANET architecture is shown in Figure 2-1 below:

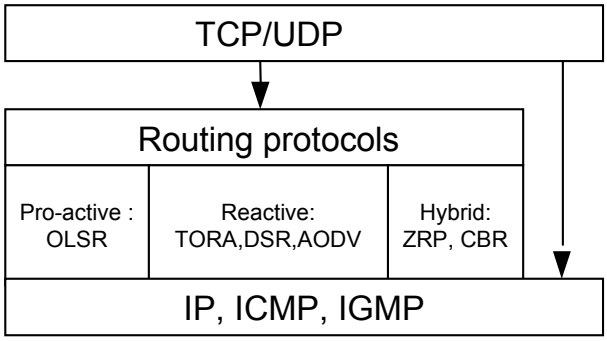

Figure 2-1: Hierarchy of MANET Routing Protocols.

Some functionalities done by different routing protocols individually are:

- **Encapsulation**. To improve the overall network performance, several control messages are encapsulated and aggregated into a single packet. In this way, it reduces the “number” of control messages to send, which, in consequence, reduces the “attempts” for the channel access. So the per-message, multiple access “delay” in contention based schemes is reduced.
- **Network Level Address Resolution**. There’s packets to map RIDs to IP addresses, which is similar to MAC address to IP address mapping. RIDs (Router IDs) provide the possibility to have more than one physical interface associated to a router.
- **Link Status Sensing**. There’s mechanism of exchange of BEACON and ECHO packets between neighbours for the neighbourhood detection. Data and ACK packets are also considered as the BEACON and ECHO equivalent packets, to reduce control traffic during data transmission.
- **One-Hop Broadcast Reliability**: To provide a reliable broadcast between the neighbours, concept of Colour and Sequence Number associated to the reliable delivery neighbourhood (RDN) can be used. When a node receives a packet with correct Colour and Sequence Number, it

acknowledges the packet. There is also a Point to multi-point selective repeat algorithm for reliable multicast.

- **Security Authentication**. MAA (MANET Authentication Architecture) can provide nodes to choose among the simple to complex authentication options, depending upon their security requirements. MAA uses cryptography requiring distribution/exchange of encryption key information.
- **Multi-Point Relaying**. Multi-point relaying is a technique which attempts to minimise the duplicate re-transmissions of the broadcast packets in the same region. For the flooding of the packets in the networks, MPR technique efficiently forms a spanning tree to diffuse the packet in the whole network, using minimum re-transmissions. The concept behind is, that instead of every router, only selective routers (called the multi-point relays of a node) re-transmit the packet, still covering the same area.

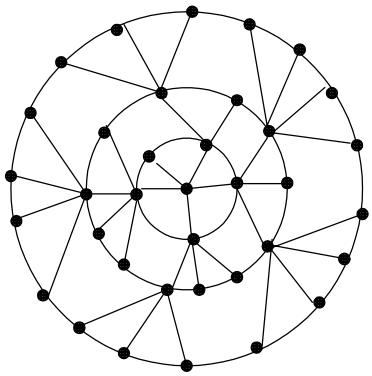

Figure 2-2: MPR Tree.

MANET has also developed a classification for the proposed routing protocols.

2.2.2.2 Classification of Routing Protocols

Several routing protocols for the mobile ad-hoc networks are presented in the MANET working group. These protocols can be mainly categorise into three types:

- Proactive,
- Reactive, and
- Hybrid.

2.2.2.3 Proactive Protocols

These protocols use an adaptive system of routing, based on the exchange of control packets. The connectivity among the neighbors is managed by periodically sending the HELLO type messages to keep the links alive. Furthermore, all the network nodes participate in exchanging the topology information, and continuously update the reachability information in the nodes routing tables. In this way, the route is immediately available when requested. The disadvantage of this scheme is that it consumes substantial bandwidth for control traffic and exchange of information, which may never be required.

So proactive protocols are effective when a high percentage of network nodes are source of traffic. Proactive protocols behave rather similar to traditional IP routing protocols; this brings better compatibility with the transport protocols and Internet applications.

2.2.2.4 Reactive Protocols

The reactive routing protocols work passively and do not take initiative for finding a route which is not required. They attempt to discover route only "on demand" by flooding their Query packet. The data packet is put on wait, until the route is found, indicated by the reception of a reply packet from the destination (or from a node having the route to the destination). In this way, resources are not consumed for sending information, which is not required, and once a route is known, bandwidth is consumed mostly for data transmission.

The disadvantage of this technique is that enormous bandwidth is consumed for the global search (flooding) and there are large delays in sending the data packets.

So reactive protocols are effective when a small percentage of network nodes are source of traffic and when network topology is very dynamic.

2.2.2.5 Hybrid Protocols

The hybrid routing protocols adopt a mixture of proactive and reactive schemes or a derivative of one, by optimizing either of the two routing techniques. Mostly the currently proposed protocols in MANET group the nodes in zones or clusters to form a sort of hierarchical routing. The routing protocol used inside the zone or cluster is different from the protocol used to find the routes for the destinations outside the zone or cluster. The suitability of these type of protocols greatly depends upon the network requirements and conditions, and hence it is seen that it is difficult to specify the application domain of the hybrid protocols, and therefore any optimization done is also arbitrarily dispersed.

2.2.3 Examples of Existing Protocols

Several protocols are discussed below in some detail.

2.2.3.1 Reactive Protocols

2.2.3.1.1 Temporally Ordered Routing Algorithm (TORA) – NRL / Washington

TORA is a reactive protocol in the MANET framework [2]. Its aim is to minimize the control traffic overhead for routing. Therefore, it provides minimal routing functionality, which gives multiple, loop free routes, which may not necessarily be the optimal routes. It also tries to establish routes as quickly as possible. To help reducing the control traffic, it minimizes the algorithmic reactions to the topological changes by reacting only when necessary and does not respond to all link changes. It also tries to localize the effect of a link change.

The protocol is best suited for very large networks, with a limited bandwidth. Because of its reactive nature, it generates a huge amount of flooding in search of a route. This makes it unsuitable for the real time, delay-constrained traffic. It tolerates the mobility of the nodes causing link breakage, without generating any control traffic, as long as this mobility does not affect the currently active routes.

The functioning of TORA is based on flooding the Query packet when a route is needed for a destination. This flooding of the Query packet is replied with an Update packet by a node, which is a neighbor of the destination node. While the Update packet passes through the network to arrive at the source node, each node in the way form a route towards the destination by directioning their links. A concept of "height" of a node is used to determine its downstream and upstream links for a specific destination. The actual data packet is transmitted when the source receives the update packet, and a route is established to the destination.

The maintaining of the routes is done using a "link-reversal" algorithm, when a node no more has a route to a destination because of a link breakage. If a partition is detected in this process, the routes are erased for that destination.

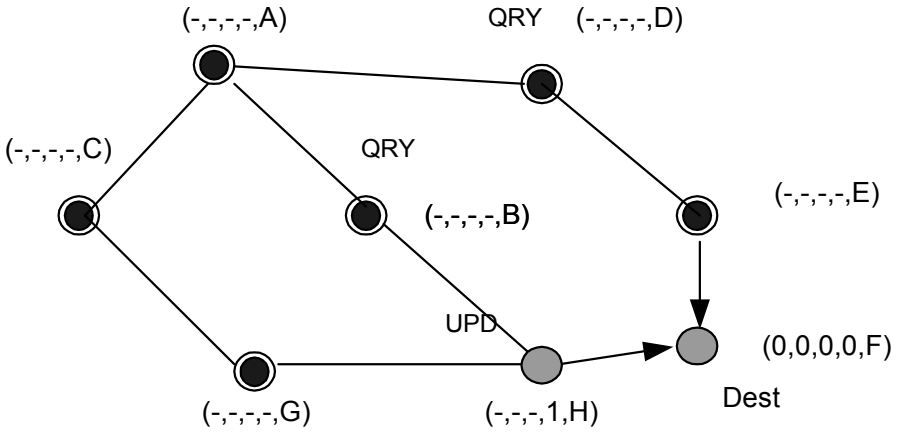

Figure 2-3: An Example of Route Searching in TORA.

2.2.3.1.2 Dynamic Source Routing (DSR) – Dave Johnson / Carnegy Melon

DSR is another reactive protocol presented in the MANET working group [3]. The protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad-hoc network. No periodic messaging is required, and no reaction to unconcerned changes in the topology is shown. The protocol uses the source routing; the complete route is put by the source node in each data packet sent. The advantage of source routing is that the intermediate nodes in the route do not need to maintain any routing information, to forward the packets to the destination. As there are no periodic router advertisements and link status packets, the overhead of DSR is greatly reduced when the network topology is quite stable, where the protocol uses most of the bandwidth for data transmission.

The functioning of DSR is based on flooding the Route Request packet when a route is required for a destination. While this Route Request packet propagates in the network, each node puts its address in the packet header. When this packet reaches the destination (or a node having route to the destination), a Route Reply packet is sent to the source node by inverting the route contained in the Route Request packet. The source then uses this route in each data packet header, it sends.

2.2.3.1.3 Ad-hoc On-Demand Distance Vector (AODV) – C. Perkins / NOKIA / Project RoofTop

AODV provides quick, loop free convergence [4]. It uses the Distance Vector algorithm by introducing a new concept of "Destination Sequence Number" to avoid the problems associated with the Distance Vector algorithm. It has triggered updates and tries to minimize the latency for the route replies, which is a characteristic of the reactive protocols.

The functioning of AODV is also based on flooding the Route Request packet in search of route for a destination. While this Route Request packet propagates in the network, a reverse route to the source is established along the way. When this packet reaches the destination (or a node having route to the destination), a Route Reply packet is sent, in unicast, to the source node using this reverse path.

The maintenance of routes is done only for the active routes. AODV also has its multicast routing protocol.

2.2.3.1.4 Pro-Active Protocol

Proactive protocols are here discussed.

2.2.3.1.4.1 Optimised Link State Routing Protocol (OLSR) – Paul Muhlethaler / INRIA

OLSR is a pro-active protocol to support the large, dense mobile networks, with high nodal mobility and topological changes [5]. The protocol is based on the link state algorithm, and hence inherits the stability of the algorithm. It uses the concept of multi-point relays to calculate the route towards any destination in the network. The multi-point relays provide the optimal routes, and due the pro-active nature of the protocol, these routes are immediately available, when needed.

The protocol is best suited for the dense networks, where lot of traffic is going on between different [source, destination] pairs at different times. The change in [source, destination] pair does not generate any extra control traffic, and so the overhead of control traffic is independent of the data traffic pattern (contrary to the reactive protocols).

The functioning of the OLSR protocol is based on periodically diffusing a topology control packet in the network. The volume of this control information is optimized to exchange MPRs (multi-point relays) of a node, instead of all its neighbors. The flooding of these control messages is optimized by using MPR forwarding and hence saves a significant amount of bandwidth in dense networks, by efficiently and selectively re-transmitting the messages. The protocol adapts rapidly to the topological changes, by increasing the frequency of TC packet, when a change in its MPR set is detected. The protocol manages a topology table to gather the network information obtained from the TC packets, and on the basis of this table, it calculates its routing table.

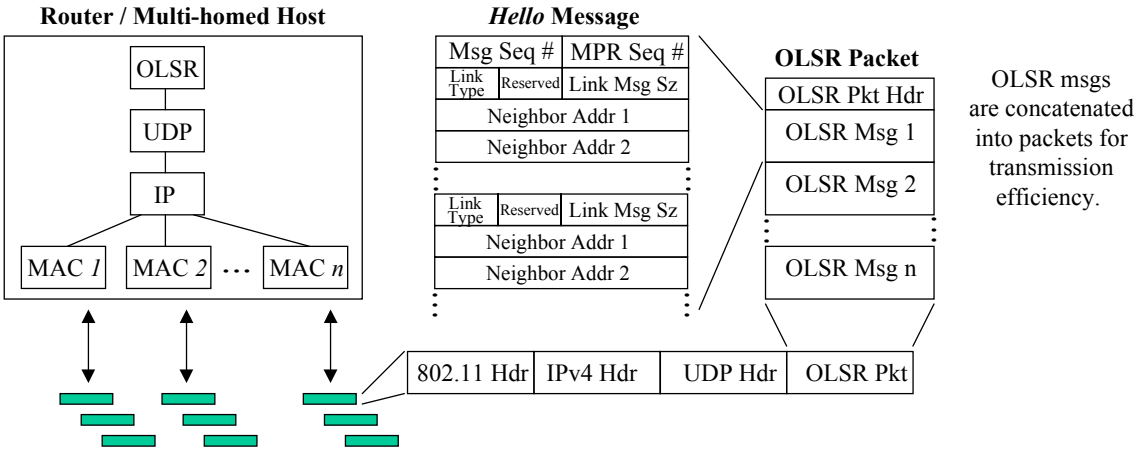

Figure 2-4: OLSR Protocol.

OLSR packets are UDP type and are emitted via port 698. Each frame is made up of the following fields:

- Frame length (in bytes) which is the PDU size;
- Sequence number;
- Type of message, number between 0 and 127 which identifies the information type;
- Message length (in bytes) which is the SDU size;
- Source address;

- TTL (Time to Live), meter which is decremented of 1 with each bound (when TTL=0, diffusion of the frame is stopped);
- Hop count, meter which is incremented of 1 with each bound; and
- Message (payload).

2.2.3.1.5 Topology Broadcast based on Reverse-Path Forwarding (TBRPF) – Richard Ogier / Stanford Research Institute

TBRPF is a proactive, link-state routing protocol designed for mobile ad-hoc networks, which provides hop by hop routing along minimum hop paths to each destination. Each node running TBRPF computes a source tree (providing paths to all reachable nodes) based on partial topology information stored in its topology table, using a modification of Dijkstra's algorithm. To minimize overhead, each node reports only part of its source tree to neighbors. This is in contrast to other protocols in which each node reports its entire source tree to neighbors. TBRPF uses a combination of periodic and differential updates to keep all neighbors informed of the reportable part of its source tree. Each node also has the option to report additional topology information (up to the fill topology), to provide improved robustness in highly mobile networks. TBRPF performs neighbor discovery using « differential » HELLO messages which report only changes in the status of neighbors. This results in HELLO messages that are much smaller than those of other link state routing protocols.

2.2.3.1.5.1 Hybrid Protocols

Next we discuss Hybrid protocols, where one attempts to combine the best properties of the proactive and reactive ones.

2.2.3.1.5.2 Hierarchical Routing for Large Networks

The case of large networks in handled first.

Large multi-hop shared channel radio networks have the problem of a reduced available bandwidth. As the number of network nodes increases, the available bandwidth per node decreases, making the already scarcely available bandwidth a precious resource. Proactive protocols tend to reduce the performance in very large networks by constantly consuming an important part of bandwidth for the link state updates. The reactive protocols, on the other hand, works well as long as there is no link change, but they paralyze the whole network for sometime by their Query flooding in search of a route. Hierarchical routing may be a better option in these large networks. The nodes of the network are grouped into clusters, which are grouped into superclusters, and so on.

Hierarchical routing is employed in variety of ways. Generally, the hierarchical routing protocols hide the details of faraway parts of the network from the nodes. In some implementations, the information about faraway parts of the network may be transmitted less frequently, while the local information is send more rapidly. Yet another form of hierarchical routing involves sending information to the nodes that need it.

The main issues in the hierarchical algorithms requires a description of how the clusters or superclusters are formed, how the cluster membership is advertised, how the routes are computed, and once the routes are established, how the data packets are forwarded.

2.2.3.1.5.3 Zone Routing Protocol (ZRP)

ZRP is hierarchical routing protocol presented in the MANET working group [6]. It is suitable for a wide variety of mobile ad-hoc networks, especially those with large network spans and diverse mobility

patterns. It has an adaptive behavior to set its functioning according to the actual network requirements. It uses a proactive scheme to build routes in its zone (with the radius of x hops), and applies a reactive scheme to find routes outside of its zone (more than x hops away).

A Zone Radius, in number of hops, is defined for the network, taking into account the network mobility, rate of topological changes and the traffic conditions. Then the Routing Zone is defined for each node, and includes the nodes whose minimum distance is less than or equal to the zone radius. Nodes whose distance is exactly equal to the zone radius are called the Peripheral Nodes. IARP (IntrAzone Routing Protocol) provides routes to destinations within the zone radius. IARP works in a pro-active manner and has the up to date routing information for its zone. When a destination node is not found in the zone, a route request message is "bordercasted" to the Peripheral nodes. Bordercasting is an operation of sending a query to all or some of its Peripheral nodes. To search the route, the peripheral nodes use IERP (IntErzone Routing Protocol), which provides routes to destinations outside the source's routing zone. IERP uses "bordercasting" at each instance, to search the routes, on-demand.

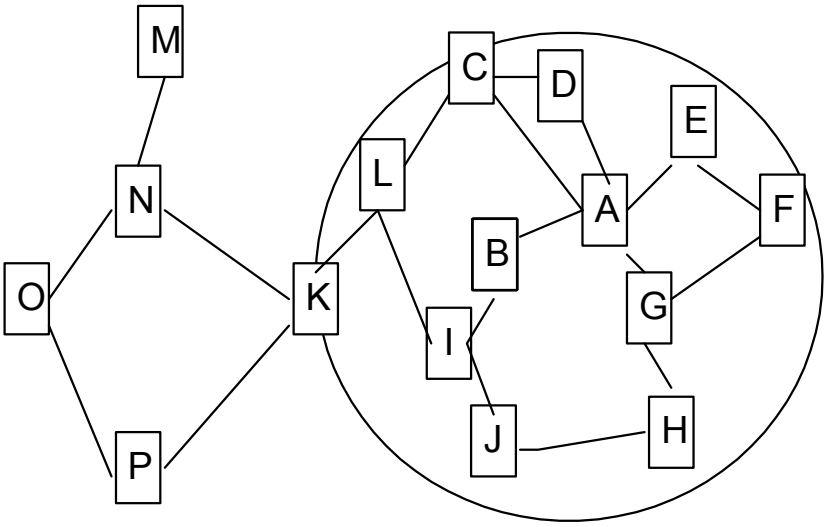

Figure 2-5: ZRP Functioning.

ZRP can be configured for a particular network by proper selection of a single parameter, the routing zone radius.

2.2.3.1.5.4 Cluster Based Routing Protocol (CBRP)

CBRP is a hybrid protocol, using 2-level hierarchical routing [7]. The nodes of the network dynamically group themselves into clusters, by selecting a cluster head. The cluster head has a complete information of the cluster topology, which it transmits to each cluster member. The clusters are joined with the "Gateway" nodes, common to the adjacent clusters. Cluster head knows inter-cluster link state topology through the gateway nodes.

CBRP discovers routes on-demand, with less flooding traffic as the Query is passed only through the cluster heads and the Gateway nodes. When a route is established, the cluster heads can optimize it afterwards, using their topology information, by creating the route between the nodes without passing through the cluster head. CBRP is suitable for middle to large networks with slow node movements, so as to stabilize in finite time with cluster formation.

2.3 CONCLUSION

Clearly mobile radio routing is in the scope of military network applications. More precisely it seems that most of related applications must concern communications in operational units at the bottom of the hierarchy like squadrons.

Numerous technical issues concerning "Mobile Radio network" are primarily the result of the scarce bandwidth of radio. That calls for new routing protocols. Now, we only have proprietary solutions to this issue most of them work at the MAC layer. MANET offers the opportunity to develop a standardized solution to this issue based on routing at the IP layer. This can be considered as an alternative to the use of MAC routing proprietary protocols and to the use of existing IP standards such as OSPF, which are not designed for this type of use.

For military use, MANET proactive protocols seem to be better if we consider that among a tactical network, a lot of users set up communications.

MANET reactive protocols seem to be better on low bandwidth subnetworks (i.e. radio networks), if the density of users is low.

2.4 TECHNICAL SPECIFICATIONS OF A FRENCH MANET TESTBED

2.4.1 Introduction

This section contains the technical specifications of the French MANET (Mobile Ad-hoc NETwork)/ OLSR demonstrator implementing the OLSR routing protocol (version 7). It contains descriptions of demonstrator functionalities, of the hardware and software delivered and description of the demonstrator architecture. The version described here has been implemented as a CELAR testbed on end of December 2002.

2.4.2 MANET/OLSR Demonstrator Features

The MANET/demonstrator features PDAs, laptops, OLSR routers, wireless devices, IP packets, and routing, as explained below. A functional overview of MANET demonstrator is described in Figure 2-6 (although laptops are not represented on this figure).

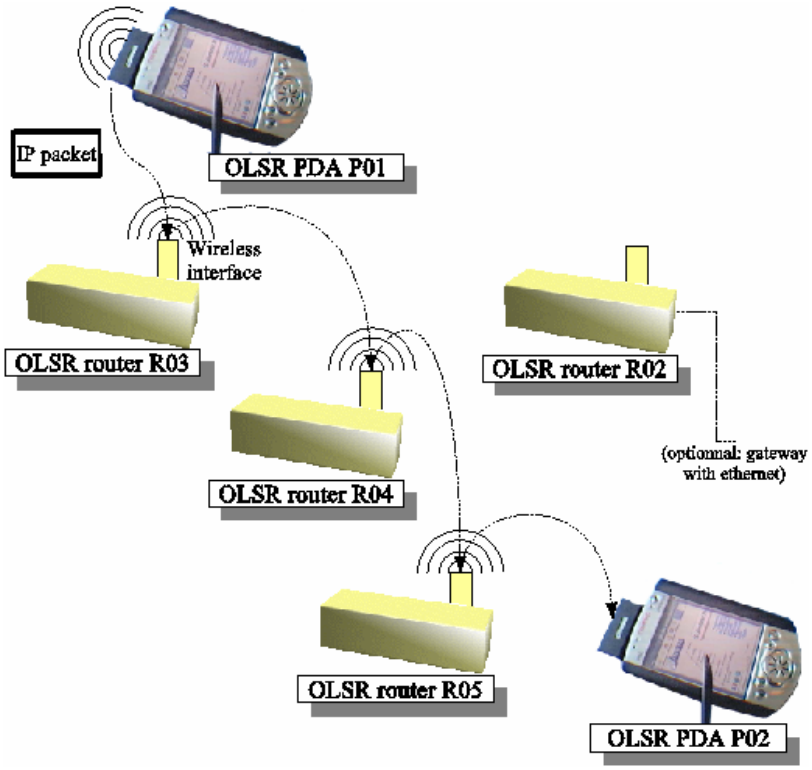

Figure 2-6: MANET/OLSR Demonstrator.

A number of equipments, including standard PDAs, standard laptops, and specific OLSR routers are, each, using wireless networking devices. Those wireless networking devices are used for data transmission using the standard IP protocol, over radio waves. The applications simply use the usual IP networking API. A pre-eminent feature is the ability to perform IP routing, using the wireless routing: that is, when the wireless range is too small for one machine to directly reach another one, an IP packet can, instead, go from machine to machine so that the destination is reached. For instance, on Figure 2-6, the data packet from the PDA P01, would go first to OLSR router R03 by the wireless interface, then will be repeated by R03 to reach router R04, then again from R04 to R05, and finally from R05 to the PDA P02.

The task of setting up IP routing is entirely delegated to the OLSR protocol: using discovery of other machines which are within range, and propagation of that information to the entire network, OLSR is able to set up routes from any machine to any other, provided that at least a path exists (i.e. the network is connected). In addition, OLSR performs this operation dynamically, allowing for low update delays, and hence for mobility. The entity performing the OLSR routing, the OLSR daemon, is central to the demonstrator.

We give an overview of the daemon in the immediately following section ; in the later sections, the demonstrator equipment, which is mostly the environment necessary to run that daemon, is specified. 2.2 OLSR routing. As it was said, the central piece of the demonstrator is the OLSR daemon, which sets up the routing. Figure 2-7 illustrates the inner workings of the OLSR routing.

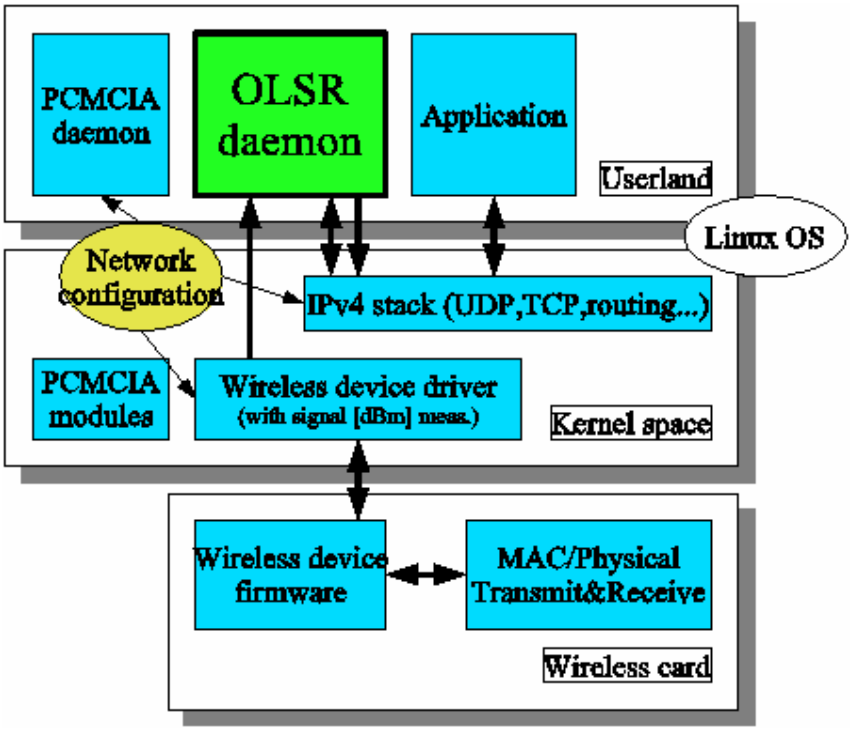

Figure 2-7: OLSR Implementation: The OLSR Daemon.

It is a piece of software running at the application level on the Linux Operating System. This OLSR daemon has three different interactions with the OS:

- It transmits and receives UDP packets (like a standard UDP application), as part of its normal behavior, for discovery of the wireless network topology.
- It configures the IP routes to each discovered destination of the wireless network. The information about the routes is kept in the kernel as part of ``routing table'' of the IP stack. Each "route" is the following information: for a given IP destination address, what is the next hop, that is, the IP address of the machine within range to which we should send the packet 1. On the Figure 2-1, on PDA P01, the next hop for reaching P02 is router R03.
- It can optionally get some meta-information from the driver about UDP packets received: what is the signal/noise with which they were received.

Figure 2-7 shows the main entities involved in the OLSR routing, i.e.:

- The OLSR daemon, implementing a version of the OLSR protocol;
- The kernel which is performing kernel-level tasks, and offers a kernel API;
- An IPv4 stack, part of the kernel, which handles TCP and UDP protocols and encapsulation, IP packet transmission/reception, and IP routing;
- The PCMCIA subsystem, part of the kernel, which allow communication with the wireless device;
- The wireless driver, part of the kernel, which interfaces with the wireless device;
- The wireless device performing MAC/physical transmission; and
- The applications using IP networking, thus implicitly using IP routing.

This results into the following software and hardware requirements:

- Because the OLSR daemon must run on all machines, and it is currently implemented using some Linux kernel API, all machines of the demonstrator are running Linux – including laptop and PDAs. The use of Linux also constrains the hardware.
- Because the PCMCIA configuration scripts, and networking configuration systems are different from one Linux distribution to another, a single fixed distribution is required for each kind of system.
- Because again of inconsistent kernel configuration (routing, ICMP redirection), but also because some low-level improvements are added in the wireless device driver, a fixed kind of driver is required (and shipped).
- Because the wireless device must be supported by the device driver, the choice of those devices is constrained.

2.4.3 Demonstrator Overview

The MANET/OLSR demonstrator includes the following hardware:

Equipment Type	Quantity	System	Linux Distribution
Olsr Router	10	(shipped by INRIA)	(shipped by INRIA)
PDA	4	iPAQ ARM	Distribution Familiar
Laptop	4	Sony VAIO	Distribution Debian 3.0

The demonstrator software includes:

Software	Description	Equipment
OLSR daemon	OLSR protocol version 7	PDA, Laptop, OLSR Router
iperf	Network performance tool	Laptop, OLSR Router
netperf	Network performance tool	Laptop, OLSR Router
Misc. monitoring software	Network performance tool	Laptop

2.4.4 Network Configuration

The IP networking configuration is the following:

Network Type	IP Addresses
Ethernet	10.103.96.0/24
Wireless	10.103.97.0/24

2.4.5 Wireless Network Specification

The wireless radio interfaces used are standard 802.11b interfaces. The technical specifications of the cards are:

Wireless device	PCMCIA, Avaya Wireless PC Card (Silver) (previous versions sold as “Orinoco Silver” and “Lucent Technologies Silver”)
Compatibility	IEEE 802.11b Standard for Wireless LANs (DSSS)
Firmware	Tested with versions 6.04 and 7.52
MAC	CSMA/CA
R-F Frequency Band	2.4 GHz (2400-2500 MHz)
Used sub-channel	Channel 11 (2462 MHz)
Modulation technique	Direct Sequence Spread Spectrum
	CCK (11 and 5.5 Mbps), DQPSK (1 Mbps)
	DBPSK (1 Mbps)
Spreading	11-chip Barker Sequence
Bit Error Rate	Better than 10-5
Nominal Output Power	10 dBm

The reported radio characteristics, range, sensitivity, delay spread are the following:

Data bit rate	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open office	160 m	270 m	400 m	550 m
Semi-open office	50 m	70 m	90 m	115 m
Closed office	25 m	35 m	40 m	50 m
Receiver sensitivity	-83 dBm	-87 dBm	-91 dBm	-94 dBm
Delay spread	65 ns	225 ns	400 ns	500 ns

2.4.6 Ad-hoc Mode

The wireless radio cards are run in a special mode, called the “Ad-Hoc” mode or “Ad-Hoc demo mode”. This mode is not a standard WiFi mode: neither the “infrastructure mode” nor the “Ad-Hoc IBSS” mode. But it is supported on many cards, including the Lucent derivated and the numerous Prism II derivated cards, because it is simply removing all the management/beaconing frames.

2.4.7 Systems Technical Specification

2.4.7.1 OLSR Router Specification

Figure 2-8: OLSR Router.

Here is a summary of the features of the routers:

Hardware	PC mini-motherboard
Processor	486 133 MHz
Memory	16 MBytes
Hard drive	None, 16 MBytes Flash memory instead
Networking	Ethernet NE2000 compatible, 10 Mbps
Wireless Networking	via PCMCIA adapter
System	Linux kernel 2.4.19
	binaries based on Slackware 7.0, 7.1 and 8.0

The OLSR router includes a Linux system, which is a system, based on Slackware 7.0, 7.1 and 8.0, which can be used by direct login (when plugging in a monitor and a keyboard) or via network by telnet.

2.4.7.2 Linux Laptop Specification

The laptop is a VAIO on which Linux is installed. The specifications are as follows:

Hardware	Sony VAIO PCG-C1MHP-FR
Processor	Transmeta Crusoe TM5800 at 867 Mhz
Memory	256 MBytes
Hard drive	30 GBytes
Networking	Ethernet 10/100 Mbps
Wireless Networking	via PCMCIA adapter (or Bluetooth)
System (2*OS)	Windows XP & Linux kernel 2.4.19
	LINUX Distribution Debian 3.0

The following software from the Debian 3.0 distribution is necessary:

Software	Usage
kernel 2.4.19	a recent version of the kernel
pcmcia-cs 3.1.22+	*for PCMCIA adaptor*
orinoco module	for PCMCIA wireless card
wireless-tools (23-2+)	*for wireless card configuration*
xirc2ps	for Xircom Ethernet device
python (2.2)	for scripts and OLSR
minicom	*for communication with iPAQ via serial*
iproute	for advanced routing configuration

2.4.7.3 Linux PDA Specification

The PDA is a iPAQ on which Linux is installed. The specifications are as follows

Hardware	Compaq iPAQ Pocket PC H3950
Processor	Intel PXA 250 at 400 Mhz
Memory	64 Mbytes SDRAM
Hard drive	None, 32 MBytes Flash memory instead
Networking	via PCMCIA adaptor
Wireless Networking	via PCMCIA adaptor
System	Linux kernel 2.4.19
	Familiar v0.6.1
Extension	PCMCIA adaptor
iproute	for advanced routing configuration

The following software from the Familiar v0.6.1 distribution is necessary:

Software	Usage
kernel 2.4.19	a recent version of the kernel
pcmcia-cs	*for PCMCIA adaptor*
orinoco module	for PCMCIA wireless card
wireless-tools (21-1.3+)	*for wireless card configuration*
xirc2ps	for wireless card configuration
python (2.2)	for scripts and OLSR
Complete compilation chain	for recompiling kernel, modules and OLSR
Complete cross-compilation chain	for cross-compiling kernel, and modules

2.4.8 Software

2.4.8.1 Overview

The following software is included:

Software	Description
olsrd and python_olsrd	The basic version of the OLSR daemon and the version with HTTP interface (port 11698)
netperf	Network performance tool
	Client and server (running on default port)
iperf	Network performance tool
route, ifconfig, iwconfig, ...	Standard Linux/Unix tools

- All IP networking applications should work, if they are not using broadcast addresses.
- All standard IP tools should be working, including route, ip, traceroute, ping, telnet.
- The tool netperf is shipped. It allows for TCP and UDP performance measurements.
- The tool iperf is shipped. It allows also for TCP and UDP performance measurements, although with different options, and different result presentation.

2.4.8.2 OLSR

The OLSR daemon shipped is compliant with the version 7 of the OLSR RFC draft (http://hipercom.inria.fr/olsr/draft-ietf-manet-olsr-07.txt). It exists in two versions, one with the name olsrd (or std_olsrd), and one with the name python_olsrd. The second might not be available for PDAs; the difference between the two versions is that the second one adds an HTTP interface, which can be used to monitor the status of a given OLSR daemon, as illustrated on Figure 2-9.

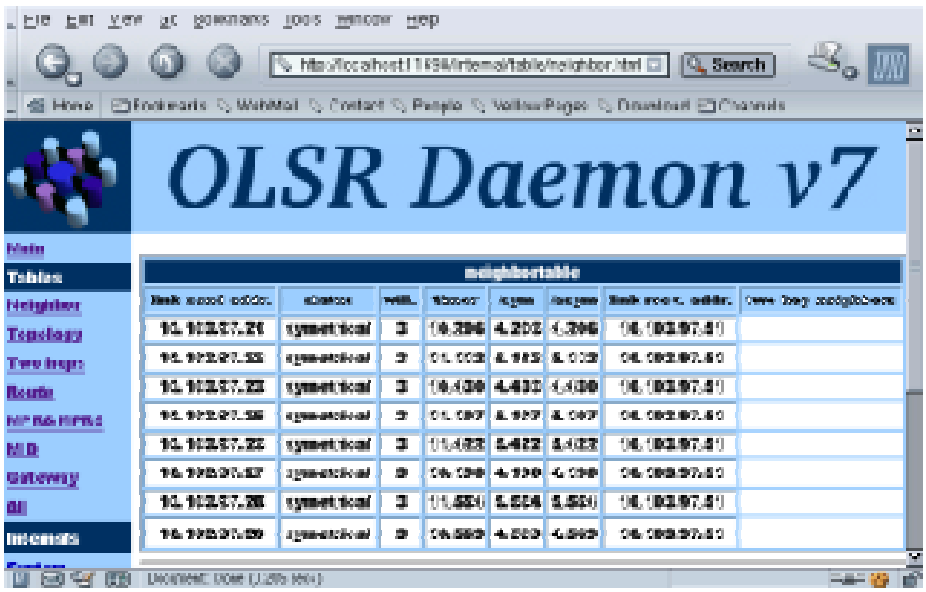

Figure 2-9: A WEB Interface to the OLSR Daemon (python_olsrd).

Version	Draft version 7
Protocol port	1680 (non-standard, standard is 698)
HTTP interface port	11698

2.4.9 References

OLSR page	http://hipercom.inria.fr/olsr/
MANET page	http://www.ietf.org/html.charters/manet-charter.html
Linux kernel	http://www.kernel.org/
Linux PCMCIA system	kernel or http://pcmcia-cs.sourceforge.net/
Linux and wireless devices	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
Debian	http://www.debian.org/
Linux on laptops	http://www.linux-laptop.net/
Linux on VAIO C1MHP	http://this.is.not-mediaways.net/but.i.am/flo/c1mhp/
Linux on PDAs	http://www.handhelds.org/
Linux familiar (iPAQ)	http://familiar.handhelds.org/
`netperf`	http://www.netperf.org/
`iperf`	http://dast.nlanr.net/Projects/Iperf/

2.4.9.1 Demonstrator Architecture (Scenario)

On the figure below, only the 10 INRIA OLSR routers are represented. The 4 mobile PDA terminals and 4 mobile VAIO terminals are not represented.

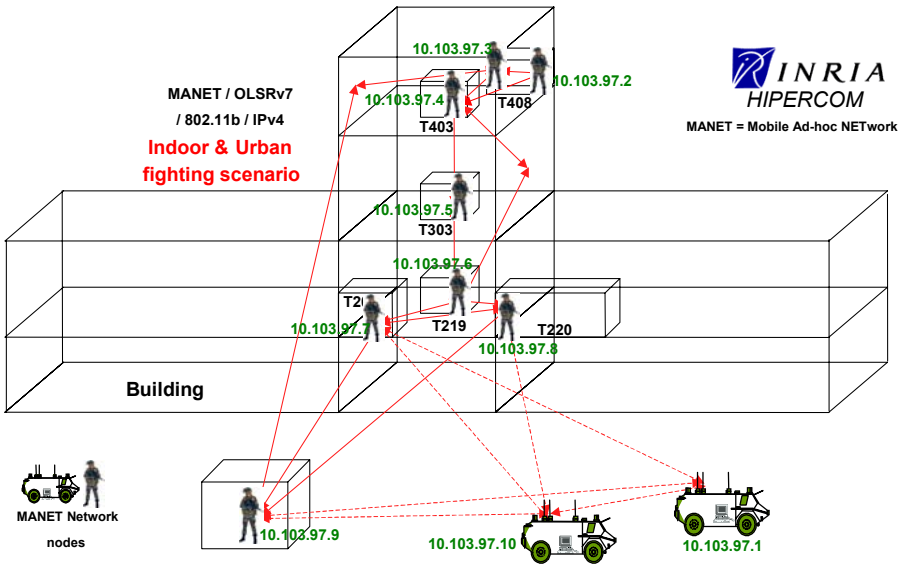

Figure 2-10: Demonstrator Architecture.

In room T408 (level 4), OLSR router (@ 10.103.97.2) is the gateway to INSC wired network.

2.4.9.2 INSC Interconnection Architecture

The figure below shows the interconnection, through FreeBSD router and 6Wind access router, between OLSR CLAN (Coalition LAN) and INSC wired network. The function of FreeBSD router is to set up IPv4/IPv6 tunnels: latest version of OLSR network – version 7, runs with IPv4, and INSC network is IPv6. the 6Wind router is the access router to IPv6 INSC network; it provides security and Quality of Service (QoS).

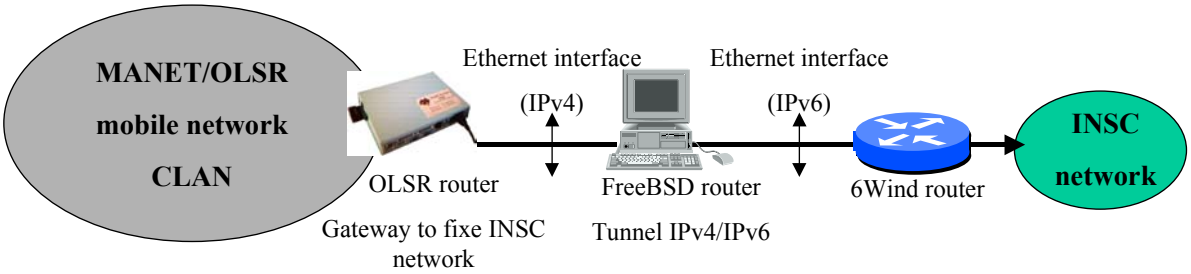

Figure 2-11: INSC Architecture.

2.5 FRENCH PR4G SAP AD-HOC NETWORK

2.5.1 Introduction

This section contains an overview of French PR4G SAP ad-hoc network. PR4G is a French military radio. SAP mode for "Packets Access Service (PAS)". SAP mode is one of modes implemented on the PR4G.

2.5.2 SAP/PAS Network Oriented Mode

PR4G SAP radio (Packet Radio Network) has the following features:

- Slotted Aloha Channel Access;
- Multiple Selective Call;
- Message Transmission (up to 63 kbps);
- Automatic Data Rate Management;
- Mono-Transceiver routing; and
- Up to 59 Pax and 10 relays.

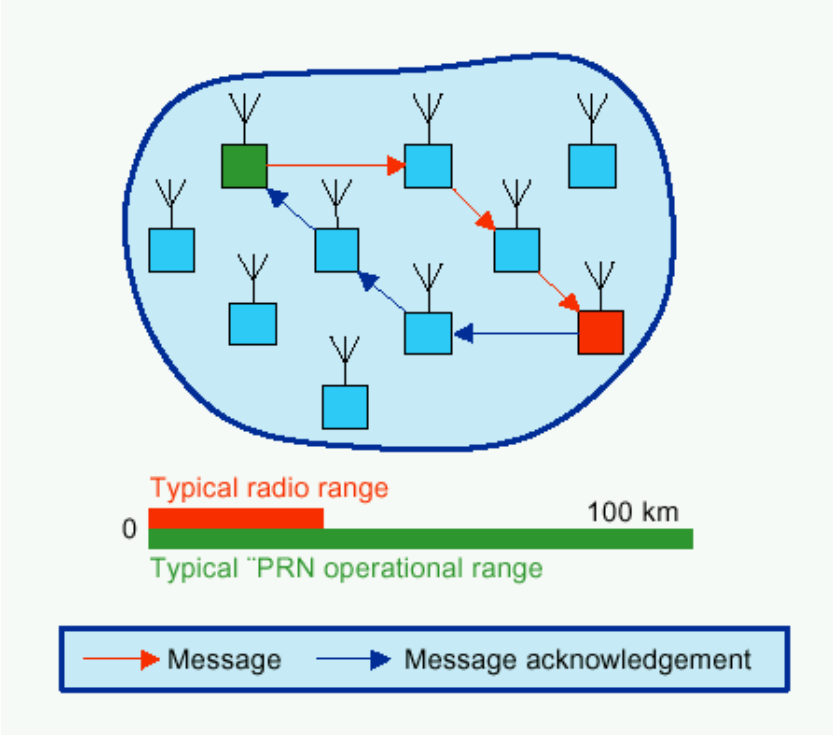

Figure 2-12: SAP/PAS.

Due to its robustness, flexibility and ability to cover large areas, Packet Radio Network technology is seen as the future for non-real time battle-field data transmission, such as Message Handling Systems (Electronic Mail).

2.5.3 Packet Radio Mode

2.5.3.1 Principles

Data communication over extended ranges via automatic routing through different CNR.

2.5.3.2 Advantages

- Fully automatic flood search routing and flow control; and
- Flexible reconfiguration capability.

2.5.3.3 Implementation

- Each subscriber T/R used as a relay station; and
- Application procedures managed externally by computer.

2.5.4 PRNET with PR4G

PRNET is one among the many possible applications using the parameterized general purpose packet data transmission mode embedded in the radio set. The Packet access service inside the radio set has the function of synchronization, coding and interleaving, channel access, packet routing. All real time functions taking advantage of transmitting synchronization and FH facilities.

The PRNET application outside the radio set provides segmentation of message, end to end message acknowledgement and management functions (routing update, flow control, data rate selection).

2.5.5 Packet Radio Application (Routing)

For any destination node, each (relaying) node computes a standard list (neighbor stations in the shortest paths – e.g. "to node z: B or C with 2 hops"), a fallback list (neighbor stations in almost shortest paths – e.g. "to node z: A or D with 3 hops").

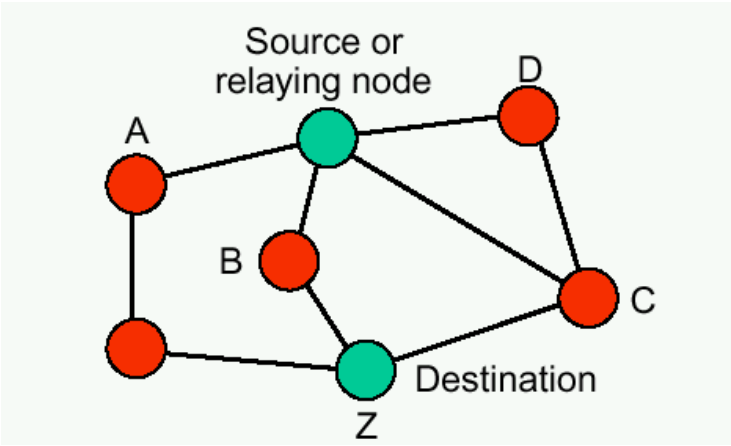

Figure 2-13: Packet Radio Application Routing.

2.5.6 Packet Radio Application Providing Routing Adaptivity

The general idea is depicted through the example below

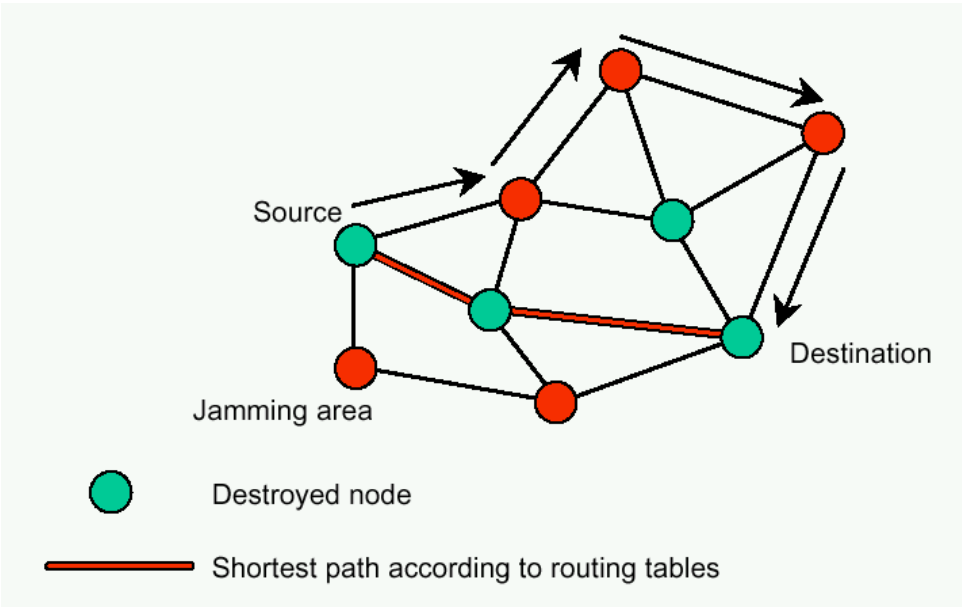

Figure 2-14: Packet Radio Routing.

2.5.7 Synchronization and User Traffic Principles

The channel access slotted based on 100 ms slots (as in TDMA mode). The features of synchronization is the following:

- No master; based on a distributed algorithm;
- Sent in dedicated sync slots; and
- Uses the main hopping channel.

For the User traffic, one have a random slot access using the main channel, and the traffic is sent in a virtual hopping channel (as in selective call mode), ensuring no risk of contention.

2.5.8 Routing Principles

- Broadcast of tables at regular periods of time; and
- Flood-search algorithm to define the optimum routing.

Figure 2-15: PR4G SAP.