Institut Eurecom[1]
Department of Mobile Communications
2229, route des Crêtes
B.P. 193
06904 Sophia Antipolis
FRANCE

Research Report RR-08-217

IPv6 mobility and ad hoc network mobility overview report

March 20th, 2008

Giuliana IAPICHINO
Prof. Christian BONNET

Tel: (+33) 4 93 00 82 52
Fax: (+33) 4 93 00 82 00
Email: {Giuliana.Iapichino, Christian.Bonnet}@eurecom.fr

[1] Institut Eurecom research is partially supported by its industrial members: BMW Group Research & Technology – BMW Group Company, Bouygues Telecom, Cisco Systems, France Telecom , Hitachi, SFR, Sharp, STMicroelectronics, Swisscom, Thales

TABLE OF CONTENTS

List of figures

1 INTRODUCTION

1.1 Scope of the Document

The scope of this document is to provide an overview on mobility mechanisms adopted in IPv6 networks as well as used in ad hoc networks, in order to have a complete view on the state of the art of mobility management. It will help in the identification of the most promising mechanisms for mobility support in Public Safety applications and in the definition of the future research line of the Ph.D. thesis.

1.2 Structure of the Document

The document starts, in section 2, with an overview on main characteristics of IPv6 protocol for mobility support. State of the art of the most important mobility mechanisms in IPv6 networks, like Mobile IPv6, HMIPv6, MIPv6 Fast Handover and Proxy MIPv6, is also provided.

Section 3 describes Mobile Ad Hoc Networks (MANETs), address autoconfiguration techniques and ad hoc routing mechanisms used in flat, hierarchical and geographical type of architecture for MANET.

Section 4 introduces Wireless Mesh Networks (WMNs) and underlines the importance of using such type of network structure for emergency applications. A quick presentation on 802.11s proposal is also provided.

Finally a conclusion on which mobility mechanisms and network architectures based on IPv6 are promising for emergency applications and need further investigation is presented.

2 IPV6 MOBILITY

2.1 IPv6 features for mobility support

IPv6 is an evolution of IPv4. The protocol is installed as a software update in most devices and operating systems. When buying up-to-date hardware and operating systems, IPv6 is usually supported and needs only activation or configuration. Current available transition mechanisms allow the step-by-step introduction of IPv6 without putting the current IPv4 infrastructure at risk.

Here is an overview of the main changes [1]:

- Extended address space: the address format is extended from 32 bits to 128 bits. This provides an IP address for every grain of sand on the planet. In addition, it also allows for hierarchical structuring of the address space in favour of optimized global routing.
- Autoconfiguration: probably the most interesting new feature of IPv6 is its *Stateless Autoconfiguration* mechanism. When a booting device in the IPv6 world comes up and ask for its network prefix, it can get one or more network prefixes from an IPv6 router on its link. Using this prefix information, it can autoconfigure for one or more valid global IP addresses by using either its MAC identifier or a private random number to build a unique IP address. In the IPv4 world, it is necessary to assign a unique IP address to every device, either by manual configuration or by using DHCP. Stateless autoconfiguration also allows for easy connection of mobile devices, such as mobile phone or handheld, when moving to foreign networks.
- Simplification of header format: the IPv6 header is much simpler than the IPv4 header and has a fixed length of 40 bytes. This allows for faster processing. It basically accommodates two times 16 bytes for the Source and Destination address and only 8 bytes for general header information.
- Improved support for options and extensions: IPv4 integrates options in the base header, whereas IPv6 carries options in so-called *extension headers,* which are inserted only if they are needed. Again, this allows for faster processing of packets. The base specification describes a set of six extension headers, including headers for routing, Mobile IPv6, quality of service and security.

Hereafter, important features for mobility support in IPv6 are described.

2.1.1 IPV6 NEIGHBOR DISCOVERY

One of the key functionalities of IPv6 is Neighbor Discovery (ND) specified in [2]. IPv6 network nodes apply Neighbor Discovery to discover their neighbor nodes, for example, to determine which hosts and routers are available on-link or which link layer address a specific neighbor has got.

Neighbor Discovery enables the following functionalities:

- Router Discovery: hosts detect routers attached to the link by applying Router Discovery.

- Prefix Discovery: nodes need to know the on-link prefixes to distinguish destinations that reside on-link from those only reachable through a router.
- Parameter Discovery: this functionality enables nodes to learn parameters like the link MTU or the hop limit value.
- Address Autoconfiguration: it is used by nodes to automatically configure an IP address for an interface.
- Address Resolution: it is the process of obtaining information about the relation of link-layer address and IP address of a neighboring node.
- Next-hop determination: this algorithm is for mapping an IP destination address into the IP address of the neighbor to which traffic for the destination should be sent.
- Neighbor Unreachability Detection (NUD): NUD enables nodes to determine that a neighbor is no longer reachable.
- Duplicate Address Detection (DAD): DAD is used by nodes to verify that an address it wishes to use is not already in use by another node.
- Redirect: A router sends a Redirect message to inform a host of a better first-hop node to reach a particular destination.

In Neighbor Discovery five different message types are used:

- Router Solicitation: nodes send out Router Solicitations to query a router to reply with a Router Advertisement, including information for autoconfiguration.
- Router Advertisement: Router Advertisements are sent by routers periodically or as reply to a Router Solicitation message. Router Advertisements signal the presence of a router on-link and they include configuration parameters for the nodes attached to the link.
- Neighbor Solicitation: Neighbor Solicitations are sent by nodes to discover other nodes on-link.
- Neighbor Advertisement: Neighbor Advertisements are sent as response to Neighbor Solicitation messages.
- Redirect: Redirect messages are sent by routers to inform a host of a better first hop for a specific destination address.

2.1.1.1 Address Resolution

Address resolution is the process of relating the network layer address (e.g. IPv6 address) to the link layer identifier (e.g. MAC address) assigned to a neighbor node's interface.
Why is there a need for link layer identifiers? In case a link is based on a shared medium, sending a link layer packet to the link means each node attached to the link receives the packet. Without link layer address information included in the packet, the nodes cannot evaluate whether the packet is destined for them and would pass the packet to their network layers. The network layer destination address included in the packet addresses the end destination node, which may not be the node itself. Therefore, also the network layer may not be able to determine if it needs to forward the packet. The only option would be that each node forwards the packet to their respective default router. In the end, depending on the number of nodes attached to the shared medium link, the traffic would be multiplied.

A way to cope with this issue is to include a link layer identifier in the link layer header of the packet, identifying the receiver of the packet.

Before delivering a network layer Protocol Data Unit (PDU), a node determines first the next-hop network layer address. Afterwards, a node needs to get knowledge about the next-hop's link layer identifier. There are several ways how to get the relation between next-hop network layer address and next-hop link layer identifier. Manual configuration of a mapping table in each node or querying a central database hosting a mapping table are possibilities.

In IPv6, a node requests this information explicitly from the next-hop node. IPv6 nodes perform address resolution by multicasting a Neighbor Solicitation messages to the link with the solicited-node multicast address corresponding to the next-hop address (target address) as destination address. The header of the message includes the link-local unicast address of the sending interface as source address. The target node returns its link-layer address in a unicast Neighbor Advertisement message addressed to the source address of the received Neighbor Solicitation.

2.1.1.2 Duplicate address detection

With IPv6 stateless address autoconfiguration (see 2.1.2), nodes create IPv6 addresses for their interfaces automatically. Before assigning an IP address to an interface, the IPv6 node evaluates the uniqueness of the IPv6 address by performing Duplicate Address Detection. A node starts this process by multicasting a Neighbor Solicitation message to the link, with the tentative IPv6 address as target address, the unspecified address as source address, and the solicited-node multicast address as destination address. All IPv6 nodes on-link receive that message and determine whether they are already using the given tentative IPv6 address. If this is the case (DAD fails), a node replies with a Neighbor Advertisement message, with a destination address of the all-nodes multicast address. RFC 2462 [3] specifies that if a node performing DAD receives a Neighbor Advertisement as reply it stops the automatically assignment of IPv6 addresses and manual configuration is required.

2.1.1.3 Neighbor Unreachability Detection

An IPv6 node actively tracks the reachability state of its neighbors. NUD is performed only for neighbors unicast packets are sent to. For NUD, only the reachability on the forward path is of interest. Reachability confirmation can be obtained from upper layers, for instance, when a host receives a TCP acknowledgement it can be sure that the corresponding IPv6 packets have reached the next-hop. If reachability information is not provided by upper layers, a node actively probes its neighbors by sending them unicast Neighbor Solicitation messages. After receiving a solicited Neighbor Advertisement message as reply, a node can consider the respective neighbor as reachable.

2.1.1.4 Router and prefix discovery

Router and Prefix Discovery is the process in which IPv6 nodes learn the address of the default router and the IP prefixes that reside on-link. Routers multicast Router Advertisement messages periodically to the all-nodes multicast address. The message contains a list of prefixes that reside on-link and the MTU of the link. Furthermore, a router signals via the Router Advertisement message that it is willing to be a default router by setting a Router Lifetime parameter greater

than zero. Obtaining a prefix, a node gets information about the range of IP address that can be reached via the respective link without going beyond a router.

2.1.2 IPV6 ADDRESS AUTOCONFIGURATION

2.1.2.1 Stateless autoconfiguration

In IPv6 a stateful as well as a stateless autoconfiguration mechanism is specified. In the stateful method hosts request configuration parameters like IPv6 addresses explicitly from a server, which keeps track of all IP addresses assigned to network nodes. Stateless address autoconfiguration means that hosts can configure an upcoming interface without an additional server. In this section stateless autoconfiguration is considered.

Hosts are expected to apply autoconfiguration as specified in [3]. Routers are expected to be configured in a different way (e.g. manually), but the automatic generation of link-local addresses and the performing of Duplicate Address Detection (DAD) is expected. Stateless address autoconfiguration [4] uses the mechanisms of Neighbor Discovery described already in section 2.1.1. A node creates a link-local address for one of its interfaces by prepending the well-known link-local prefix FE80::0 to the interface identifier.
The interface identifier is typically 64 bits long and based on IEEE EUI-64 format. The EUI interface identifier can be derived form the MAC address. After receiving Router Advertisement messages containing prefix information, a node is able to create site-local and global IPv6 addresses for the interface the message is received from. To form a site-local or global IPv6 address the respective prefix is appended by an interface identifier. The prefix length and the interface identifier length (typically 64 bit) must be total 128 bits. Otherwise the automatically creation of an address fails. Before assigning these so created IPv6 addresses to an interface, DAD must be performed. If the DAD process fails, manual configuration is required. DAD expects full multicast capable links. Additionally, an IPv6 node gets default router information from a Router Advertisement. The IPv6 source address (link-local scope) of the router is included in the message which can be used as default router address. A router signals its willingness to be a default router by a RouterLifetime value greater than zero in the Router Advertisement message.

2.1.2.2 Stateful Autoconfiguration

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specified in [5] provides a way for stateful autoconfiguration. DHCPv6 enables servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCPv6 can be used in combination with stateless autoconfiguration to complete the autoconfiguration process. DHCPv6 is a client/server protocol. Clients and servers exchange DHCP messages using UDP. Clients listen for DHCP messages on UDP port 546, servers and relay agents listen for DHCP messages on UDP port 547. Clients use a link-local address obtained through IPv6 stateless autoconfiguration or addresses determined

through other mechanisms as source address in a DHCP communication. In most cases, a client multicasts DHCP messages to the All_DHCP_Relay_Agents_and_Servers address (FF02::1:2). This multicast address has link scope. It is used by a client to communicate with on-link relay agents and servers. All servers and relay agents are members of this multicast group and listen to messages sent to it. If no DHCP server is available on-link, a DHCP relay agent on the client's link may relay messages between the client and server. The operation of the relay agent is transparent to the client.

2.2 Mobile IPv6

Mobile IPv6 (MIPv6) [6] specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. Each Mobile Node (MN) is always identified by its Home Address (HoA), regardless of its current point of attachment to the Internet. While situated away from its home, a MN is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its Care-of Address (CoA). The protocol enables IPv6 nodes to cache the binding of a MN's HoA with its CoA, and to then send any packets destined for the MN directly to it at this CoA. Packets may be routed to the MN using this address regardless of the MN's current point of attachment to the Internet.

The MN may also continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a MN away from its home link is thus transparent to transport and higher layer protocols and applications. The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, MIPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with the MN's IP address remaining unchanged in spite of such movement.

2.2.1 HOW MOBILE IPV6 WORKS

Figure 1 shows the components of MIPv6 and how they interact.
A MN is always expected to be addressable at its HoA, whether it is currently attached to its home link or is away from home. The HoA is an IP address assigned to the mobile node within its home subnet prefix on its home link. While a MN is at home, packets addressed to its HoA are routed to the MN's home link, using conventional Internet routing mechanisms.

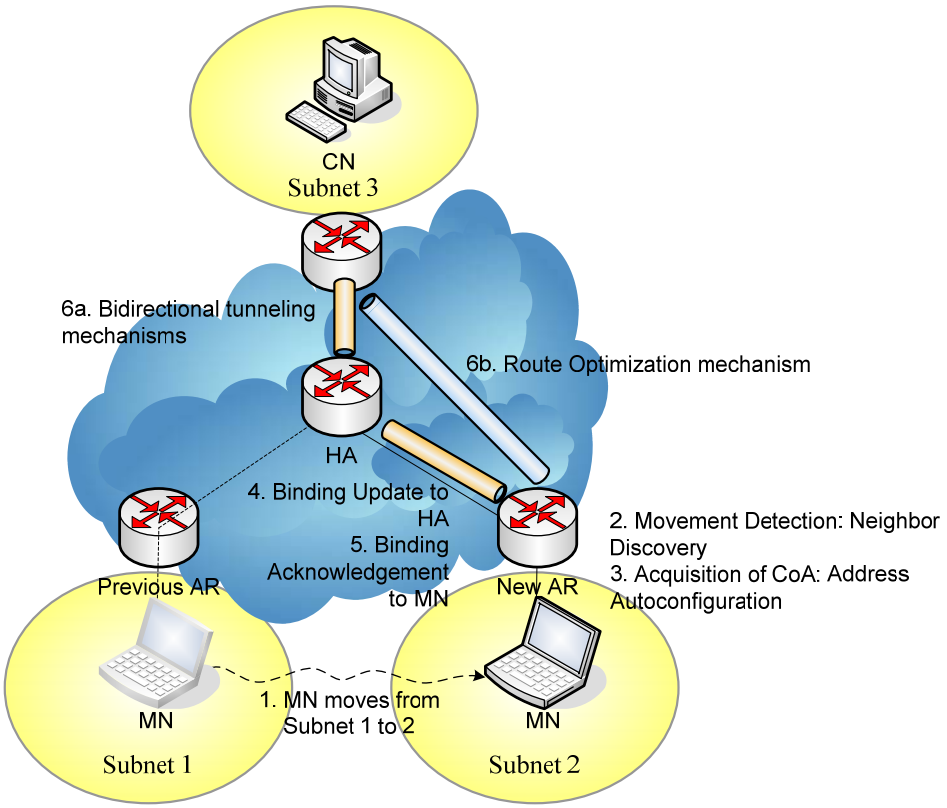

Figure 1: Mobile IPv6

While a MN is attached to some foreign link away from home, it is also addressable at one or more CoAs. A CoA is an IP address associated with a MN that has the subnet prefix of a particular foreign link. The MN can acquire its CoA through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration (see sections 2.1.2.1 and 2.1.2.2). As long as the MN stays in this location, packets addressed to this CoA will be routed to the MN. The MN may also accept packets from several CoAs, such as when it is moving but still reachable at the previous link.

The association between a MN's home address and care-of address is known as a "binding" for the MN. While away from home, a MN registers its primary CoA with a router on its home link, requesting this router to function as the Home Agent (HA) for the MN. The MN performs this binding registration by sending a Binding Update message to the HA. The HA replies to the MN by returning a Binding Acknowledgement message.
Any node communicating with a MN is called a Correspondent Node (CN) of the MN, and may itself be either a stationary node or a mobile node. MNs can provide information about their current location to CNs. This happens through the correspondent registration. As a part of this procedure, a return routability test is performed in order to authorize the establishment of the binding.

There are two possible modes for communications between the MN and a CN.
The first mode, ***bidirectional tunneling***, does not require MIPv6 support from the CN and is available even if the MN has not registered its current binding with the CN. Packets from the CN

are routed to the home agent and then tunneled to the MN. Packets to the CN are tunneled from the MN to the HA ("reverse tunneled") and then routed normally from the home network to the CN. In this mode, the HA uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the MN's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the MN's primary CoA. This tunneling is performed using IPv6 encapsulation [7].

With the second mode, that is ***route optimization,*** the communication between MN and CN can be direct without going through the HA. This is one of the main advantages of MIPv6 over MIPv4, where route optimization is not possible. Route optimization requires that the MN registers its current binding at the CN. Packets from the CN can be routed directly to the CoA of the MN. When sending a packet to any IPv6 destination, the CN checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the MN by way of the CoA indicated in this binding.

2.3 Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [8] is an extension to MIPv6 to improve local mobility handling, reducing significantly the signalling and the handover delay between MN, CN and HA. HMIPv6 is based on the functionalities of a new node called Mobility Anchor Point (MAP), a router located in the network visited by the MN and used by the MN as a local HA.

A MN entering a MAP domain receives Router Advertisements containing information on one or more local MAPs. The MN can bind its current location (on-link CoA) with an address on the MAP's subnet (Regional Care-of Address (RCoA)). Acting as a local HA, the MAP receives all packets on behalf of the MN it is serving and encapsulates and forwards them directly to the MN's current address. If the MN changes its current address within a local MAP domain (On-link Care-of Address (LCoA)), it only needs to register the new address with the MAP. Hence, only the RCoA needs to be registered with CNs and the HA. The RCoA does not change as long as the MN moves within a MAP domain. This makes the MN's mobility transparent to the CN it is communicating with.

2.3.1 HMIPV6 OPERATIONS

As soon as the MN arrives in a new network, it discovers the global address of MAP through Router Advertisement messages sent by the new Access Router (AR) (see Figure 2). This *discovery phase* informs the MN about the presence of a MAP and its distance. The process of MAP discovery continues as the MN moves from one subnet to the next. Every time the MN detects movement, it also detects whether it is still in the same MAP domain. As the MN roams within a MAP domain, it continues to receive the same MAP option included in Router

Advertisements from its AR. If a change in the advertised MAP's address is received, the MN needs to send a Binding Update (BU) to its HA and CN.

When the MN moves in a new MAP domain (*registration phase),* it needs to configure two CoAs: an RCoA on the MAP's link and LCoA. The RCoA is formed in a stateless manner. After forming the RCoA based on the prefix received in the MAP option, the MN sends a local BU to the MAP that includes the MN's RCoA in the Home Address Option. The LCoA is used as the source address of the BU. This BU binds the MN's RCoA (similar to a Home Address) to its LCoA. The MAP (acting as a HA) then performs DAD (when a new binding is being created) for the MN's RCoA on its link and return a Binding Acknowledgement to the MN.

Following a successful registration with the MAP, a bi-directional tunnel between the MN and the MAP is established. All packets sent by the MN are tunnelled to the MAP. The outer header contains the MN's LCoA in the source address field and the MAP's address in the destination address field. The inner header contains the MN's RCoA in the source address field and the peer's address in the destination address field. Similarly, all packets addressed to the MN's RCoA are intercepted by the MAP and tunnelled to the MN's LCoA.

After registering with the MAP, the MN has to register its new RCoA with its HA by sending a BU that specifies the binding (RCoA, Home Address) as in MIPv6. The MN's Home Address is used in the home address option and the RCoA is used as the care-of address in the source address field. The mobile node may also send a similar BU (i.e., that specifies the binding between the Home Address and the RCoA) to its current correspondent nodes.

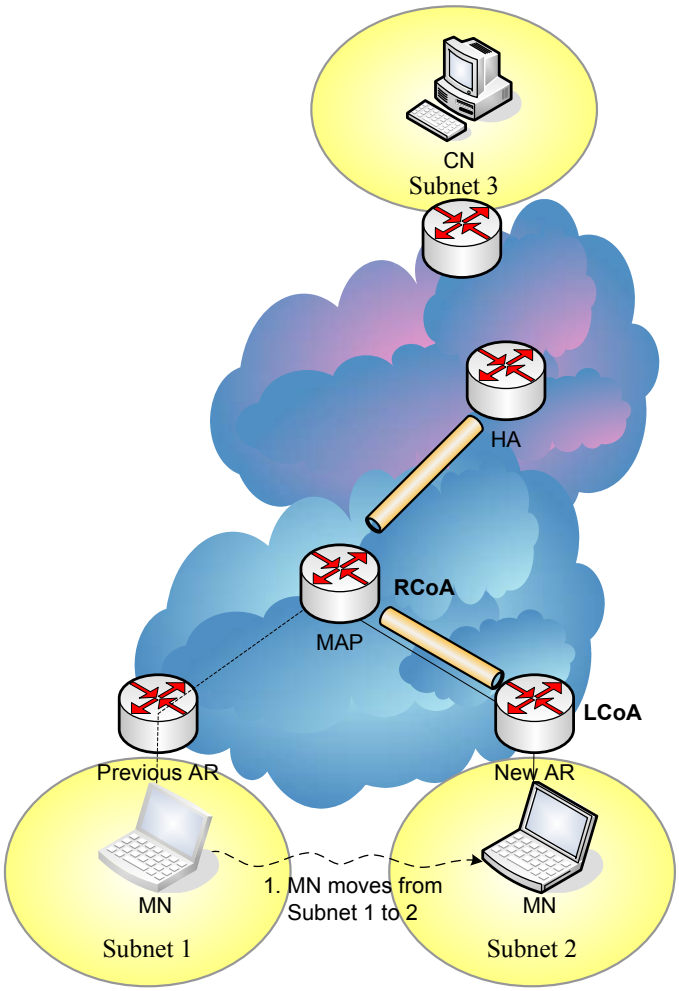

Figure 2: Hierarchical Mobile IPv6

2.4 Mobile IPv6 Fast Handover

MIPv6 describes the protocol operations for a MN to maintain connectivity to the Internet during its handover from one AR to another. These operations involve movement detection, IP address configuration and location update. The combined handover latency is often sufficient to affect real-time applications. Throughput-sensitive applications can also benefit from reducing this latency.

The Mobile IPv6 Fast Handover protocol (FMIPv6) [9] has been proposed as a way to minimize the interruption in service experienced by a Mobile IPv6 node as it changes its point of attachment to the Internet. Without such a mechanism, a MN cannot send or receive packets from the time that it disconnects from one point of attachment in one subnet to the time it registers a new care-of address from the new point of attachment in a new subnet. Such an interruption would be unacceptable for real-time services such as VoIP.

The basic idea behind a Mobile IPv6 fast handover is to leverage information from the link-layer technology to either predict or rapidly respond to a handover event. This allows IP connectivity

to be restored at the new point of attachment sooner than would otherwise be possible. By tunneling data between the old and new access routers, it is possible to provide IP connectivity in advance of actual Mobile IP registration with the HA or CN. This allows real-time services to be reestablished without waiting for such Mobile IP registration to complete. Because Mobile IP registration involves time-consuming Internet round-trips, the Mobile IPv6 fast handover can provide for a smaller interruption in real-time services than an ordinary Mobile IP handover.

2.4.1 FMIPV6 OPERATIONS

FMIPv6 enables an MN to quickly detect that it has moved to a new subnet by providing the new access point and the associated subnet prefix information when the MN is still connected to its current subnet. For instance, an MN may discover available access points using link-layer specific mechanisms (i.e., a "scan" in WLAN) and then request subnet information corresponding to one or more of those discovered access points. The MN may do this after performing router discovery or at any time while connected to its current router. The result of resolving an identifier associated with an access point is a [AP-ID, AR-Info]-tuple, which an MN can use in readily detecting movement: when attachment to an access point with AP-ID takes place, the MN knows the corresponding new router's coordinates including its prefix, IP address and L2 address.

The Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages are used for aiding movement detection. Through them, the MN also formulates a prospective New CoA (NCoA) when it is still present on the PAR's link. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to the new subnet link (NAR's link) when the MN has received a Fast Binding Acknowledgment (FBack) message prior to its movement.

To reduce the Binding Update latency, the protocol specifies a tunnel between the Previous CoA (PCoA) and the NCoA (see Figure 3). A MN sends a Fast Binding Update (FBU) message to its Previous Access Router (PAR) to establish this tunnel. When feasible, the MN sends an FBU from PAR's link. Otherwise, it should be sent immediately after attachment to NAR has been detected. As a result, PAR begins tunneling packets arriving for PCoA to NCoA. Such a tunnel remains active until the MN completes the Binding Update with its correspondents. In the opposite direction, the MN reverses tunnel packets to PAR until it completes the Binding Update. PAR forwards the inner packet in the tunnel to its destination (i.e., to the MN's correspondent). Such a reverse tunnel ensures that packets containing PCoA as a source IP address are not dropped due to ingress filtering.

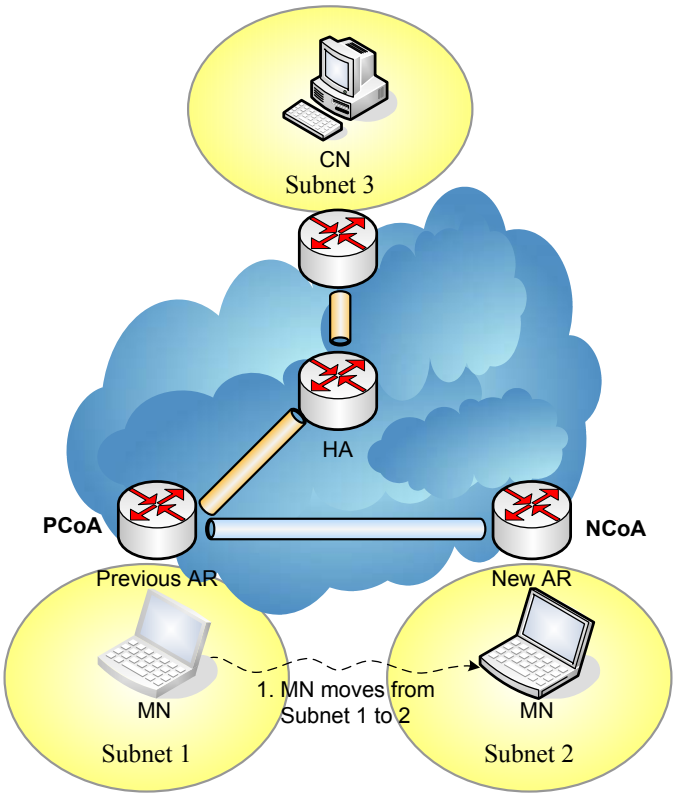

Figure 3: Fast Handover for Mobile IPv6

2.5 Proxy Mobile IPv6

As described in section 2.2, Mobile IPv6 requires client functionality in the IPv6 stack of a MN as the exchanging of signaling messages between the MN and HA enables the creation and maintenance of a binding between the MN's home address and its CoA. Thus, MIPv6 requires the IP host to send IP mobility management signaling messages to the HA, which is located in the network.

Network-based mobility is another approach to solving the IP mobility challenge. It is possible to support mobility for IPv6 nodes without host involvement by extending MIPv6 signaling messages between a network node and a HA. This approach to supporting mobility does not require the MN to be involved in the exchange of signaling messages between itself and the HA. A proxy mobility agent in the network performs the signaling with the HA and does the mobility management on behalf of the MN attached to the network. Because of the use and extension of Mobile IPv6 signaling and HA functionality, this protocol is referred to as Proxy Mobile IPv6 (PMIPv6) [10].

2.5.1 HOW PMIPV6 WORKS

IETF has recommended a Network-based approach to Localized Mobility Management called NetLMM based on Proxy Mobile IPv6. The key objective is to provide network-based IP mobility management support to MNs, without requiring their participation in any IP mobility related signaling. To reach this important goal, not considered in MIPv6, HMIPv6 and FMIPv6, the Proxy Mobile IPv6 makes use of two mobility entities in the network, which track the MN's movements and initiate the mobility signaling and setup the required routing state.

The core functional entities in the NETLMM infrastructure are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is responsible for maintaining the MN's reachability state and is the topological anchor point for the MN's home network prefix.
The MAG is the entity that performs the mobility management on behalf of a MN and it resides on the access link where the MN is anchored. The MAG is responsible for detecting the MN's movements to and from the access link and for initiating binding registrations to the MN's LMA.
The architecture of a Proxy Mobile IPv6 domain is shown in Figure 4.

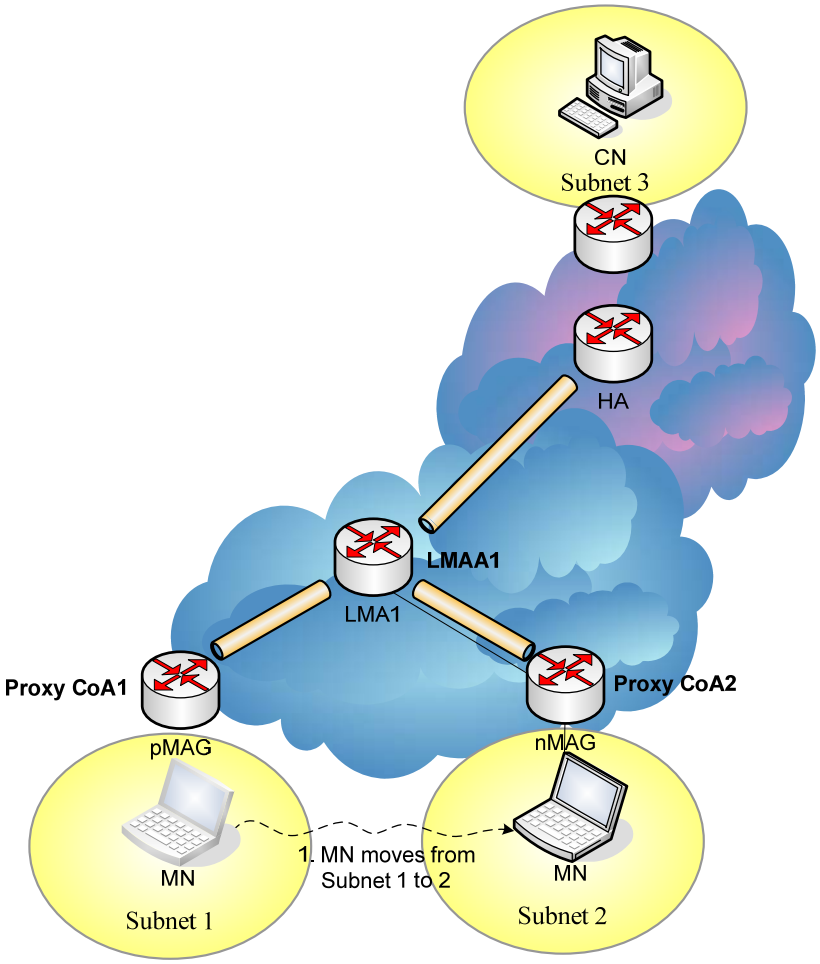

Figure 4: Proxy Mobile IPv6

As shown in Figure 5, once a MN enters a Proxy Mobile IPv6 domain and attaches to an access link, the MAG on that access link, after identifying the MN and acquiring its identity, determines if the MN is authorized for the network-based mobility management service. If the network determines that the network-based mobility management service needs to be offered to that mobile node, the network will ensure that the MN using any of the address configuration mechanisms permitted by the network will be able to obtain the address configuration on the connected interface and move anywhere in that Proxy Mobile IPv6 domain. The obtained address configuration includes the address(es) from its home network prefix, the default router address on the link and other related configuration parameters. From the perspective of the mobile node, the entire Proxy Mobile IPv6 domain appears as a single link, the network ensures that the mobile node believes it is always on the same link where it obtained its initial address configuration, even after changing its point of attachment in that network.

For updating the LMA about the current location of the MN, the MAG sends to it a Proxy Binding Update message. Upon accepting this Proxy Binding Update message, the LMA sends a Proxy Binding Acknowledgement message including the MN's home network prefix. It also creates the Binding Cache entry and sets up its endpoint of the bi-directional tunnel to the MAG.

The MAG on receiving the Proxy Binding Acknowledgement message sets up its endpoint of the bi-directional tunnel to the LMA and also sets up the data path for the MN's traffic. At this point the MAG has all the required information for emulating the MN's home link. It sends Router Advertisement messages to the MN on the access link advertising the MN's home network prefix as the hosted on-link-prefix.

The MN on receiving these Router Advertisement messages on the access link attempts to configure its interface either using stateful or stateless address configuration modes, based on the modes that are permitted on that access link. At the end of a successful address configuration procedure, the MN ends up with an address from its home network prefix.
Once the address configuration is complete, the MN has a valid address from its home network prefix at the current point of attachment. The serving MAG and the LMA also have proper routing states for handling the traffic sent to and from the MN using an address from its home network prefix.

The LMA, being the topological anchor point for the MN's home network prefix, receives any packets that are sent to the MN by any node in the network and it forwards them to the MAG through the bi-directional tunnel. The MAG on other end of the tunnel, after receiving the packet, removes the outer header and forwards the packet on the access link to the MN. The MAG typically acts as a default router on the access link. It intercepts any packet that the MN sends to any CN and sends them to its LMA through the bi-directional tunnel. The LMA on the other end of the tunnel, after receiving the packet, removes the outer header and routes the packet to the destination.

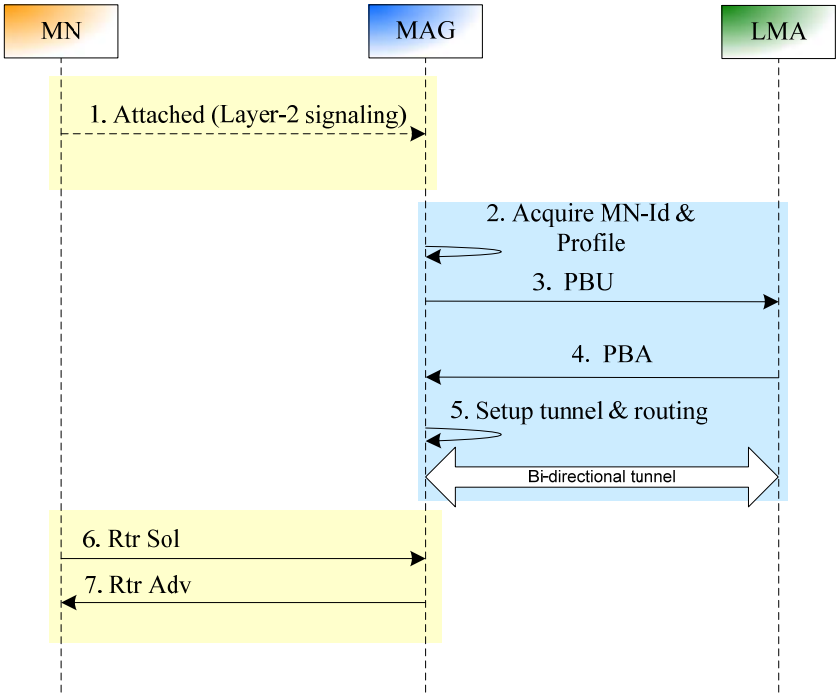

Figure 5: Proxy MIPv6 – MN attachment

Figure 6 shows the signaling call flow for the MN's handoff from previously attached MAG (pMAG) to the newly attached MAG (nMAG).
After obtaining the initial address configuration in the Proxy Mobile IPv6 domain, if the MN changes its point of attachment, the pMAG detects the MN's detachment from the link, signals the LMA and removes the binding and routing state for that MN. The LMA, upon receiving this request, identifies the corresponding mobility session for which the binding update request was received and, once it accepts, the request waits for certain amount of time for allowing the nMAG to update the binding.

The nMAG upon detecting the MN on its access link signals the LMA for updating the binding state. Once that signaling is complete, the MN continues to receive the Router Advertisements containing its home network prefix, making it believe it is still on the same link and it will use the same address configuration on the new access link.

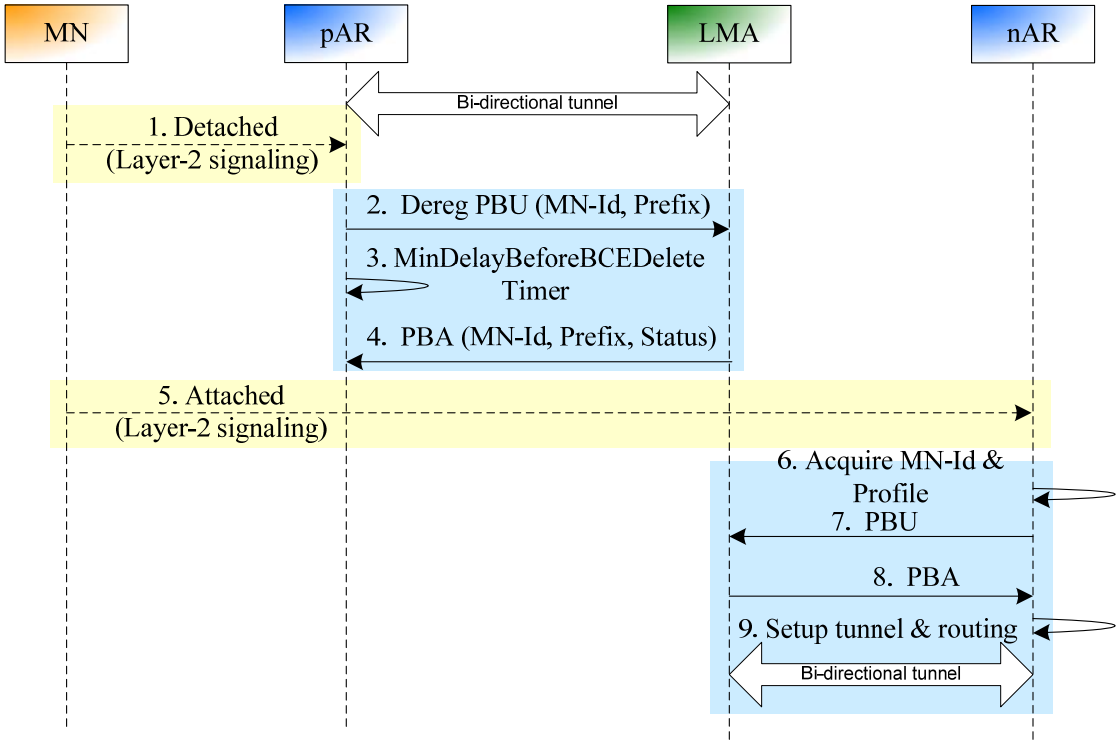

Figure 6: Proxy MIPv6 – MN handoff

3 MOBILE AD-HOC NETWORKING

Broadly, there are two major architectures for wireless networking: *single-hop* and *multi-hop*. The single-hop model is based on the cellular model, provides one-hop wireless connectivity between mobile hosts and static nodes known as *base station*. This type of networks relies on a fixed backbone infrastructure that interconnects all base stations by means of high-speed wired links.
Typically, a certain number of base stations are located on a geographical region in order to obtain coverage of such region, so whatever the position of the user is, there always exists a base station that connects that user to the network. The multi-hop model, on the other hand, requires neither a fixed and/or wired infrastructure nor a predefined interconnectivity. One of the most popular types of multi-hop network is called Mobile Ad hoc Network (MANET) [11].

MANET consists of a collection of wireless mobile nodes forming dynamic autonomous networks through a fully mobile infrastructure. This means that nodes communicate with each other without the intervention of centralized access points or base stations, and hence they are not relying on any fixed infrastructure. Nodes in this network model share the same random access wireless channel. They cooperate in a friendly manner to engage in multi-hop forwarding. Each node functions not only as a host but also as a router that maintains routes to and forwards data packets for other nodes in the network that may not be within direct wireless transmission range [12]. Routing in ad hoc networks faces extreme challenges from node mobility/dynamics, potentially very large numbers of nodes, and limited communication resources (e.g., bandwidth and energy). The routing protocols for ad hoc wireless networks have to adapt quickly to frequent and unpredictable topology changes and must be parsimonious of communications and processing resources.

One of the original motivations for MANET is found in the military need for battlefield survivability. Indeed, a fully mobile platform provides a fluid network where each entity moves about freely without any of restrictions imposed by a fixed platform. Also, the military cannot rely on access to a fixed, pre-placed communication infrastructure in battlefield environment. In some regions, such as the desert or in space, there is no terrestrial communication infrastructure. In other regions, access is unavailable or unreliable because of the destruction of the local infrastructure or eavesdropping of the information. Therefore, a rapidly and easily deployable mobile infrastructure seems very promising in such situations, but also in public safety applications as the usage scenario is very similar.

Many open issues need to be addressed in MANET and the most critical ones regard mobility management, in particular the problem of addressing techniques in wireless ad hoc networks and of ad hoc routing schemes for MANETs. Both aspects are described and summarized hereafter.

3.1 Ad hoc addressing for MANET

The major requirement of ad hoc addressing schemes is ensuring the uniqueness of node addresses so that no ambiguity appears when they try to communicate. This is not as trivial as it seems, especially because of the dynamic topology of ad hoc networks. A MANET cloud can be split into several parts and several MANET clouds can merge into one. Tens to thousands of nodes coexisting in a single network may participate concurrently in the configuration process. Moreover, the wireless nature, such as limited bandwidth, power, and high error rate makes the problem even more challenging. Besides handling a dynamic topology, the protocols must take into account scalability, robustness, and effectiveness. Finally, in IPv6, a protocol is expected to tackle not only the local addressing, but also the global addressing.

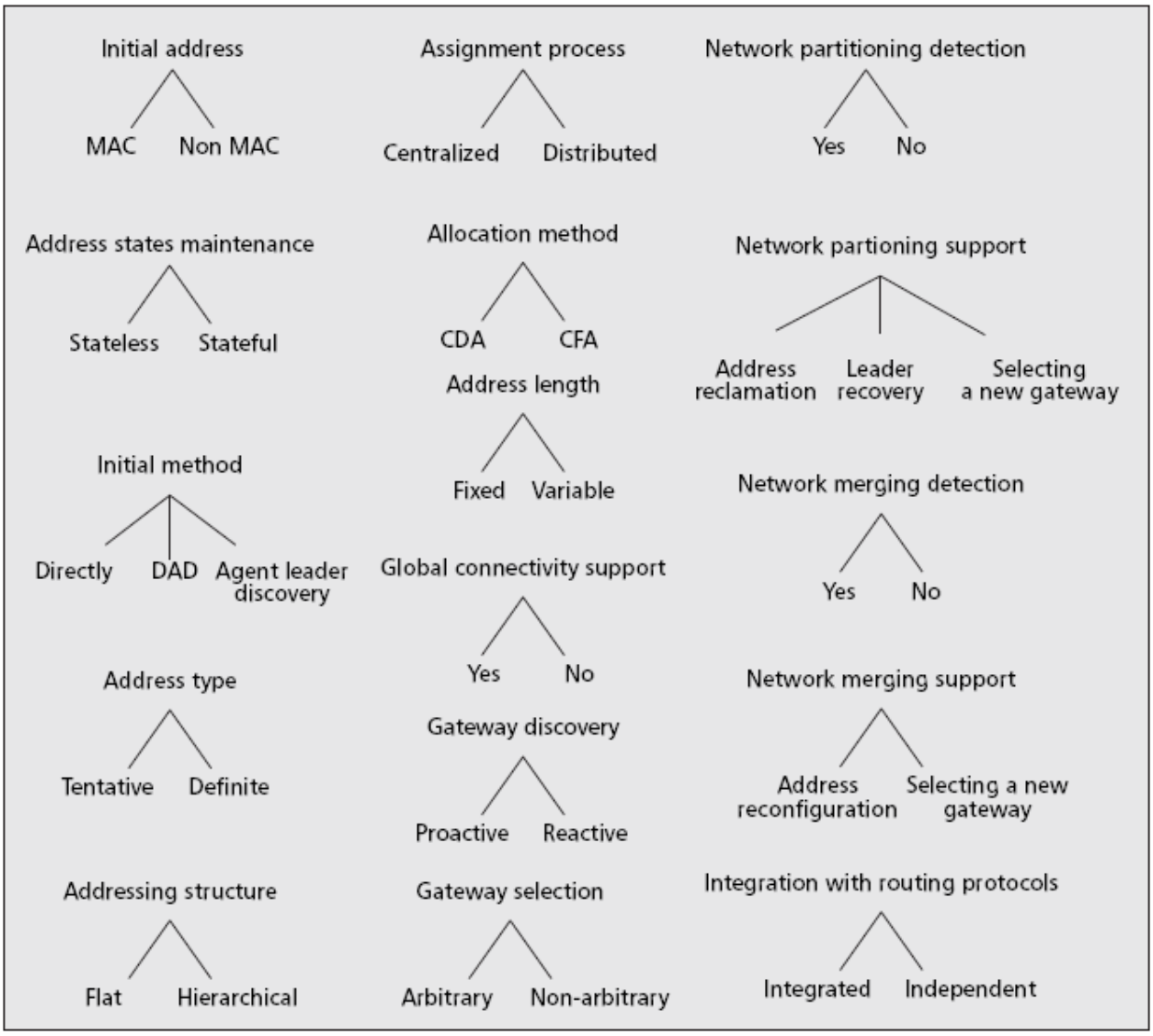

Figure 7: Addressing schemes and techniques for MANET

To ensure the properly working address autoconfiguration, several steps must be accomplished by that protocol. A complete analysis of the different ways of performing these steps is presented in the following and all of them are listed together with their subdivisions in Figure 7 [13].

- ***Initial Address*** - To obtain an address, a new node should have an initial address as its temporary identity. This can be classified either as a MAC or non-MAC address type. A non-MAC address is usually chosen randomly from a set of temporary addresses.

- ***Maintaining Address State*** - A configured address can be *stateless* or *stateful*, depending on who maintains the address. In ad hoc networks, even though dedicated servers are not always available or reachable, a stateful address still can be configured either in a centralized or distributed way. Furthermore, not always a full list of addresses is to be maintained; in fact, some protocols propose lightweight solutions by maintaining only the current highest value of the address or the address of logical neighbors.

- ***Initial Method*** - After configuring an address, nodes in IPv6-based protocols use the address *directly* to send a packet without necessarily verifying the uniqueness of the configured address. The probability of conflicts during the configuration process is extremely low, and the impact is minimal within a limited area. In addition, a passive detection is employed to resolve future possible conflicts. However, most protocols do not allow new nodes to directly claim a local address. Instead, by using an initial address, a newly joined node may attempt a local IP address by performing *DAD* or *agent discovery*. Stateless addressing requires the new node to select a tentative address and perform DAD by broadcasting a request to all the nodes. Stateful addressing usually requires a new node to find an agent or a leader that controls address configuration, either in a proactive or reactive way.

- ***Choosing a New Address*** - A node may obtain an address in the form of a *tentative* or *definite* address. A tentative address, usually randomly chosen by a new node, is an address whose uniqueness still must be verified using a DAD mechanism. A definite address requires no verification by other nodes in the assignment process. In schemes where the current address list is well maintained, the agent or leader easily can assign a non-occupied address to a new node.

- ***Addressing Structure*** - The protocols either have a *flat* or *hierarchical* addressing structure. Protocols that use flat addressing do not require any server assistance. Protocols that use a hierarchical structure often are called leader-based protocols, where one or more leaders appear in the network. The task of the leaders is defined differently in each protocol, such as *assigner* - assigning an address to a new node; *maintainer* - maintaining the state of addresses, *network identifiers* or a combination of these. Generally, the leader is elected either through distributed communication or the leader functionality is distributed. Whereas almost all of the hierarchical protocols for IPv4 allow only the presence of one leader in each network; according to some protocols for IPv6, multiple leaders can be present concurrently in a network. In such protocols, a network is divided into several subnets, and the leader of each subnet supplies a network prefix using similar mechanisms, such as RA messages in IPv6. In protocols designed for hybrid networks, leaders also behave as gateways, providing Internet connectivity for the other ad hoc

nodes. Further, the organization of IPv6 hierarchical addressing can be *non-structured* or *structured*. In non-structured networks, there are no boundaries between leaders and their descendants in sub networks. Nodes that use prefixes of leaders can be placed anywhere in the network. In structured networks, the subnetworks are clustered physically or logically. Physical clustering uses physical boundaries, such as hop counts. In logical clustering, nodes in the same cluster create a logical tree that places a gateway as the root and others as leaves.

- ***Assignment Process*** - The assignment process describes how a new node obtains an address. This can be executed in a *centralized* or *distributed* manner. Most hierarchical addressing approaches use centralized assignment, whereas flat addressing approaches use distributed assignment. However, the existence of a leader does not always imply centralized assignment.

- ***Allocation Method*** - The protocols accomplish address allocation using either *conflict detection allocation* (CDA) or *conflict-free allocation* (CFA). The CDA method is based on selecting an address from a pool of available addresses and then performing DAD. In IPv4, DAD is executed only on one level to verify the uniqueness of a link local address. However, the global address configuration in IPv6- based protocols requires DAD to be executed on two levels. The first local DAD is intended to detect conflicts with the local addresses. The second, network-wide or global DAD, is executed after a node obtains a prefix and configures the global address to test the validity of the configured address. In contrast to CDA, no duplicate detection is performed by the CFA method. The uniqueness of the allocated address can be assured without any cross check.

- ***Address Length*** - Most of the protocols use a *fixed* address length. Usually, it is 32 or 128 bits long to be compatible with the IP architecture. The major drawback of having such a long address is the excessive overhead caused by flooding or periodic signaling adopted by the addressing protocols.

- ***Global Connectivity and Gateway Discovery*** - Almost all protocols for IPv6 consider ad hoc networks as hybrid networks and thus, providing connectivity to the Internet is one of the important issues in their designs. A principle that is similar to IPv6 is adopted: the network prefixes of nodes acting as gateways are used to configure global addresses for other ad hoc nodes. There are two interesting aspects, namely, *gateway discovery* and *selection*, when multiple gateways are present. The schemes use a reactive or proactive approach to discover gateways. In the reactive approach, the newly arrived node broadcasts gateway solicitations (GSs) to acquire a network prefix on demand. In the proactive approach, gateway nodes periodically flood the network with gateway advertisements (GAs) containing prefix information. When multiple gateways are present, basically each interface of a node can be assigned with different prefixes. However, because most ad hoc routing protocols do not consider having multiple addresses for one interface, only one global address can be assigned to each interface. Obviously, selecting the “best” prefix among the available ones will improve the routing performance. Yet, all protocols for IPv6 do not deal with this in their designs.

- ***Network Partitioning: Detection and Support*** - Network partitioning occurs when a node leaves the original network. If a group of nodes leaves the network gracefully, then the nodes may notify others about their departure. Hence, the addresses can be reused in the original network by other nodes that join later. In many protocols, the node must send "bye" messages to release its address; either only to its neighbors or to all the nodes. However, when the node leaves abruptly, most protocols use the partition identifier (PID), which is periodically announced by the leader (in a hierarchical structure) or checked between neighboring nodes (in a flat structure) as a means to detect such events. The effect of network partitioning is a bit different in the cases of protocols for IPv4 and IPv6. In IPv4, a node that disappears from a network will take away its address so that it cannot be used by others. Therefore, the effect is considered significant only to protocols that have small address spaces or they are sensitive to address leakage. For hierarchical protocols, a different problem appears in the case of a departing leader. When the leader departs without informing other nodes, the task of a leader will be affected. In IPv6, partitioning may cause more serious problems to global addressing. Suddenly, if a MANET breaks into two separate parts, some nodes in each part might be required to change their network prefixes when current gateways are unreachable. Nevertheless, no protocol has so far solved this problem. Although most protocols for IPv6 do not specify methods to handle partitioning, a typical solution is that nodes should wait for a certain period of time to discover whether the connection to the current gateway is lost and then discover another gateway.

- ***Network Merging: Detection and Support*** - Conflicting addresses is a major problem when networks merge. That is, some nodes in each network may currently be using the same address. When the autoconfiguration protocol considers only link local addressing, address conflicts can occur in the protocols for both IPv4 and IPv6. Eventually, this also will be the case of global IPv6 addresses. If the same network prefixes are used in the different fragments, address collisions can occur whenever those fragments merge. However, many protocols assume that each gateway will use a topologically different and correct network prefix through manual configuration or dynamic set-up mechanisms. Thus, the uniqueness of the address can still be guaranteed in the case of network merging. Similar to partitioning, IPv4-based protocols generally use a PID to detect merging. However, most IPv6-based protocols do not have a mechanism for the detection of merging, even for local address configuration. Most likely, the reason is that a 64-bit interface identifier is considered to be long enough, and DAD performed previously is adequate to guarantee conflict-free addresses. When two networks merge, a simple solution adopted by most of the protocols for IPv4 is to have *all nodes of one partition* release their old addresses and reconfigure, while the addresses of the nodes from another partition remain unchanged. The choice of the partition that changes addresses is based on a particular criterion, for example, the partition with the least number of nodes, smaller PID, and so on.

- ***Integration with Routing Protocol*** — Although most MANET research focuses on developing efficient routing protocols, address configuration issues emerge as complementary research to support ad hoc routing. As a consequence, control traffic from routing and configuration protocols concurrently traverse everywhere in the network. To

reduce overhead caused by both protocols, several *integrated* approaches have been proposed. The main idea of the cross-layer designs is to reuse information from ongoing routing protocol traffic to support the addressing protocol or vice versa. Generally, addressing protocols are *independent* of the underlying routing protocols. The reason is that many routing protocols exist - each optimized for a special network setting; therefore, addressing schemes should adapt to any of those. Even though not restricted to a specific routing solution, some addressing schemes will achieve optimizations over particular routing protocols.

3.2 Ad hoc routing for MANET

Routing is defined as a mechanism by which user traffic is directed and transported through the network from the source node to the destination node. The primary goal of routing for mobile ad hoc network is correct and efficient route establishment between nodes. Route construction should be done with a minimum of overhead and bandwidth consumption. It is desirable that a routing protocol to be loop-free, distributed, adaptive and dynamic. The main routing functionalities are listed below:

- ***Path generation*** which generates paths according to the assembled and distributed state information of the network and the application. Note that, proactive protocols mainly use link-state or distance-vector algorithm for the path generation, while reactive protocols apply route discovery procedure.
- ***Path selection*** which selects appropriate paths based on network and application state information. Path selection procedure in proactive protocols is done based on shortest path algorithms, such as Dijkstra [14] algorithm for the link state routing and Distributed Bellman-Ford [15] for the distance-vector. Reactive protocols basically compute a *metric* such as number of hops during the route discovery procedure and select the path whose metric is the best.
- ***Data forwarding*** which forwards user traffic along the selected path.

Designing a new routing algorithm may necessitate examining the main strengths and weaknesses of each approach and comparing the different existing approaches. In the literature related to routing protocols used in mobile ad hoc networks, there exist two main design choices: (i) flat vs. hierarchical vs. geographical network architecture; (ii) proactive vs. reactive vs. hybrid strategy [16].

- ***Flat vs. hierarchical vs. geographical network architecture:*** one of the most critical design challenges in ad hoc routing concerns whether all nodes should have a uniform responsibility in the network or not. In a flat architecture, all nodes carry the same responsibility. *Flat architectures* do not optimize bandwidth resource utilization in large networks because control messages have to be transmitted globally throughout the network, but they are appropriate for highly dynamic network topology. The scalability

decreases significantly when the number of nodes increases. On the contrary, in *hierarchical architectures*, aggregating nodes into clusters and clusters into super-clusters conceals the details of the network topology. Some nodes, such as cluster heads and gateway nodes have a higher computation communication load than other nodes. Hence, the mobility management becomes complex. The network reliability may also be affected due to single points of failure associated with the defined critical nodes. However, control messages may only have to be propagated within a cluster. Thus, the multilevel hierarchy reduces the storage requirement and the communication overhead of large wireless networks by providing a mechanism for localizing each node. In addition, hierarchical architectures are more suitable for low mobility case. On the other hand, the *geographical approach* makes use of geographical information, i.e. obtained through Global Positioning System (GPS) or through reference points on some fixed coordinate system, to route traffic in MANET. The use of geolocation information can prevent network-wide searches for destinations, as either control packets or data packets can be sent in the general direction of the destination if the recent geographical coordinates for that destination are known. This reduces the control overhead generated in the network; however, all nodes must have continual access to their geographical coordinates for this approach to be useful.

- ***Proactive vs. reactive vs. hybrid strategy:*** another important design challenge for routing in ad hoc networks concerns whether nodes should keep track of routes to all possible destinations, or instead keep track of only those destinations that are of immediate interest. A node in an ad hoc network does not need a route to a destination until that destination has to be the recipient of packets sent by the node, either as the actual source of the packet or as an intermediate node long a path from the source to the destination. Protocols that keep track of routes for all destinations in the ad hoc networks have the advantage that communications with arbitrary destinations experience minimal initial delay from the point of view of the application. When the application starts, a route can be immediately selected from the routing table. Such protocols are called *proactive* because they store route information even before it is needed. They are also called table driven because routes are available as part of a well-maintained table. These protocols are based on either Link State (LS) or distance-vector algorithm. In this strategy, the trade-off is made between the cost of *full-update* against *no-search* strategies. To overcome the wasted work in maintaining unrequired routes, *on-demand* or *reactive* protocols have been designed. In these protocols, routing information is acquired only when it is actually needed. Reactive routing protocols save the overhead of maintaining unused routes at each node, but the latency for many applications will drastically increase. Most applications are likely to suffer a long delay when they start because a route to the destination will have to be acquired before the communication can begin. In this approach, *full-search* strategy is used at the expense of *no-update* strategy. Hybrid routing protocols aggregate a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. As a result, there is trade-off between the

search and update strategies. This trade-off is subject to the size of a zone and the dynamics of a zone.

As shown in Figure 8, it is possible to combine the above mentioned design choices and classify the most important routing protocol in MANET into them [17].

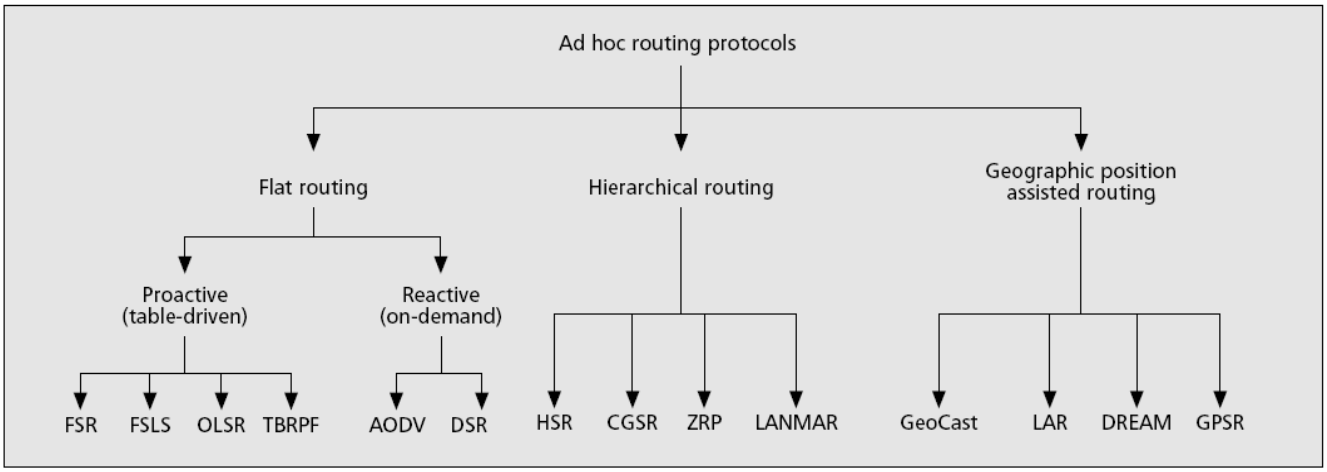

Figure 8: Classification of ad hoc routing protocols

3.2.1 ROUTING IN A FLAT NETWORK STRUCTURE

Ad hoc routing protocols in a flat network structure belong to two categories, proactive and on demand routing. The description of one of the most known routing protocol for each category is provided hereafter.

3.2.1.1 Proactive routing protocol

Proactive routing protocols share a common feature, that is, background routing information exchange regardless of communication requests. The protocols have many desirable properties, especially for applications including real-time communications and Quality of Service (QoS) guarantees, such as low-latency route access and alternate QoS path support and monitoring. Many proactive routing protocols have been proposed for efficiency and scalability.

Optimized Link State Routing Protocol

Optimized Link State Routing Protocol (OLSR) [18] is an LS protocol. It periodically exchanges topology information with other nodes in the network. The protocol uses *Multi Point Relays (MPRs)* to reduce the number of "superfluous" broadcast packet retransmissions and also the size of the LS update packets, leading to efficient flooding of control messages in the network.

A node, say node A, periodically broadcasts HELLO messages to all immediate neighbors to exchange neighborhood information (i.e., list of neighbors) and to compute the MPR set. From neighbor lists, node A figures out the nodes that are two hops away and computes the minimum set of one hop relay points required to reach the two-hop neighbors. Such set is the MPR set. Figure 9 illustrates the MPR set of node A. The optimum (minimum size) MPR computation is NP-complete. Efficient heuristics are used. Each node informs its neighbors about its MPR set in the HELLO message. Upon receiving such a HELLO, each node records the nodes (called MPR *selectors*) that select it as one of their MPRs.

In routing information dissemination, OLSR differs from pure LS protocols in two aspects. First, by construction, only the MPR nodes of A need to forward the link state updates issued by A. Second, the link state update of node A is reduced in size since it includes only the neighbors that select node A as one of their MPR nodes. In this way, partial topology information is propagated, that is, say, node A can be reached only from its MPR selectors. OLSR computes the shortest path to an arbitrary destination using the topology map consisting of all of its neighbors and of the MPRs of all other nodes. OLSR is particularly suited for dense networks. When the network is sparse, every neighbor of a node becomes a multipoint relay. The OLSR then reduces to a pure LS protocol.

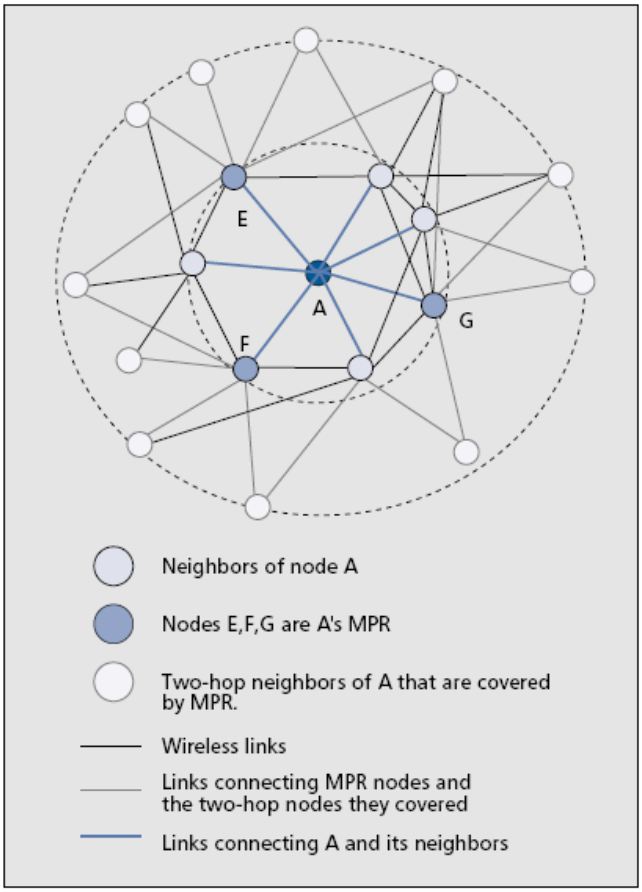

Figure 9: OLSR – Multi Point Relays

3.2.1.2 On-demand routing protocols

On-demand routing is a popular routing category for wireless ad hoc routing. The design follows the idea that each node tries to reduce routing overhead by only sending routing packets when a communication is awaiting. Among the many proposed protocols, Ad Hoc On Demand Distance Vector Routing (AODV) [19] and Dynamic Source Routing (DSR) [20] have been extensively evaluated in the MANET literature and are being considered by the Internet Engineering Task Force (IETF) MANET Working Group as the leading candidates for standardization. On-demand algorithms typically have a route discovery phase. Query packets are flooded into the network by the sources in search of a path. The phase completes when a route is found or all the possible outgoing paths from the source are searched. There are different approaches for discovering routes in on-demand algorithms.

Ad Hoc On Demand Distance Vector Routing

In AODV, on receiving a query, the transit nodes "learn" the path to the source (called *backward learning*) and enter the route in the forwarding table. The intended destination eventually receives the query and can thus respond using the path traced by the query. This permits establishment of a full duplex path. To reduce new path search overhead, the query packet is dropped during flooding if it encounters a node which already has a route to the destination. After the path has been established, it is maintained as long as the source uses it. A link failure will be reported to the source recursively through the intermediate nodes. This in turn will trigger another query-response procedure in order to find a new route.

Dynamic Source Routing

An alternate scheme for tracing on-demand paths is DSR. DSR uses *source routing*, that is, a source indicates in a data packet's header the sequence of intermediate nodes on the routing path. In DSR, the query packet copies in its header the IDs of the intermediate nodes it has traversed. The destination then retrieves the entire path from the query packet, and uses it (via source routing) to respond to the source, providing the source with the path at the same time. Data packets carry the source route in the packet headers. A DSR node aggressively caches the routes it has leaned so far to minimize the cost incurred by the route discovery. Source routing enables DSR nodes to keep multiple routes to a destination. When link breakage is detected (through *passive acknowledgments*), route reconstruction can be delayed if the source can use another valid route directly. If no such alternate routes exist, a new search for a route must be reinvoked. The path included in the packet header makes the detection of loops very easy.

To reduce the route search overhead, both protocols provide optimizations by taking advantage of existing route information at intermediate nodes. *Promiscuous listening* (overhearing neighbor propagation) used by DSR helps nodes to learn as many route updates as they can without actually participating in routing. *Expanding ring search* (controlled by the *time-to-live* field of route request packets) used by AODV limits the search area for a previous discovered destination using the prior hop distance.

3.2.2 HIERARCHICAL ROUTING

Typically, when wireless network size increase (beyond certain thresholds), current "flat" routing schemes become infeasible because of link and processing overhead. One way to solve this problem, and to produce scalable and efficient solutions is hierarchical routing. An example of hierarchical routing is the Internet hierarchy, which has been practiced in the wired network for a long time. Wireless hierarchical routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside a group. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole); thus, control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading node (*clusterhead*) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility. Since mobile nodes have only a single omni-directional radio for wireless communications, this type of hierarchical organization will be referred to as *logical hierarchy* to distinguish it from the physically hierarchical network structure.

3.2.2.1 Hierarchical State routing

Hierarchical State Routing (HSR) [21] is a multilevel clustering-based LS routing protocol. It maintains a logical hierarchical topology by using the clustering scheme recursively. Nodes at the same logical level are grouped into clusters. The elected clusterheads at the lower level become members of the next higher level. These new members in turn organize themselves in clusters, and so on. The goal of clustering is to reduce routing overhead (i.e., routing table storage, processing, and transmission) at each level. An example of a three-level hierarchical structure is demonstrated in Figure 10. Generally, there are three kinds of nodes in a cluster: clusterheads (e.g., nodes 1, 2, 3, and 4), gateways (e.g., nodes 6, 7, 8, and 11), and internal nodes (e.g., nodes 5, 9, and 10). A clusterhead acts as a local coordinator for transmissions within the cluster.

HSR is based on LS routing. At the first level of clustering (also the physical level), each node monitors the state of the link to each neighbor (i.e., link up/down and possibly QoS parameters, e.g., bandwidth) and broadcasts it within the cluster. The clusterhead summarizes link state information within its cluster and propagates it to the neighbor cluster heads (via the gateways). The knowledge of connectivity between neighbor clusterheads leads to the formation of level 2 clusters. For example, as shown in Figure 10, neighbor clusterheads 1 and 2 become members of the level 2 cluster C2. Link state entries at level 2 nodes contain the "virtual" links in C2. A "virtual" link between neighbor nodes 1 and 2 consists of the level 1 path from clusterhead 1 to clusterhead 2 through gateway 6. The virtual link can be viewed as a "tunnel" implemented through lower level nodes. Applying the aforementioned clustering procedure recursively, new cluster heads are elected at each level, and become members of the higher-level cluster. If QoS parameters are required, the clusterheads will summarize the information from the level they belong to and carry it into the higher level. After obtaining the link state information at one level, each virtual node floods it down to nodes of the lower-level clusters. As a result, each physical

node has “hierarchical” topology information through the hierarchical address of each node (described below), as opposed to a full topology view as in flat LS schemes.

The hierarchy so developed requires a new address for each node, the hierarchical address. The node IDs shown in Figure 10 (at level = 1) are physical (e.g., MAC layer) addresses. They are hardwired and unique to each node. In HSR, the *hierarchical ID* (HID) of a node is defined as the sequence of MAC addresses of the nodes on the path from the top hierarchy to the node itself. For example, in Figure 10 the hierarchical address of node 5, HID(5), is <1,1,5>. The advantage of this hierarchical address scheme is that each node can dynamically and locally update its own HID on receiving the routing updates from the nodes higher up in the hierarchy. The hierarchical address is sufficient to deliver a packet to its destination from anywhere in the network using HSR tables. Gateway nodes can communicate with multiple clusterheads and thus can be reached from the top hierarchy via multiple paths. Consequently, a gateway has multiple hierarchical addresses, similar to a router in the wired Internet, equipped with multiple subnet addresses. These benefits come at the cost of longer (hierarchical) addresses and frequent updates of the cluster hierarchy and the hierarchical addresses as nodes move. In principle, a continuously changing hierarchical address makes it difficult to locate and keep track of nodes.

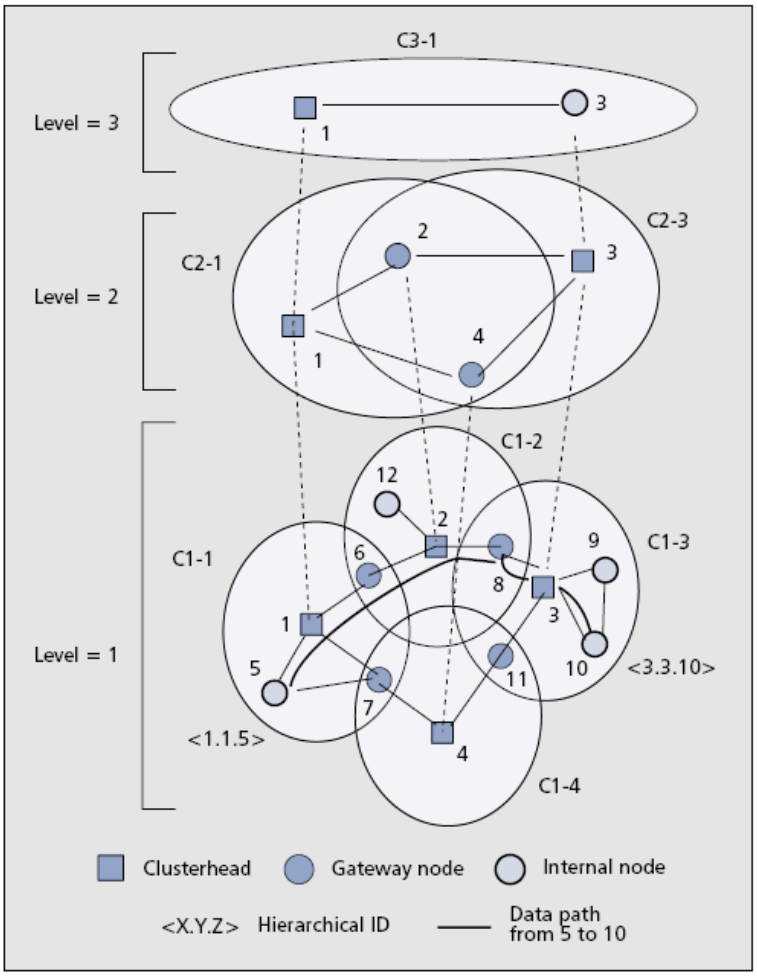

Figure 10: HSR – an example of multilevel clustering

3.2.3 GEOGRAPHIC ROUTING

The advances in the development of GPS nowadays make it possible to provide location information with a precision within a few meters. It also provides universal timing. While location information can be used for directional routing in distributed ad hoc systems, the universal clock can provide global synchronizing among GPS equipped nodes. Research has shown that geographical location information can improve routing performance in ad hoc networks. Additional care must be taken into account in a mobile environment, because locations may not be accurate by the time the information is used. All the protocols in this category assume that the nodes know their positions.

3.2.3.1 Location Aided routing

The Location-Aided Routing (LAR) protocol presented in [22] is an on-demand protocol based on source routing. The protocol utilizes location information to limit the area for discovering a new route to a smaller *request zone*. As a consequence, the number of route request messages is reduced. The operation of LAR is similar to DSR. Using location information, LAR performs the route discovery through *limited flooding* (i.e., floods the requests to a request zone). Only nodes in the request zone will forward route requests. LAR provides two schemes to determine the request zone.

Scheme 1: The source estimates a circular area (*expected zone*) in which the destination is expected to be found at the current time. The position and size of the circle is calculated based on the knowledge of the previous destination location, the time instant associated with the previous location record, and the average moving speed of the destination. The smallest rectangular region that includes the expected zone and the source is the request zone (Figure 11a). The coordinates of the four corners of the zone are attached to a route request by the source. During the route request flood, only nodes inside the request zone forward the request message.

Scheme 2: The source calculates the distance to the destination based on the destination location known to it. This distance, along with the destination location, is included in a route request message and sent to neighbors. When a node receives the request, it calculates its distance to the destination. A node will relay a request message only if its distance to the destination is less than or equal to the distance included in the request message. For example, in Figure 11b, nodes *I* and *J* will forward the requests from *S*. Before a node relays the request, it updates the distance field in the message with its own distance to the destination.

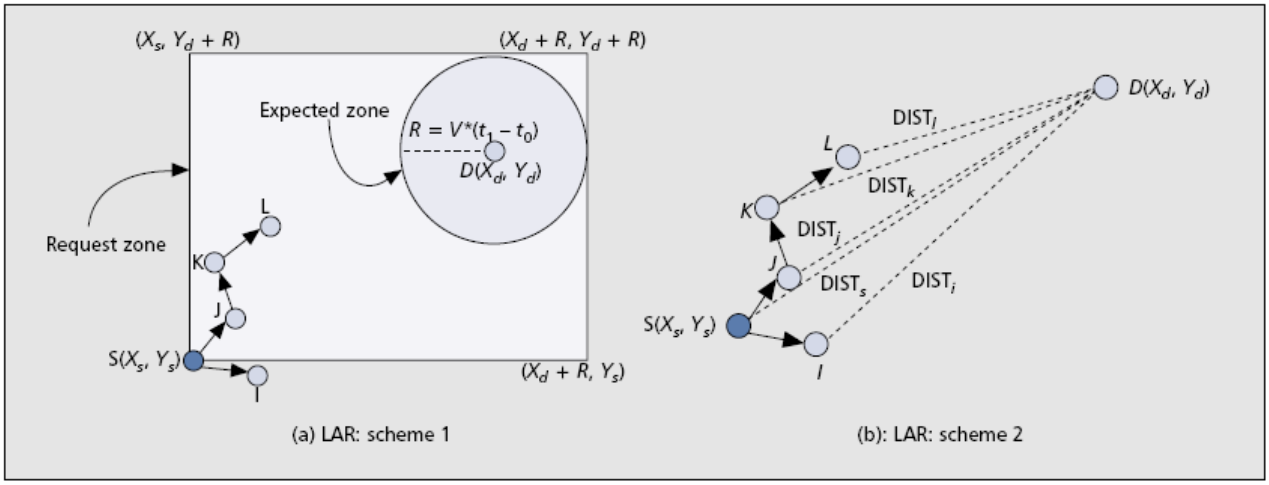

Figure 11: LAR: a) scheme 1: expected zone; b) scheme 2: closer distances

4 WIRELESS MESH NETWORKS

Wireless mesh networks (WMNs) are multi-hop wireless networks with self-healing and self-configuring capabilities [23]. WMNs are dynamically self-organized, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. These features, plus the ability to provide wireless broadband connectivity at a comparatively low cost, make WMNs a promising technology for a wide range of applications as public safety and crisis management communications.

4.1 Network architecture

WMNs consist of two types of nodes mesh routers and mesh clients [24]. Other than the routing capability for gateway/bridge functions as in a conventional wireless router, a mesh router contains additional routing functions to support mesh networking. Through multi-hop communications, the same coverage can be achieved by a mesh router with much lower transmission power. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. In spite of all these differences, mesh and conventional wireless routers are usually built based on a similar hardware platform.
Mesh clients also have necessary functions for mesh networking, and thus, can also work as a router. However, gateway or bridge functions do not exist in these nodes. In addition, mesh clients usually have only one wireless interface. As a consequence, the hardware platform and the software for mesh clients can be much simpler than those for mesh routers. Mesh clients have a higher variety of devices compared to mesh routers. They can be a laptop/desktop PC, pocket PC, PDA, IP phone.

The architecture of WMNs can be classified into three main groups based on the functionality of the nodes:

- **Infrastructure/Backbone WMNs**: The architecture is shown in Figure 12, where dash and solid lines indicate wireless and wired links, respectively. This type of WMNs includes mesh routers forming an infrastructure for clients that connect to them. The WMN infrastructure/ backbone can be built using various types of radio technologies, in addition to the mostly used IEEE 802.11 technologies. The mesh routers form a mesh of self-configuring, self-healing links among themselves. With gateway functionality, mesh routers can be connected to the Internet. This approach, also referred to as infrastructure meshing, provides backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers. Conventional clients with Ethernet interface can be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers. If different radio technologies are used, clients must communicate with the base stations that have Ethernet connections to mesh routers.

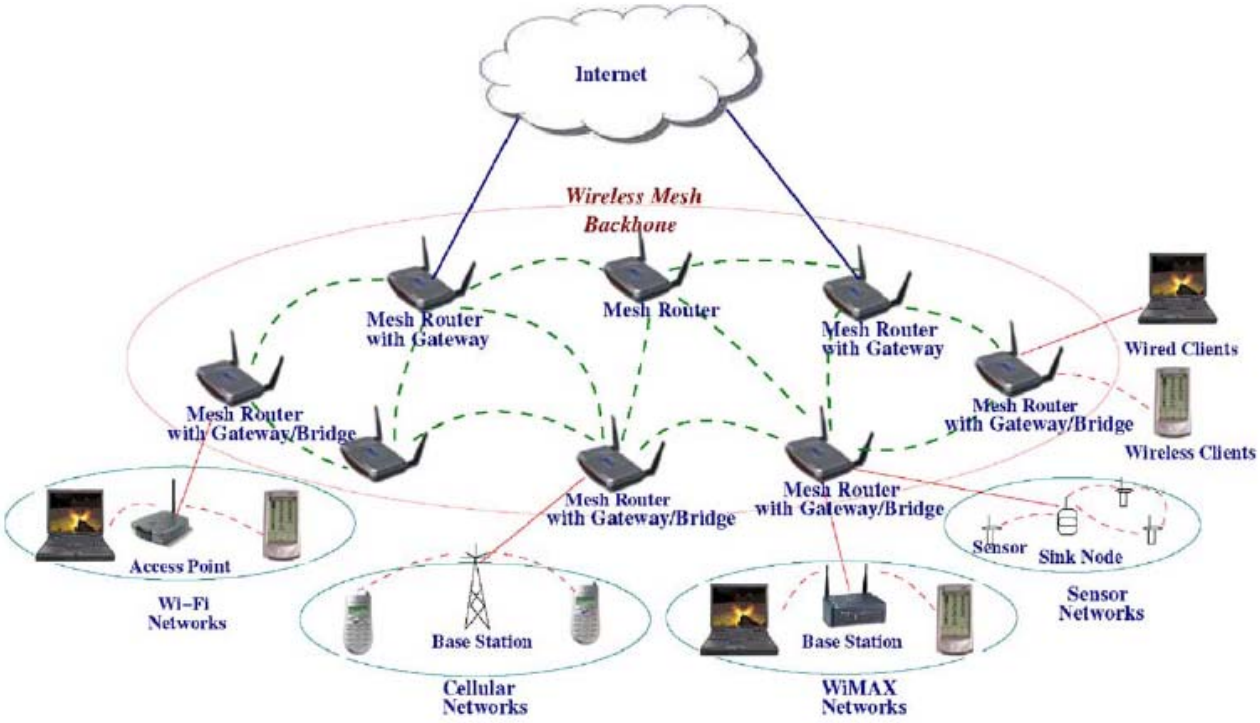

Figure 12: Infrastrucure/backbone WMNs

- **Client WMNs**: client meshing provides peer-to peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end user applications to customers. Hence, a mesh router is not required for these types of networks. The basic architecture is shown in Figure 13. In Client WMNs, a packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMNs are usually formed using one type of radios on devices. Moreover, the requirements on end-user devices is increased when compared to infrastructure meshing, since, in Client WMNs, the end-users must perform additional functions such as routing and self-configuration.

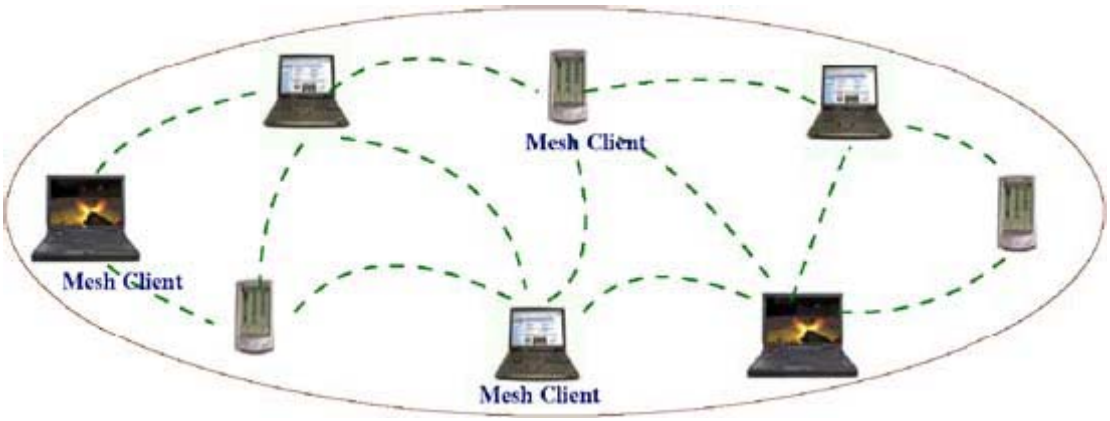

Figure 13: Client WMNs

- **Hybrid WMNs**: this architecture is the combination of infrastructure and client meshing as shown in Figure 14. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN.

Figure 14: Hybrid WMNs

4.2 Main characteristics

The most important characteristics of WMNs are explained as follows:

- *Multi-hop wireless network.* An objective to develop WMNs is to extend the coverage range of current wireless networks without sacrificing the channel capacity. Another objective is to provide Non-Line-Of-Sight (NLOS) connectivity among the users without direct Line-Of-Sight (LOS) links. To meet these requirements, the mesh-style multi-hopping is indispensable, which achieves higher throughput without sacrificing effective radio range via shorter link distances, less interference between the nodes, and more efficient frequency re-use.
- *Support for ad hoc networking and capability of self-forming, self-healing and self-organization.* WMNs enhance network performance, because of flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity, i.e. multipoint-to-multipoint communications. Due to these features, WMNs have low upfront investment requirement and the network can grow gradually as needed.
- *Mobility dependence on the type of mesh nodes.* Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes.
- *Multiple types of network access.* In WMNs, both backhaul access to the Internet and peer-to-peer (P2P) communications are supported. In addition, the integration of WMNs with other wireless networks and providing services to end-users of these networks can be accomplished through WMNs.
- *Dependence of power-consumption constraints on the type of mesh nodes.* Mesh routers usually do not have strict constraints on power consumption. However, mesh clients may require power efficient protocols. As an example, a mesh-capable sensor requires its communication protocols to be power efficient. Thus, the MAC or routing protocols optimized for mesh routers may not be appropriate for mesh clients such as sensors, because power efficiency is the primary concern for wireless sensor networks.
- *Compatibility and interoperability with existing wireless networks.* For example, WMNs built based on IEEE 802.11 technologies must be compatible with IEEE 802.11 standards in the sense of supporting both mesh capable and conventional Wi-Fi clients. Such WMNs also need to be interoperable with other wireless networks such as WiMAX, Zig-Bee, and cellular networks.

Based on their characteristics, WMNs are generally considered as a type of ad-hoc networks due to the lack of wired infrastructure that exists in cellular or Wi-Fi networks through deployment of base stations or access points. While ad hoc networking techniques are required by WMNs, the additional capabilities necessitate more sophisticated algorithms and design principles for the realization of WMNs. More specifically, instead of being a type of ad-hoc networking, WMNs aim to diversify the capabilities of ad hoc networks. Consequently, ad hoc networks can actually be considered as a subset of WMNs. To illustrate this point, the differences between WMNs and ad hoc networks are outlined below. In this comparison, the hybrid architecture is considered, since it comprises all the advantages of WMNs.

- *Wireless infrastructure/backbone.* As discussed before, WMNs consist of a wireless backbone with mesh routers. The wireless backbone provides large coverage, connectivity, and robustness in the wireless domain. However, the connectivity in ad hoc networks depends on the individual contributions of end-users which may not be reliable.
- *Integration.* WMNs support conventional clients that use the same radio technologies as a mesh router. This is accomplished through a host-routing function available in mesh routers. WMNs also enable integration of various existing networks such as Wi-Fi, the Internet, cellular and sensor networks through gateway/bridge functionalities in the mesh routers. Consequently, users in one network are provided with services in other networks, through the use of the wireless infrastructure. The integrated wireless networks through WMNs resemble the Internet backbone, since the physical location of network nodes becomes less important than the capacity and network topology.
- *Dedicated routing and configuration.* In ad hoc networks, end-user devices also perform routing and configuration functionalities for all other nodes. However, WMNs contain mesh routers for these functionalities. Hence, the load on end-user devices is significantly decreased, which provides lower energy consumption and high-end application capabilities to possibly mobile and energy constrained end-users. Moreover, the end-user requirements are limited which decreases the cost of devices that can be used in WMNs.
- *Multiple radios.* As discussed before, mesh routers can be equipped with multiple radios to perform routing and access functionalities. This enables separation of two main types of traffic in the wireless domain. While routing and configuration are performed between mesh routers, the access to the network by end users can be carried out on a different radio. This significantly improves the capacity of the network. On the other hand, in ad hoc networks, these functionalities are performed in the same channel, and as a result, the performance decreases.
- *Mobility.* Since ad hoc networks provide routing using the end-user devices, the network topology and connectivity depend on the movement of users. This imposes additional challenges on routing protocols as well as on network configuration and deployment.

4.3 Wireless Mesh Networks for Public Safety Communications

The availability of high-performance and low-cost commodity hardware based on IEEE 802.11 standards has been one of the key drivers behind the recent surge of interest in WMN technology, in terms of both research and product development. Several companies are offering mesh networking products for a range of application scenarios, including public safety and disaster recovery communications. Most of these products are based on IEEE 802.11 hardware, but the majority implements their own proprietary mesh protocols for routing and network configuration. Unfortunately, this makes integrating mesh routers from different vendors into a single WMN difficult, if not impossible. Efforts are under way in several IEEE working groups to define mesh networking standards.

IEEE 802.11s is the most relevant emerging standard for WMN technology in the context of public safety and disaster recovery communications (see section 4.3.4). Its aim is to extend the

MAC protocol of 802.11 networks to support mesh functionality. This is in contrast to most current WMNs, which implement mesh functionality at the network layer. The IEEE 802.11s standardization effort is in its early stages, so we cannot expect the approval of a standard or the availability of products before one year.

To assess the suitability of WMN technology for public safety and disaster recovery applications, it is necessary to consider this application domain's specific requirements [25].

4.3.1 FUNCTIONAL REQUIREMENTS

The functional requirements specify a set of features and capabilities that public safety communication systems should provide.

Interoperability

The interoperability of communication devices within and across different agencies and jurisdictions is a top priority. As already mentioned, most current WMN products are based on commodity IEEE 802.11 hardware. Even though the majority of these commercial systems implement proprietary mesh protocols for routing and network configuration, all these networks use IP at the network layer, which makes interoperability between WMNs and between WMNs and other networks easy. An IP-based network is therefore the ideal common platform for communication between multiple emergency response services and different jurisdictions.

Voice and data service support

Voice and data are the two main service categories required for public safety communications. Even though we could consider voice just another data service, it has a separate category due to its primary role in first-responder communication. Moreover, interactive data services should be supported, including instant messaging and video conferencing. Further requirements are Internet connectivity and support for Web-based services. The system should also be able to support real-time transmission of vital statistics of objects or persons, such as firefighters' heart rates or oxygen tank levels. Non-interactive data services including email and file transfer also need support. Given that they're essentially IP networks, WMNs can provide all applications and services available on the Internet, including voice and video. The wide range of services that WMNs support is one of the key advantages over traditional public safety communication systems.

Mobility support

Public safety users must have access to constant communication while traveling at reasonable speeds. The mobility requirement includes the ability to roam between different networks, potentially operated by different agencies and jurisdictions. IEEE 802.11 technology, on which most commercial WMN systems are built, hasn't been specifically designed to handle mobile clients traveling at high speeds. Experiments have shown that IEEE 802.11 can support mobile clients with speeds of up to 180 km per hour, but further research is necessary to explore the technology's limits in this regard. When mobile clients move from the coverage of one mesh router to another, the client's communication sessions must be handed over from one mesh router to the next - that is, the packets the client sends and receives must be redirected via the new mesh router. There's currently no standard way to transparently and seamlessly achieve this handover in a WMN. In a hybrid WMN, mobile clients also run the mesh routing protocol and therefore can independently discover new routes in case of a handover. For infrastructure WMNs, in which mobile clients are passive and simply associate with the nearest mesh router, client mobility and handover requires a different mechanism. Researchers have discussed possible solutions to this problem, including Mobile IP, Mobile Network Address Translation (NAT), and a simple solution based on the Dynamic Host Configuration Protocol (DHCP) protocol. However, because no single standard solution currently exists, the problem is an area of active research.

4.3.2 PERFORMANCE REQUIREMENTS

In addition to the aforementioned functional requirements, performance requirements for public safety communication systems are needed in the following key areas.

Robustness

Communication systems for crisis management and disaster recovery must be highly reliable and robust and should be able to function in potentially adverse and hostile environments. Recent disasters have highlighted the shortcomings of currently deployed technology in this regard.
Robustness is clearly one of the strengths of WMNs. One of their key features is the inherent redundancy of the mesh topology with multiple redundant paths between communication end points. The lack of a single point of failure guarantees connectivity even in the event of individual link or node failures. The ability to self-heal and dynamically adapt to a changing environment is another crucial characteristic of WMNs. Mesh routing protocols can establish valid paths between nodes even under challenging and dynamic conditions.

Scalability

Two types of scalability requirements are envisaged.
Horizontal scalability refers to the network's ability to grow efficiently and cost-effectively in terms of geographical coverage.

Vertical scalability stands for the ability to efficiently support an increasing number of users.
It is possible to increase a WMN's coverage area (horizontal scalability) by deploying additional mesh routers or, in the case of a hybrid WMN, with the addition of more clients. Consequently, the average number of hops in a communication path will increase. Unfortunately, research has shown that the throughput of multihop wireless networks degrades with the number of hops involved in an end-to-end path. One of the main problems here is *cochannel interference* - interference due to data transmitted simultaneously on the same channel by multiple nodes within each others' interference range. This is a more significant problem for WMNs than WLANs. The issue of vertical scalability is still an open research problem for WMNs. It's difficult to determine how many users a WMN can support because this depends on various parameters such as network topology and type of applications. The scalability problem is further aggravated because most WMNs operate in unlicensed industrial, scientific, and medical (ISM) frequency bands and therefore have to share the spectrum with other WLANs as well as a range of other wireless devices. Public safety and emergency response practitioners are typically skeptical of using any unlicensed frequency bands for their mission-critical communications. Spectrum allocation is obviously a key issue in this context, and it can vary greatly from country to country.

Quality of service

As a first priority, a public safety communication system must be able to provide reliable voice communication. Then, the system must transmit image and video data to allow rendering in acceptable quality. The system should be able to differentiate between traffic of different priority levels because high-priority traffic should get precedence to guarantee delivery of urgent messages in situations of network congestion.
Current WMNs based on commodity hardware fail to provide strict QoS guarantees. The 802.11 MAC mechanism is based on a randomized algorithm (Carrier Sense Multiple Access with Collision Avoidance [CSMA/CA]) that makes it difficult to give any guarantees regarding performance parameters such as delay, throughput, or jitter. IEEE 802.11e, a recent extension to the 802.11 standard, supports QoS and differentiation of traffic classes for single hop wireless networks. However, this QoS issue in multihop wireless mesh networks is still an open research problem.

4.3.3 OPEN RESEARCH ISSUES

Mobility management

Mobility management consists of two important tasks: location and handoff management.
Location management handles location registration and call delivery, while handoff management is responsible for handoff initiation, new connection generation, and data flow control for call handoff. The mobility management schemes developed for cellular or mobile IP networks could be useful for WMNs. However, the centralized scheme is generally not applicable on WMNs which are based on distributed and ad hoc architecture.

Thus, distributed mobility management is a preferred solution for WMNs. Mobility management schemes of ad hoc networks are mainly comprised of two types: distributed and hierarchical mobility management. These schemes may not perform well for WMNs due to the specific features of WMNs. More specifically, the backbone of WMNs does not have high mobility as mobile nodes in ad hoc networks, but connections between all mesh routers are wireless. Mesh clients may constantly roam across different mesh routers. These features also render the mobility management schemes for cellular networks ineffective for WMNs. As a result, new mobility management schemes need to be developed for WMNs.
Location service is a desired feature in WMNs. Location information can enhance the performance of MAC and routing protocols. It can help to develop promising location-related applications. Proposing efficient algorithms for location service is still an open research topic. Mobility management is closely related to multiple layers of network protocols. The development of multi-layer mobility management schemes is an interesting topic.

Routing protocols and metrics

Another active research area in this context considers routing protocols and metrics. Traditional mobile ad hoc network routing protocols, which form the basis of most WMN technology, use simple hop count as their routing metric. However, research has clearly shown the limitations of shortest-path routing in multi-hop wireless networks in general, and in WMNs in particular. The problem is that the hop-count metric prefers shorter paths consisting of low quality wireless links over longer, but higher quality paths, resulting in poor performance.
New routing metrics have recently been proposed that account for additional factors for route establishment, such as link quality, link capacity, and interference. Interference-aware routing metrics can minimize co-channel interference in multi-radio WMNs by establishing *channel diverse paths*, or paths in which transmission on neighboring nodes is done on non overlapping channels, resulting in significant performance improvements.

4.3.4 IEEE 802.11S

The study group for ESS mesh networking of the IEEE 802.11 working group became task group "s" (TGs) in July 2004. Its goal is the development of a flexible and extensible standard for wireless mesh networks based on IEEE 802.11. One of the key functionalities of IEEE 802.11s is the wireless multi-hop routing, which sets up the paths for the wireless forwarding [26].

The nodes of a wireless mesh network are called *Mesh Points (MPs)* in IEEE 802.11s. A mesh point is an IEEE 802.11 station that has mesh capabilities in addition to the basic station functionality. This means that it can participate in the mesh routing protocol and can forward data frames on behalf of other mesh points according to the IEEE 802.11s standard. In Figure 15, all nodes in the cloud are MPs and comprise the wireless mesh network. MPs can be end customer devices such as laptops as well as infrastructure devices such as access points.

Mesh points with additional access point functionality are called *Mesh Access Points (MAPs)*. Conventional WLAN clients, which are *nonmesh IEEE 802.11 Stations (STAs)*, can connect through the MAPs to the wireless mesh network.
MPs with additional portal functionality are called *Mesh Portal Points (MPPs)*. They can bridge data frames to other IEEE 802 networks, especially to a wired network such as an Ethernet.

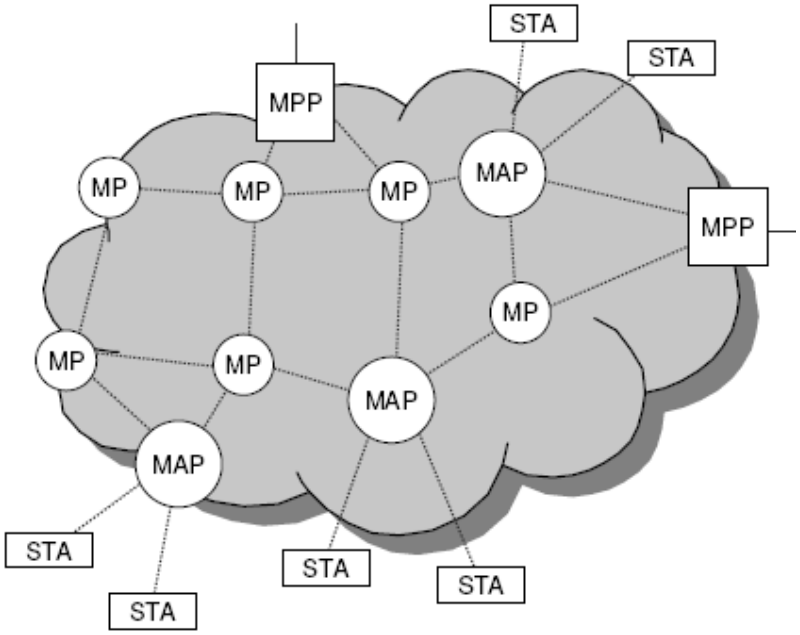

Figure 15: Example of IEEE 802.11s WLAN mesh network

Figure 16 illustrates the relation between the different (mesh) node types.

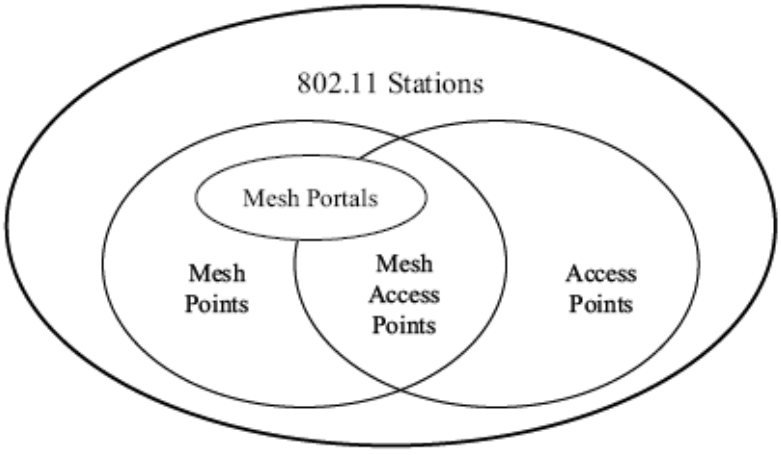

Figure 16: Relation between different IEEE 802.11 mesh nodes

The target size of an IEEE 802.11s WLAN mesh network is up to 32 mesh points according to [26]. However, this number should not be taken as a strict limit. It only says that a solution for large wireless mesh networks with several hundreds of mesh points is not required by IEEE

802.11s. In practice, IEEE 802.11s should be able to handle networks with up to ca. 50 mesh points.
The routing is on layer 2. The routing protocol uses MAC addresses and a radio-aware routing metric. It provides mesh unicast, multicast, and broadcast data delivery. In order to make the difference to routing on layer 3 with IP addresses more distinct, the preferred term for routing is *path selection* in IEEE 802.11s. The mesh routing architecture is extensible. This gives IEEE 802.11s mesh networks the flexibility to adapt to different usage scenarios by using routing protocols that are specialized and optimized for the anticipated scenario. IEEE 802.11s will support devices with a single radio as well as devices with multiple radios.

IEEE 802.11s will amend the MAC but changes to the PHY layer are not required. It is also compatible with higher layer protocols. Mesh security is based on IEEE 802.11i.

IEEE 802.11s WLAN mesh networks will be applicable to a large variety of usage scenarios. The four most important usage scenarios identified by the task group are:

- *residential* for wireless home networks;
- *office* for wireless networks in office environments;
- *campus/community/public access* for wireless backhaul meshes for internet access;
- *public safety* for flexible and fast setup of wireless communications for emergency staff.

The IEEE 802.11s draft can be split into four major parts - routing, MAC enhancements, security, and general IEEE 802.11 related topics. The key functionality is the wireless multi-hop routing and forwarding based on *Hybrid Wireless Mesh Protocol (HWMP)*.

4.3.4.1 Hybrid Wireless Mesh Protocol

HWMP is the default routing protocol for IEEE 802.11s WLAN mesh networking. Every IEEE 802.11s compliant device is required to implement this path selection protocol and to be capable of using it. This allows interoperability between devices of different vendors. As a hybrid routing protocol, HWMP contains both reactive routing components as well as proactive routing components.

The foundation of HWMP is an adaptation of the reactive routing protocol AODV called *Radio-Metric AODV (RM-AODV)* [28]. While AODV works on layer 3 with IP addresses and uses the hop count as routing metric, RM-AODV works on layer 2 with MAC addresses and uses a radio-aware routing metric for the path selection. The on-demand path setup is achieved by a path discovery mechanism that is very similar to the one of AODV. If a MP needs a path to a destination, it broadcasts a *Path Request Message (PREQ)* into the mesh network. MPs will rebroadcast the updated PREQ whenever the received PREQ corresponds to a newer or better path to the source. Similarly, the requested destination MP will respond with a *Path Reply Message (PREP)* whenever a received PREQ corresponds to a newer or better path to the source. Intermediate MPs that have already a valid path to the requested destination, can respond with a PREP, if the *Destination Only* flag is not set. Depending on the new *Reply and Forward* flag,

they can also rebroadcast the updated PREQ. This will result in a current path metric in addition to the fast path discovery.

The proactive component of HWMP is the extension with a proactive routing tree to specially designated MPs. Any MP that is configured to be a root MP, will periodically broadcast *proactive PREQ messages* or *Root Announcement Messages (RANNs)* into the wireless mesh network, which will create and maintain a tree of paths to the root MP. Depending on the configuration of this root portal, mesh points that receive a root portal announcement register with the root portal or not (*registration mode* or *non-registration mode*). The created and maintained tree allows proactive routing towards mesh portals. This proactive extension of HWMP uses the same distance vector methodology as RM-AODV and reuses routing control messages of RM-AODV.

CONCLUSIONS

For emergency mobile communications, mobility support to rescue teams acting in the disaster area is one of the most important requirements. IPv6, thanks to its advanced features for mobility, is the best protocol to be used in a crisis scenario. Several advanced mobility management proposal based on IPv6, like MIPv6, HMIPv6, FMIPv6 and PMIPv6, have been presented as possible candidates to be adopted in the disaster site. In particular, Proxy Mobile IPv6 seems to be the most promising one as it permits to beneficiate of a simple mobility management mechanism without requiring any modification in the user terminal. The requirements of user-centric approach, all-IP architecture and terminal independent mobility for Public Safety units, as mobile wireless nodes may not have a protocol stack for mobility, suggest leading future investigation on PMIPv6 protocol.

Mobile ad hoc network, consisting of mobile devices that communicate with each other with wireless communication technologies in an ad hoc fashion, has been presented as the starting point for the design of a dynamic and flexible mobile architecture in the terrestrial domain for Public Safety applications. Two aspects have been underlined as the most important and challenging points that need further investigation: addressing and routing techniques and protocols for mobile wireless ad hoc networks. Their combination together with IPv6 mobility mechanisms will improve mobility management aspects for rescue teams in a disaster scenario.

MANETs and especially WMNs are perfect candidates for the terrestrial infrastructure in the disaster area due to their self-healing and self-configuring capabilities and multi-hop nature. These features, plus the ability to provide wireless broadband connectivity at a comparatively low cost, make WMNs a promising technology for emergency applications. Moreover, the new emerging standard for WMNs technologies in the context of public safety and disaster recovery communications, the IEEE 802.11s, able to extend the MAC protocol of 802.11 networks to support mesh functionalities, brings additional interest on this technology.

REFERENCES

[1] S. Hagen, "IPv6 essentials", O'Reilly, May 2006.

[2] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, December 1998.

[3] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", IETF RFC 2462, December 1998.

[4] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", IETF RFC 3513, April 2003.

[5] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", IETF RFC 3315, July 2003.

[6] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, June 2003.

[7] Conta and S. Deering, "Generic Packet Tunneling in IPv6 Specification", IETF RFC 2473, December 1998.

[8] H. Soliman, C. Castelluccia, K. El Malki and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management", IETF RFC 4140, August 2005.

[9] R. Koodli, "Fast Handovers for Mobile IPv6", IETF RFC 4068, July 2005.

[10] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy Mobile IPv6", Internet Draft, draft-ietf-netlmm-proxymip6-11.txt (work in progress), February 2008.

[11] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC 2501, Jan. 1999.

[12] Charles E. Perkins, "Ad Hoc Networking", Addison-Wesley, 2001.

[13] N. I. Cempaka Wangi, R. Venkatesha Prasad, M. Jacobsson and I. Niemegeers, "Address Autoconfiguration in wireless ad hoc networks: protocols and techniques", IEEE Wireless Communications, Feb. 2008.

[14] E.W. Dijkstra, "A note on two problems in connection with graphs," in Proceedings of Numerische Math, 1959.

[15] D. Bertseks and R. Gallager, "Data Networks", Prentice-Hall, Inc., 1987.

[16] S. Basagni et al., "Mobile ad hoc networking", Wiley-IEEE, 2004.

[17] X. Hong, K. Xu, and M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE Network Mag., Jul. 2002.

[18] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, Oct. 2003.

[19] C. Perkins, E.Royer and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing", IETF RFC 3561, July 2003.

[20] D. Johnson, Y. Hu and D. Maltz, "Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", IETF RFC 4728, Feb. 2007.

[21] G. Pei et al., "A Wireless Hierarchical Routing Protocol with Group Mobility," Proc. IEEE WCNC '99, New Orleans, LA, Sept. 1999.

[22] Y.-B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," ACM/IEEE Int'l. Conf. Mobile Comp. Net., 1998, pp. 66–75.

[23] I.F. Akyildiz and Wang Xudong, "A Survey on Wireless Mesh Networks", IEEE Comm. Magazine, vol. 43, no. 9, 2005, pp. 23–30.

[24] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey", Computer Networks, vol. 47, no. 4, March 2005.

[25] M. Portmann and A.A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications", IEEE Internet Computing, vol. 12, no. 1, 2008, pp. 18–25.

[26] Osama Aboul-Magd et al., "Joint SEE-Mesh/Wi-Mesh proposal to 802.11 TGs", IEEE 802.11-06/0328r0, Feb. 2006.

[27] Avinash Joshi et al., "HWMP specification", IEEE 802.11-06/1778r1, Nov. 2006.

[28] Aoki, H. et al. 802.11 TGs Simple Efficient Extensible Mesh (SEE-Mesh) Proposal. IEEE P802.11 Wireless LANs, Document IEEE 802.11-05/0562r0, June 2005.

ACRONYMS

AODV	Ad Hoc On Demand Distance Vector Routing
BU	Binding Update
CoA	Care-of Address
CN	Correspondent Node
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DSR	Dynamic Source Routing
FBack	Fast Binding Acknowledgment
FMIPv6	Mobile IPv6 Fast Handover
GPS	Global Positioning System
HA	Home Agent
HMIPv6	Hierarchical Mobile IPv6
HoA	Home Address
HWMP	Hybrid Wireless Mesh Protocol
HID	Hierarchical ID
IETF	Internet Engineering Task Force
LAR	Location-Aided Routing
LCoA	On-link Care-of Address
LMA	Local Mobility Anchor
LOS	Line-Of-Sight
LS	Link State
MAG	Mobile Access Gateway
MANET	Mobile Ad hoc Network
MAP	Mesh Access Point
MIPv6	Mobile IPv6
MN	Mobile Node
MP	Mesh Point
MPP	Mesh Portal Point
MPR	Multi Point Relay
NAT	Network Address Translation
NCoA	New CoA
ND	Neighbor Discovery
NLOS	Non-Line-Of-Sight
NUD	Neighbor Unreachability Detection
OLSR	Optimized Link State Routing Protocol
P2P	Peer-to-Peer
PCoA	Previous CoA
PDU	Protocol Data Unit
PMIPv6	Proxy Mobile IPv6
PREP	Path Reply Message
PREQ	Path Request Message
PrRtAdv	Proxy Router Advertisement

QoS	Quality of Service
RANN	Root Announcement Message
RCoA	Regional Care-of Address
RM-AODV	Radio Metric-AODV
RtSolPr	Router Solicitation for Proxy Advertisement
STA	Stations
WMN	Wireless Mesh Network