Chapter 19

Multihop MAC: IEEE 802.11s Wireless Mesh Networks

Ricardo C. Carrano[1], Débora C. Muchaluat Saade[1], Miguel Elias M. Campista[2], Igor M. Moraes[2], Célio Vinicius N. de Albuquerque[3], Luiz Claudio S. Magalhães[1], Marcelo G. Rubinstein[4], Luís Henrique M. K. Costa[2] and Otto Carlos M. B. Duarte[2]

[1] {carrano,debora,schara}@midiacom.uff.br, TET/UFF, Brazil.
[2] {miguel,igor,luish,otto}@gta.ufrj.br, GTA/COPPE/POLI/UFRJ, Brazil.
[3] celio@ic.uff.br, IC/UFF, Brazil.
[4] rubi@uerj.br, PEL/DETEL/FEN/UERJ, Brazil.

Abstract

This chapter presents IEEE 802.11s, an emerging standard for wireless mesh networks (WMNs). IEEE 802.11s proposes multihop forwarding at the MAC level, which is a new approach for building WMNs. Traditional solutions for WMNs use network-level routing protocols to allow multihop forwarding among wireless mesh nodes. IEEE 802.11s specifies multihop MAC functions for mesh nodes using a mandatory path selection mechanism named HWMP (Hybrid Wireless Mesh Protocol) and also provides a path selection framework for alternative mechanisms and future extensions. This chapter discusses the emerging standard details and compares this new solution for WMNs to traditional ones.

Keywords: Wireless mesh networks, multihop, IEEE 802.11s, HWMP, path selection, routing protocols, and routing metrics.

19.1 Introduction

Wireless local area networks (WLANs) are well-known for being easy to deploy and support for user mobility. Although IEEE 802.11a, b and g standards are extremely popular and can be found in most laptops, PDAs and all sort of untethered equipment, wireless technology still faces some challenges and many research fields related to it are open to active development.

One of the main evolving fields is multihop ad hoc wireless networks that are based on, or extend, current wireless standards and technologies. This new trend is relevant since infrastructured wireless networks, though providing a number of advantages, can be highly empowered if nodes are able to forward traffic sourced by other nodes in an ad hoc self-configuring fashion. Multihop forwarding can, for instance, extend the coverage of wireless access points without the need of additional infrastructure.

Inexpensive IEEE 802.11 routers are also currently used in the deployment of low cost wireless backbones. Networks where the placement of each router forming a wireless backbone is chosen in order to create radio coverage for network access in a certain area, or to interconnect distant wired networks, are called Wireless Mesh Networks, or WMNs. Therefore, by this definition, WMNs would not be true ad hoc networks because they are planned (or engineered) but would nevertheless benefit from the wireless technology. Examples of WMN pilots can be found in [Campista *et al.* (2008); Bruno *et al.* (2005); Akyildiz and Wang (2005); Akyildiz *et al.* (2005); Aguayo *et al.* (2004); Couto *et al.* (2003)].

In contrast to a WMN, a Mobile Ad hoc Network (MANET) is a self-configuring network where there are no fixed routers. In a MANET, routers are free to move and network topology can change quickly and dramatically. Traffic routing functions are carried on by some or all of the participating nodes. Being ad hoc or engineered, or somewhere in between these two paradigms, wireless multihop networks share a common challenge: the development of routing protocols capable of coping with specific challenges posed by wireless networks, such as node mobility, fast-changing characteristics of the radio environment and medium access contention. After some decades of research in routing algorithms and routing metrics, there is a natural tendency that routing protocols shall be based, in varying degrees, on preexistent routing mechanisms.

The traditional approach to multihop forwarding has been the implementation of routing protocols at the network level, which brings the obvious advantage of being link-layer independent. After all, internetworking has been the realm and main goal of routing protocols.

A more recent proposal in WMN design addresses the implementation of multihop forwarding techniques at the link level, as an extension of WLAN functionalities [Camp and Knightly (2008); Faccin *et al.* (April 2006)]. This type of solution can widely spread the use of WMNs since it is going to be provided by end-user equipment. Additionally, quality-aware metrics can be easily implemented at the MAC level, allowing a better utilization of the wireless mesh network.

The IEEE Task Group 802.11s[IEEE (2007)] is currently developing an emerging standard for mesh networking at the MAC level. This new approach for building a WMN makes it appear as a LAN for layer-three protocols. IEEE 802.11s specifies multihop MAC functions for mesh nodes using a mandatory path selection mechanism, named HWMP (Hybrid Wireless Mesh Protocol), and provides a path selection framework for alternative mechanisms and future extensions.

The main goal of this chapter is to present the IEEE 802.11s emerging standard proposals, focusing on path selection mechanisms, and discuss and compare both - layer-two and layer-three - approaches for building WMNs. Section 19.2 describes the most relevant routing metrics and protocols used in current wireless mesh networks that employ the traditional layer-three approach. Section 19.3, on the other hand, is devoted to a detailed description of layer-two multihop techniques proposed by IEEE 802.11s. Final remarks are provided in Section 19.4.

19.2 Traditional Network-Level WMNs

In wireless mesh networks backbone routers communicate through multiple hops similar to that of ad hoc networks (Fig. 19.1). On the other hand, users carrying devices such as laptops or PDAs are often not responsible for routing, and connect to the backbone via mesh routers playing the role of access points. Thus, as previously mentioned, in mesh networks some nodes are dedicated to provide a backbone, unlike the ad hoc case. Wireless mesh networks have other two peculiarities. First, routers are typically stationary. As a consequence, the WMN routing metrics should measure wireless link quality instead of number of hops. Second, in WMNs, most of the network traffic flows towards the gateways, assuming that the common-case application is Internet access. This particular traffic matrix tends to present traffic concentration on the links close to the gateways. This characteristic can be explored to optimize WMN routing protocols. This section presents some of the most representative metrics and layer-three routing protocols proposed in the literature.

19.2.1 *Routing Metrics*

In ad hoc networks, the most used metric is hop count. In such networks, this metric is convenient because of the user mobility, which may incur in many link breakages. It is more important to quickly recover and have a route to the destination than to have a high-quality route. On the other hand, in WMNs, routers are usually stationary. Hence, routing metrics are more concerned with link-quality variations than specifically with link breakages. We refer to these as quality-aware metrics [Koksal and Balakrishnan (2006)].

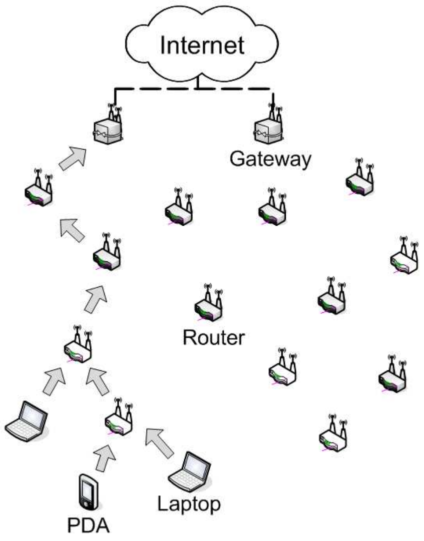


Fig. 19.1 A typical wireless mesh network.

WMN routing metrics are continuously evolving. One of the first metrics specifically proposed to be used in WMNs is called Expected Transmission Count (ETX) [Couto *et al.* (2003); Draves *et al.* (2004a)]. ETX represents the expected number of transmissions a node needs to successfully transmit a packet to a neighbor. To compute ETX, each node periodically broadcasts small probe packets containing the number of received probes from each neighbor. The number of received probes is calculated during the last T time interval using a sliding window. A node A computes the ETX of the link to a node B by using the delivery ratio of probes sent on the forward (df) and reverse (dr) directions. These delivery ratios correspond, respectively, to the fraction of successfully received probes from A as announced by B, and the fraction of successfully received probes from B, during the same interval, T. Thus, the ETX of link AB is given by:

$$ETX = \frac{1}{df \times dr}. \tag{19.1}$$

The ETX computation takes into account both forward and reverse directions to consider data- and ACK-frame transmissions. ETX is an additive metric, and the best route is the one with the lowest sum of ETXs along the route to the destination. It is worth noting that the number of broadcast probes in a network with n nodes is $O(n)$.

The Minimum Loss (ML) metric [Passos *et al.* (2006)] is also based on probing to compute the delivery ratio. Rather than calculating ETX, the ML metric finds the route with the lowest end-to-end loss probability, as follows:

$$ML = \prod_{i=1}^{l} df_i \times dr_i, \tag{19.2}$$

where l is the number of links in a path. Thus, ML is not cumulative, differently from ETX. Instead, it multiplies the delivery ratio of the links in the reverse and forward directions to find the best path. The authors of ML argue that the use of multiplication reduces the number of route changes, improving network performance. Iannone *et al.* [Iannone *et al.* (2007)] use another simple end-to-end metric, in which the idea is to avoid bottlenecks. Their metric is denoted here by I_p and is defined as follows:

$$I_p = \max_{1 \le i \le l} \left(\frac{1}{R_i} \right), \tag{19.3}$$

where R_i is the PHY rate of the link i in a path p composed of l links. The lower the I_p value, the better the route.

The implementation of ETX has revealed two shortcomings: broadcasts are usually performed at the network basic rate and probes are smaller than typical data packets. Thus, unless the network is operating at low rates, the performance of ETX is low because it neither distinguishes links with different bandwidths nor it considers data-packet sizes. To cope with these issues, the Expected Transmission Time metric (ETT) [Draves *et al.* (2004b); Aguayo *et al.* (2005)] was proposed. ETT represents the time a data packet needs to be successfully transmitted to each neighbor. Basically, ETT adjusts ETX to different PHY rates and data-packet sizes.

The ETT computation is a matter of implementation choice. Currently, there are two main approaches. For Draves *et al.* [Draves *et al.* (2004b)], ETT is the product between ETX and the average time a single data packet requires to be delivered, as seen in Equation 19.4.

$$ETT = ETX \times t. \tag{19.4}$$

To calculate the time t, the authors divide a fixed data-packet size (S) by the estimated bandwidth (B) of each link ($t = S/B$). The authors prefer to periodically estimate the bandwidth rather than use the transmission rate as informed by the firmware. This is because the IEEE 802.11 standard does not define an algorithm to select the transmission rate, it only defines physical transmission rates according to modulation schemes. Therefore, manufacturers are free to implement algorithms to automatically select the best transmission rate. This feature is called auto-rate, and usually does not give information about bandwidth, which is required to compute ETT. The packet-pair technique is then used to calculate the bandwidth (B) per link. This technique is well-known from wired networks, and consists of transmitting a sequence of two back-to-back packets to estimate bottleneck bandwidth. In the implementation of Draves *et al.*, two packets are unicast in sequence, a small one followed by a large one, to estimate the link bandwidth to each neighbor. Each neighbor measures the inter-arrival period between the two packets and reports it back to the sender. The computed bandwidth is the size of the large packet of the sequence divided by the minimum delay received for that link. In a n-node network where each node has v adjacencies, estimating the bandwidth is $O(n.v)$. Another approach to compute ETT is considered by Aguayo *et al.* [Aguayo *et al.* (2005); Couto (2004)]. The authors estimate the loss probability by considering that IEEE 802.11 uses data and ACK frames. The idea is to periodically compute the loss rate of data and ACK frames to each neighbor. The former is estimated by broadcasting a number of packets of the same size as data frames, one packet for each data rate as defined in IEEE 802.11. The latter is estimated by broadcasting small packets of the same size as ACK frames transmitted at the basic rate, which is the rate used for ACKs. Note that broadcasting packets at higher data rates may require firmware modifications. According to Aguayo *et al.*, ETT considers the best throughput achievable (r_t) and the delivery probability of ACK packets in the reverse direction (p_{ACK}). Thus, it is defined as:

$$ETT = \frac{1}{r_t \times p_{ACK}}. \tag{19.5}$$

Computing ETT in a n-node network is $O(n.m)$, where m is the number of possible data rates. Similarly to ETX, the chosen route is the one with the lowest sum of ETT values for each link to the destination. Cross-layer approaches are receiving special attention in WMNs [Akyildiz and Wang (2005)]. Among the available techniques, the use of multiple channels is commonplace. Through multiple channels it is possible to improve network throughput by using, at the same time, the available non-overlapping channels defined by IEEE 802.11. This technique, however, needs to deal with two issues to become effective, namely, intra-flow and inter-flow interference. The intra-flow interference occurs when different nodes transmitting packets from the same flow interfere with each other. Maximizing the number of channels is not trivial, considering that nodes must maintain connectivity. The inter-flow interference, on the other hand, is the interference between concurrent flows. The Weighted Cumulative ETT (WCETT) [Draves *et al.* (2004b)] changes ETT to also consider intra-flow interference. This metric is the sum of two components: end-to-end delay and channel diversity. Let p denote a path composed of l links, and c the maximum number of channels in the wireless system, the first component (Γ_1) of WCETT is given by:

$$\Gamma_1 = \sum_{i=1}^{l} ETT_i, \tag{19.6}$$

where ETT_i is the ETT of link i. This first component computes the end-to-end ETT. The second component (Γ_2), on the other hand, computes the ETT of links on the same channel along the path to estimate channel diversity. Then, the second component is given by:

$$\Gamma_2 = max_{1 \leq j \leq c}(X_j),\ where\ X_j = \sum_{link\ i\ is\ on\ channel\ j} ETT_i. \tag{19.7}$$

The higher the channel diversity, the more balanced is the sum of ETTs among the different channels along the path. Hence, computing Γ_2 gives an idea of the traffic balance among the different channels, or if there is a predominant channel being used. Furthermore, a tunable parameter (β) is used to combine both components or prioritize one of them. Equation 19.8 shows the WCETT metric.

$$WCETT = (1-\beta) \times \Gamma_1 + \beta \times \Gamma_2 = (1-\beta) \times \sum_{i=1}^{l} ETT_i + \beta \times \max_{1 \le j \le c} (X_j). \quad (19.8)$$

Unlike ETX and ETT, WCETT is an end-to-end metric. Thus, its outcome is the total cost of the route. This metric computes end-to-end values because it must consider all channels used along the path in order to avoid intra-flow interference.

The Normalized Bottleneck Link Capacity (NBLC) [Liu and Liao (2008)] metric also uses multiple radios and channels to improve network throughput. Differently from WCETT, NBLC considers the traffic load on each link and thus can perform load balancing among links. NBLC is an estimate of the residual bandwidth of a path. To compute NBLC, each node periodically measures the percentage of busy air time on each radio (tuned to a certain channel) and then obtains the percentage of residual air time. Each node periodically broadcasts this information to its k-hop neighbors using a dedicated control channel. For a specific channel used by a node, the actual residual channel capacity is approximated by the lowest residual channel capacity reported by interfering neighbors of the node or observed by the node itself. Based on this calculation, each node can determine the percentage of free-to-use channel air time on each outgoing link, called the Residual Link Capacity (RLC). Additionally, intra-flow interference is considered. For a link on a path, the actual air time consumed for the transmission of one packet along the path includes not only the air time spent in forwarding the packet on the link, but also the air time spent in keeping away from interference with the transmissions on links operating on the same channel on the same path. This amount of consumed air time, called Cumulative Expected Busy Time (CEBT), for a certain link on a path is obtained by aggregating the ETT values for the links of the path that operate on the same channel and interfere with this link. For a path p composed of l links, the NBLC metric is given by:

$$NBLC_p = \min_{link\ i\ \in\ p} \left(\frac{RLC_i}{CEBT_{i,p}} \right) \times \gamma^l, \quad (19.9)$$

where γ is the probability of a packet being dropped by an intermediate node. The chosen route is the one with the higher NBLC value.

Metrics such as WCETT do not guarantee shortest paths and do not avoid inter-flow interference [Yang *et al.* (2005)]. Link-state routing protocols need minimum-cost routes to be loop-free. Moreover, not avoiding inter-flow interference may lead WCETT to choose routes in congested areas. The Metric of Interference and Channel-switching (MIC) addresses these issues [Yang *et al.* (2005)]. MIC is also an end-to-end metric and its computation is based on two components: Interference-aware Resource Usage (IRU) and Channel Switching Cost (CSC). The first one is defined as:

$$IRU_i = ETT_i \times N_i, \tag{19.10}$$

where N_i is the set of neighbors affected by a transmission on link i, and ETT_i is the ETT of the same link. This first component takes into account the number of interfering nodes in the neighborhood to estimate inter-flow interference. The CSC computed by a node n of a path p is defined as:

$$CSC_n = \begin{cases} w_1, \, if \; c_{n-1} \neq c_n \\ w_2, \, if \; c_{n-1} = c_n, \end{cases} \tag{19.11}$$

where $0 \leq w_1 < w_2$, c_n is the channel used by node n, and c_{n-1} is the channel used by the previous node on the same path. CSC values are summed for all nodes of a path. As w_2 is always greater than w_1, when the same channel is repeated on consecutive links, the sum of CSC values gets higher and consequently the metric avoids intra-flow interference. In addition, MIC uses virtual nodes to guarantee minimum-cost route computation. The MIC metric is defined as:

$$MIC = \frac{1}{N_t \times min(ETT)} \times \sum_{i=1}^{l} IRU_i + \sum_{n=1}^{N_p} CSC_n, \tag{19.12}$$

where N_t is the total number of nodes in the network, $min(ETT)$ is the minimum known ETT, l is the number of links in path p, and N_p is the number of nodes in path p.

One critical problem of wireless networks is the fast link-quality variation. Metrics based on average values computed on a time-window interval, such as ETX, may not follow the link-quality variations or may produce prohibitive control overhead. Indoor environments make this problem even more difficult due to obstacles, interfering wireless devices, walking people etc. To cope with this, modified ETX (mETX) and Effective Number of Transmissions (ENT) were proposed [Koksal and Balakrishnan (2006)]. These metrics consider the variance in addition to link-quality average values. Thus, the main goal is to reflect physical-layer variations onto routing metrics.

The mETX metric is also calculated by broadcasting probes. The difference between mETX and ETX is that rather than considering probe losses, mETX works at the bit level. The mETX metric computes the bit error probability using the position of the corrupted bit in the probe and the inter-dependence of bit errors throughout successive transmissions. This is possible because probes are composed by a previously known sequence of bits. The metric mETX is defined in Equation 19.13, where μ_Σ and σ_Σ^2 denote the average and the variance of the packet error probability summed over the duration of one packet, respectively.

$$mETX = exp(\mu_\Sigma + \frac{\sigma_\Sigma^2}{2}). \tag{19.13}$$

ENT is an alternative approach that measures the number of successive retransmissions per link considering the variance. ENT also broadcasts probes and limits route computation to links that show an acceptable number of retransmissions according to upper-layer requirements. If a link shows a number of expected transmissions higher than the maximum tolerated by an upper-layer protocol (e.g. TCP), ENT excludes this link from routing computation assigning an infinity-value metric to it. ENT slightly modifies the mETX computation to consider the probability that the number of successive retransmissions per link exceeds a given threshold. ENT is defined as:

$$ENT = exp(\mu_\Sigma + 2\delta\sigma_\Sigma^2), \tag{19.14}$$

where δ denotes the strictness of the loss rate requirement. Both mETX and ENT are aware of the probe size, therefore the inclusion of the data rate is trivial with the two metrics.

The Distribution-Based Expected Transmission Count (DBETX) [Cunha *et al.* (2008)] metric also takes into account medium instability by considering fading of wireless channels. To compute DBETX, first each node must estimate the probability density function (pdf) of the SINR (Signal to Interference and Noise Ratio). Then, for a given modulation, it is possible to calculate the expected Bit Error Rate (BER) and the expected Packet Error Rate (PER). The success probability of a link (P_{Suc}) is $1 - PER$. Differently from other metrics, DBETX also takes into account the maximum number of MAC sublayer retransmissions (MaxRetry) to select a route. This cross-layer technique is similar to the one used by ENT. Nevertheless, DBETX considers lower-layer retransmissions instead of upper-layer requirements. DBETX is based on the Average Number of Transmissions (ANT) and on the MAC sublayer outage probability ($P_{out_{MAC}}$). ANT represents the expected number of retransmissions on a link considering the MaxRetry limit, as follows:

$$ANT = \begin{cases} \frac{1}{P_{Suc}}, \text{ if } P_{Suc} > P_{lim} \\ \frac{1}{P_{lim}}, \text{ otherwise,} \end{cases} \tag{19.15}$$

where

$$P_{lim} = \frac{1}{MaxRetry}. \tag{19.16}$$

The MAC sublayer outage is the condition that arrives when the current success probability of a link results in an expected number of retransmissions higher than MaxRetry. Thus, DBETX is given by:

$$DBETX = E[ANT] \times \frac{1}{1 - P_{out_{MAC}}}. \tag{19.17}$$

Another metric that also considers link-quality variation is iAWARE [Subramanian *et al.* (2006)]. This metric uses SNR (Signal to Noise Ratio) and SINR to continuously reproduce neighboring interference variations into routing metrics. The iAWARE metric estimates the average time the medium is busy because of transmissions from each interfering neighbor. The higher the interference, the higher the iAWARE value. Thus, unlike mETX, ENT, and DBETX, iAWARE considers intra- and inter-flow interference, medium instability, and data-transmission time. Let i denote a link between nodes u and v. To compute iAWARE, a node u measures the Interference Ratio ($IR_i(u)$) for a node u on link i. $IR_i(u)$ is defined as follows:

$$IR_i(u) = \frac{SINR_i(u)}{SNR_i(u)}. \tag{19.18}$$

In Equation 19.18, the Signal to Interference and Noise Ratio at node u on link i ($SINR_i(u)$) is given by:

$$SINR_i(u) = \frac{P_u(v)}{N_t + \sum_{n \in N_u - v} \tau(v) P_u(n)}, \tag{19.19}$$

where $P_u(v)$ is the signal strength of a packet from node v at node u, N_t is the total number of nodes in the network, N_u is the set of nodes that interfere on node u, and $\tau(v)$ is the normalized weight at which node n produces traffic averaged over a period of time. The Signal to Noise Ratio at node u on link i ($SNR_i(u)$) is defined as:

$$SNR_i(u) = \frac{P_u(v)}{N_t}. \tag{19.20}$$

Equation 19.21 shows the iAWARE metric of a link i, where IR_i is the minimum Interference Ratio ($min(IR_i(u), IR_i(v))$) to consider both data- and ACK-transmission directions on link i.

$$iAWARE_i = \frac{ETT_i}{IR_i}. \tag{19.21}$$

If there is no interference on link i, $SINR_i(u) = SNR_i(u)$ and then $IR_i = 1$. In this case, iAWARE depends only on the ETT_i of the link. Similarly to WCETT, the iAWARE metric also avoids intra-flow interference. To reach this goal, the iAWARE metric becomes a sum of two components tuned by a parameter β. In a wireless system composed of c different channels, iAWARE defines X_j as follows:

$$X_j = \sum_{conflicting\ link\ i\ is\ on\ channel\ j} iAWARE_i. \tag{19.22}$$

where $1 \leq j \leq c$, and the conflicting links are those which interfere on link i. The iAWARE metric of a path p is defined as in Equation 19.23.

$$iAWARE_p = (1 - \beta) \times \sum_{i=1}^{l} iAWARE_i + \beta \times \max_{1 \leq j \leq c} (X_j). \tag{19.23}$$

where l denotes the number of links on p.

Although there is an increasing number of routing metrics, no consensus has been reached. Up to now, most routing protocol implementations prefer metrics with simpler designs such as ETX or ETT. A summary of the main characteristics of WMN routing metrics can be found in [Campista *et al.* (2008)].

19.2.2 *Routing Protocols*

Ad hoc routing protocols usually use one of three strategies, namely reactive, proactive, or a combination of them. In the reactive strategy, as soon as a node has a data packet to send, it requests a route to the intended destination. If a node does not have data packets to send to a particular destination, the node will never request a route to it. The proactive strategy operates similar to that of classic routing on wired networks. Routers have at least one valid route always up-to-date to any destination in the network.

Many routing protocols of wireless mesh networks still use similar strategies to compute routes. Nevertheless, they are adapted to the peculiarities of WMNs and use one of the quality-aware routing metrics (Section 19.2.1). We use a taxonomy for the main WMN routing protocols according to [Campista *et al.* (2008)]. We divide them into four classes, namely, ad hoc-based, controlled-flooding, traffic-aware, and opportunistic. These protocol classes mainly differ on route discovery and maintenance procedures. In WMNs, most routing protocols assume that the network is composed by the set of wireless backbone nodes, and user nodes do not participate in the routing process. If a user device temporarily works as a backbone node, it must run the same routing protocol.

Ad hoc-based Protocols

WMN ad hoc-based protocols adapt ad hoc routing protocols to deal with link-quality variations. Routers keep track of the quality of other links to make route computation more accurate. Therefore, they continuously update their metrics and disseminate them to other routers. The Link Quality Source Routing (LQSR) protocol [Draves *et al.* (2004b)] is an ad hoc based. LQSR combines link-state proactive routing with the reactive strategy from ad hoc networks. It is fundamentally a link-state routing protocol and uses a complete view of the network topology to perform shortest-path computation. Nevertheless, LQSR uses route discovery procedures similar to those of reactive protocols to reduce routing overhead, which may become high because of medium instability and node mobility. During route discovery, LQSR obtains current link-state information of the traversed links, reducing the periodicity of link-state updates.

The SrcRR protocol [Couto (2004)] is another example of ad hoc-based protocol. It uses a discovery procedure similar to reactive protocols only to update the routing information of the traversed links. SrcRR further reduces control overhead, but computes routes from a reduced view of the network. Both LQSR and SrcRR implement route discovery procedures based on the Dynamic Source Routing (DSR) [David B. Johnson and Broch (2001)], using source routing, and use ETX. The Mesh Distance Vector (MeshDV) protocol [Iannone and Fdida (2005)] deals with user mobility and unlike LQSR and SrcRR, MeshDV considers not only backbone nodes but also user devices. Each node of the backbone maintains one table with the IP addresses of directly connected users and another table with the IP addresses of users connected to other backbone nodes. This scheme allows routers to be aware of users current location. MeshDV runs the Destination-Sequenced Distance Vector (DSDV) [Perkins and Bhagwat (1994)] routing protocol in the backbone and can use two metrics: hop count or I_p, as seen in Section 19.2.1.

One open research issue in wireless networks is the deployment of physical layer techniques to improve the overall efficiency of routing protocols. The Multi Radio LQSR (MR-LQSR) [Draves *et al.* (2004b)] is one example of such protocol. It adapts LQSR to operate over multiple channels and multiple interfaces and uses the metric WCETT. Although the use of WCETT does not guarantee minimum-cost paths, MR-LQSR is loop-free because it uses source routing. Another routing protocol that exploits physical-layer techniques to improve network performance is DOLSR (Directional Optimized Link-State Routing), which employs directional antennas [Das *et al.* (2006)]. The DOLSR protocol can use metrics such as number of hops, residual bandwidth, or ETX.

Controlled-flooding Protocols

Flooding the network with routing updates may produce scalability issues, especially if frequent changes on medium conditions are considered. Controlled-flooding protocols implement algorithms to reduce control overhead. One possible approach assumes that flooding the network is not efficient because the majority of traffic in wireless networks is between nodes close to each other. Therefore, there is no need to send control packets to nodes that are farther away as frequently as to nearby ones. Another way to reduce routing overhead is to limit the number of nodes responsible for flooding the network, avoiding redundancies. Protocols that adopt the second approach run algorithms to find the minimum set of nodes needed to forward routing information to all destinations in the network.

The Localized On-demand Link State (LOLS) [Wang *et al.* (2005); Nelakuditi *et al.* (2005)] attributes a long-term cost and a short-term cost to links. Long-term and short-term costs represent, respectively, the usual (historical) and the current cost of a link. In order to reduce the control overhead, short-term costs are frequently sent to neighbors, whereas long-term costs are sent at higher periods of time. LOLS computes routes using ETX or ETT.

Another typical example of a controlled-flooding protocol is the Mobile Mesh Routing Protocol (MMRP) developed by MITRE Corporation [MITRE Corporation (2006)]. MMRP assigns an age to its routing messages in the same way as OSPF protocol. Thus, whenever a node sends a routing message, it subtracts the age of the message from the estimated time needed to forward it. When age value reaches zero, the respective message is dropped, preventing its retransmission. MMRP does not specify a metric to be used with.

The Optimized Link State Routing (OLSR) [Clausen *et al.* (2001); Clausen and Jacquet (2003)] is yet another example of a controlled-flooding protocol. Original OLSR uses hop count as a metric, but OLSR was adapted to use ETX in WMNs. It uses the fraction of HELLO messages lost in a given interval of time to calculate ETX. OLSR could also be considered ad hoc-based; however, it uses MultiPoint

Relays (MPRs) to control flooding. OLSR limits the number of nodes in charge of disseminating control packets to avoid redundancies. Therefore, each node selects its MPR set, which is composed by nodes responsible for forwarding routing information from the selector node. Each node fills its MPR set with the minimum number of one-hop neighbors needed to reach every two-hop neighbors. There are also additional implementations of OLSR that use ML [Passos *et al.* (2006)] and ETT [Campista *et al.* (2008)] metrics.

Traffic-aware Protocols

Traffic-aware, or tree-based, routing protocols explore the traffic matrix typical of WMNs. They assume that backhaul access is the common-case application and, therefore, consider a network topology similar to a tree. One example is the Ad hoc On-demand Distance Vector-Spanning Tree (AODV-ST) [Ramachandran *et al.* (2005)]. This protocol is an adaptation of the AODV reactive protocol from ad hoc networks. In AODV-ST, the gateway periodically requests routes to every node in the network to initiate the creation of spanning trees in order to maintain its routing table updated. Thus, AODV-ST maintains a tree where the gateway is the root. Communications that do not include the gateway work as in the original AODV. AODV-ST supports ETX and ETT metrics.

Raniwala and Chiueh [Raniwala and Chiueh (2005)] propose a routing algorithm based on the spanning tree used in wired networks. Route maintenance is done with join and leave requests. They use the hop count and other metrics for load-balancing not specific to WMNs.

Opportunistic Protocols

Opportunistic protocols improve classical routing by exploring cooperative diversity schemes. Classical routing protocols compute a sequence of hops to the destination before sending a data packet, either using hop-by-hop or source routing. In case of link failure, successive link-layer retransmissions are performed until successful reception at the next-hop neighbor or until the maximum number of link-layer retransmissions is reached. This approach may incur in high delay and poor performance because wireless links require time to recover from transient failures. Cooperative diversity schemes, on the other hand, exploit the broadcast nature of radio-frequency transmissions to use multiple paths towards a destination. Each destination requires suitable transceivers to choose one of the relayed signals or to use a combination of them. Opportunistic protocols adapt cooperative diversity to standard IEEE 802.11 transceivers. Therefore, only one node forwards each packet. For example, opportunistic protocols choose, on-the-fly, which hop offers the best throughput. These protocols guarantee that data is always forwarded whenever there is at least one next hop. Besides, the chosen route likely uses the best quality links, considering short-term variations.

The ExOR protocol combines routing with MAC sublayer functionality [Biswas and Morris (2005)]. Routers send broadcast packets in batches, with no previous route computation. Packets are transmitted in batches to reduce protocol overhead, which may lead to underutilization of network resources. In addition, broadcasting data packets improves reliability because only one intermediate router is required to overhear a transmission. Nevertheless, it does not guarantee that the packets are received, because they are not acknowledged. Thus, an additional mechanism is needed to indicate the correct reception of data. Among the intermediate routers that have heard the transmission, only one retransmits at a time. The source router defines a forwarding list and adds it to the header of the data packets. This list contains the addresses of neighbors ordered by forwarding priority. Routers are classified in the forwarding list according to their proximity to the destination, computed with a metric similar to ETX. The metric used by ExOR only considers the loss rate in the forward direction because there are no acknowledgments. Upon reception of a data packet, the intermediate router checks the forwarding list. If its address is listed, it waits for the reception of the whole batch of packets. It is possible, however, that a router does not receive the entire batch. To avoid this problem, ExOR operates as follows. The highest-priority router that has received packets forwards them and indicates to the lower-priority routers the packets that were transmitted. The lower-priority routers therefore transmit the remaining packets, avoiding duplicates. The transmissions are performed until the destination indicates the reception.

The Resilient Opportunistic MEsh Routing protocol (ROMER) [Yuan *et al.* (2005)] focuses on resilience and high throughput by using multipath forwarding. ROMER combines long-term best routes, shortest-path or minimum-latency, and on-the-fly opportunistic gain to provide resilient routes and to deal with short-term variations on medium quality. ROMER computes long-term routes and opportunistically expands or shrinks them at runtime to fully exploit short-term higher-quality links. These long-term routes are computed using the minimum number of hops or the minimum average delay. Unlike ExOR, ROMER performs transmissions on a packet basis to enable faster reaction to medium variations. The highest-throughput route is chosen according to the maximum PHY rate as indicated by the MAC sublayer.

In order to improve the efficiency of WMNs, proposals of quality-aware metrics have become a recent trend. However, the pratical implementation of such metrics demands access to lower layer information thus cross-layer techniques have been proposed. Following this trend it is expected that WMNs could greatly benefit from multihop forwarding at the MAC layer.

19.3 Multihop MAC: IEEE 802.11s

In September 2003, IEEE started a study group to investigate adding wireless mesh networks as an amendment for its IEEE 802.11 standard. One year later, the study group became the Task Group "s" (TGs), which issued its first draft later in March 2006. By the time of this writing, IEEE 802.11s is still a draft (currently in version

1.08) [IEEE (2007)], therefore some degree of change should be expected before IEEE 802.11s becomes a standard. In fact, many improvements have been made in the current draft, considering previous versions of the document, and the reader should always keep in mind that this is still a work in progress. Nevertheless, commercial implementations of this draft are already available in some wireless devices [OLPC (2008); Open802.11s (2008)].

The recent emergence of handheld communication devices, constrained in many ways (power, processing, memory), demands a solution that may be easily embedded in network interface cards (NIC) and in systems-on-chip (SoC), and a MAC layer solution, being lightweight in contrast to a full implementation of ad hoc routing, fits that purpose.

In order to support multihop forwarding at the MAC layer, the current draft introduces changes in MAC frame formats, and an optional medium access method as well as many other optimizations to improve performance and security of wireless mesh networks. In this section, we focus on path selection mechanisms and new frame formats, since these aspects are the most closely related to multihop forwarding at the MAC level. Additional features are briefly discussed in subsection 19.3.5.

Originally, two path selection mechanisms were proposed in the draft. RA-OLSR (Radio-Aware Optimized Link State Routing) [Zhang *et al.* (2007)], which is a proactive controlled-flooding protocol based on OLSR [Clausen *et al.* (2001)] but adapted to work at layer-two instead of three, and a hybrid traffic-aware protocol, named HWMP (Hybrid Wireless Mesh Protocol) [Bahr (2006)], based on AODV [Perkins and Royer (1999)], which is actually the mandatory protocol and the only one remaining on the current proposal (version 1.08). RA-OLSR was removed in favor of an extensible path selection framework that enables alternative implementations of path selection protocols and metrics within the mesh framework.

Before going into the path selection mechanisms though, we must briefly discuss the mesh creation mechanisms and describe the architecture proposed by the emerging standard.

19.3.1 *Multihop-MAC Mesh Network Architecture*

According to the IEEE 802.11s draft, nodes in a mesh network fall into one of the four categories as illustrated in Fig. 19.2:

- Client or Station (STA) is a node that requests services but does not forward frames, nor participates in path discovery mechanisms;
- Mesh Point (MP) is a node that participates in the formation and operation of the mesh cloud;
- Mesh Access Point (MAP) is an MP who has an attached access point (AP) to provide services for clients (STA); and
- Mesh Portal Point (MPP) is an MP with the additional functionality of acting as a bridge or gateway between the mesh cloud and external net-

works.

Fig. 19.2 illustrates a possible ad hoc topology for this architecture. The doted lines represent the mesh network itself (mesh cloud) in which other non-802.11s nodes may participate indirectly (solid lines) connecting to mesh nodes extended with access point functionalities (MAPs).

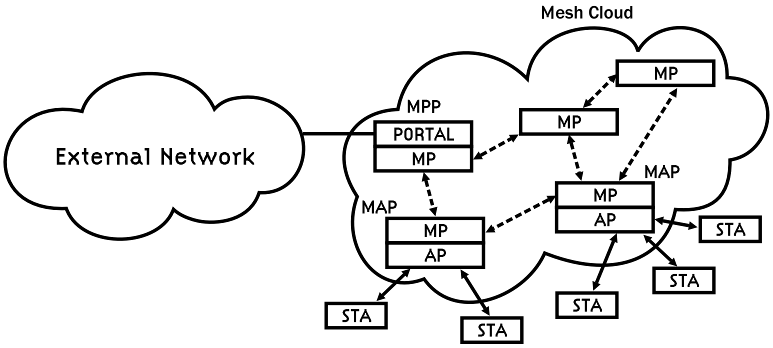


Fig. 19.2 IEEE 802.11s wireless mesh network.

In this topology example, there is only one MPP (PORTAL/MP), but nothing prevents a mesh network from having many. In that case each node must dynamically choose one of them for sending traffic outside the mesh network bounds.

Fig. 19.2 must be understood as a snapshot for a dynamic topology, where nodes may move in unpredictable and diverse ways, and links are formed or disrupted not only because of mobility, but also due to the changing conditions of the wireless medium. In that sense, the role of MPP is opportunistic and the network should provide the means (protocols and mechanisms) for announcing throughout the mesh cloud the set of nodes that are able to work as MPPs. These announcement mechanisms will be described in the following sections.

19.3.2 *Mesh Creation*

In infrastructured wireless networks, a Service Set Identifier (SSID) is used to distinguish the set of access points, which maintains a certain functional correlation and belong to the same local area network.

In a mesh network the same need for an identity exists, but instead of overloading the definition and function of the SSID, the draft proposes a Mesh identifier or Mesh ID. Similarly to 802.11, beacon frames are used to announce a Mesh ID, which should never be confused with the standard SSID employed by regular infrastructured wireless network. To avoid misleading a non-mesh station when trying to associate to a mesh network, Mesh Points (MPs) broadcast beacons with the SSID set to a wildcard value.

The Mesh ID is one of the three elements that characterize a mesh network. The other two are a path selection protocol and a path selection metric. Together these three elements define a profile. A Mesh Point may support different profiles, but all nodes in a mesh cloud, at a given moment, must share the same profile.

The 802.11s mandatory profile defines HWMP as the path discovery mechanism and the Airtime Link metric as the path selection metric, as it will be described in the following sections. The draft does not prevent other protocols or metrics from being used in a mesh cloud and even defines frameworks for those alternative mechanisms, but it advises that a mesh network shall not use more than one profile at the same time. This recommendation may be interpreted as an attempt to avoid complexity of profile renegotiation that may be too expensive for a simple device to handle. If a mesh cloud is formed with non-mandatory elements (protocol and metric), it is not obliged to fall back in order to accommodate a new mesh member that only supports the mandatory profile.

A mesh network is formed as MPs find neighbors that share the same profile. The neighbor discovery mechanism is similar to what is currently proposed by the 802.11 standard - active or passive scanning. In order to achieve this, regular (802.11) beacon frames and probe response frames are extended to include mesh related fields. As it will be discussed in the following sections, the draft does not only introduce new frames but also extends pre-existent ones.

To conclude our analysis on the mesh creation procedures we should comment on the establishment of the peer links - edges of a mesh graph. A Mesh Point shall create and maintain peer links to its neighbors that share its active profile (an MP may keep many profiles, but only one is active at a given moment). Once a neighbor candidate is found, through active or passive scanning, an MP uses the Mesh Peer Link Management protocol [IEEE (2007)] to open a mesh peer link.

A mesh peer link is univocally identified by the MAC addresses of both participants and a pair of link identifiers, generated by each of the MPs in order to minimize reuse in short time intervals.

To establish a peer link, both MPs exchange `Peer Link Open` and `Peer Link Confirm` frames as depicted in Fig. 19.3. Whenever an MP wants to close a peer link it should send a `Peer Link Close` frame to the peer MP.

19.3.3 *Path Selection Mechanisms*

IEEE 802.11s proposes a mandatory path selection protocol: a hybrid (proactive/reactive) traffic-aware protocol named HWMP - Hybrid Wireless Mesh Protocol. Although the standard assures compatibility between devices of different vendors by dictating mandatory mechanisms (HWMP and the Airtime Link Metric), it also includes an extensible framework that may be used to support specific application needs.

In order to exchange these configuration parameters, a `Mesh Configuration`

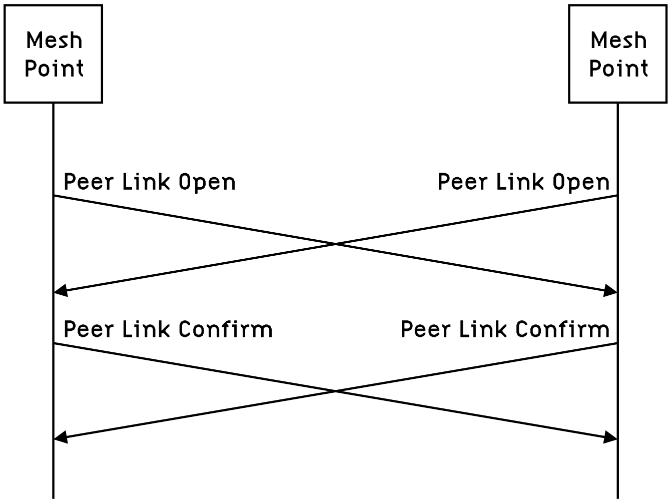


Fig. 19.3 IEEE 802.11s mesh peer-link creation.

element is transported by beacon frames, `Peer Link Open` frames and `Peer Link Confirm` frames. The `Mesh Configuration` element contains, among other subfields, an Active Path Selection Protocol Identifier and an Active Path Selection Metric Identifier.

19.3.3.1 *HWMP and Airtime Link Metric*

As a hybrid protocol, HWMP aims at merging advantages of both proactive and reactive approaches. It is inspired on the Ad Hoc On Demand Distance Vector (AODV) protocol [Perkins and Royer (1999)] and on its extension AODV-ST [Ramachandran *et al.* (2005)].

HWMP can be configured to operate in two modes: on-demand reactive mode and tree-based proactive mode. On-demand mode is appropriate to establish a path between MPs in a peer-to-peer basis, while in proactive mode, a tree-based topology is calculated once an MP announces itself as a root MP. The tree-based approach can improve path selection efficiency when there is a tendency of forwarding significant portions of network traffic to some specific nodes, for instance to a Mesh Portal Point (MPP).

What makes the protocol truly hybrid is the fact that both modes may be used concurrently. The main advantage of this approach is that, in certain circumstances, although readily available, the tree-based path may not be optimal and an on-demand path discovery may be employed to determine a more appropriate path. One example of such a circumstance is the case where two non-root nodes are able to exchange data through a low cost path (even directly by a single mesh link), but instead they are forced to send their frames to a distant root node up and down the tree.

In 802.11s the mandatory metric is the Airtime Link metric. This metric accounts for the amount of time consumed to transmit a test frame and its value takes into account the bit rate at which the frame can be transmitted, the overhead posed by the PHY implementation in use and also the probability of retransmission, which relates to the error rate in a link. The draft does not specify how to calculate the frame loss probability, leaving this choice to the implementation. Nodes transmitting at low data rates may use all the bandwidth in a network with their long transmissions the same way a high error rate link can occupy the medium for a long time. The Airtime Link metric is designed to avoid both. According to the standard, the Airtime Link metric is calculated as:

$$c_a = \left[O + \frac{B_t}{r} \right] \frac{1}{1 - e_f}, \tag{19.24}$$

where O is a constant overhead latency that varies according to the PHY layer implementation, B_t is the test frame size (1024 bytes), r is the data rate in Mb/s at which the MP would transmit a test frame and e_f is the measured test frame error rate.

During path discovery, each node in the path contributes to the metric calculation by using management frames for exchanging routing information. Independently of the operating mode (proactive or reactive), HWMP functions are carried on by management frames with the following set of information elements:

- `Path Request` (PREQ) elements are broadcast by a source Mesh Point that wants to discover a path to a destination Mesh Point;
- `Path Reply` (PREP) elements are sent from the destination Mesh Point back to the source Mesh Point, in response to a PREQ;
- `Path Error` (PERR) elements are used to notify that a path is not available anymore; and
- `Root Announcement` (RANN) elements are flooded into the network in one of the proactive operation modes (there are two proactive modes in HWMP as it will be described later).

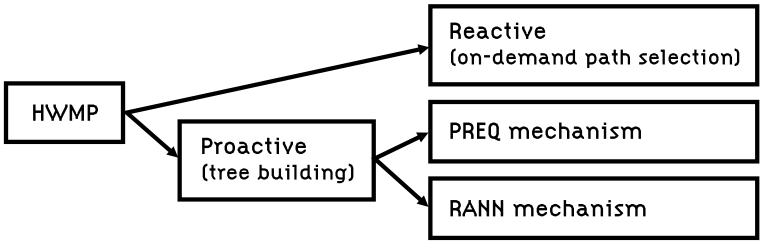


Fig. 19.4 IEEE 802.11s HWMP mechanisms.

The above-listed frames are employed in all of the three mechanisms HWMP provides. The mechanisms are summarized in Fig. 19.4. The first one, which is reactive, is called on-demand path selection. The other two are proactive and are named PREQ and RANN mechanisms.

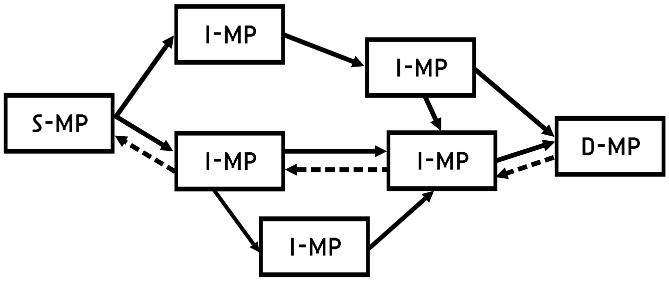


Fig. 19.5 802.11s on-demand path discovery example.

Fig. 19.5 displays a topology example for the on-demand path discovery mechanism. The Source Mesh Point (S-MP) needs to find a path to the Destination Mesh Point (D-MP) and in order to do so S-MP needs the cooperation of Intermediate Mesh Points (I-MPs).

The mechanism works as follows. First, S-MP broadcasts a PREQ frame[1]. Whenever an I-MP node receives a PREQ, it checks to see if it already knows a path to D-MP. If this is the case, this I-MP node issues a PREP frame back to S-MP. S-MP can prevent intermediate nodes from answering PREQs by setting a DO (Destination Only) flag in the PREQ frame. In that case, only D-MP is allowed to respond with a PREP frame. Therefore, when receiving a PREQ with DO set to “1”, any I-MP node may broadcast the PREQ frame again and the process repeats until the request eventually gets to D-MP. Only if the DO flag is not set, an I-MP node (that knows a path to D-MP) may answer PREQ with a PREP frame. Solid-line arrows in Fig. 19.5 represent PREQs while dotted-line arrows represent PREPs.

Another flag, RF (Reply and Forward) can also be used to control the behavior of intermediate nodes. If RF is set to 1, and DO is set to 0, an intermediate node may respond with a PREP frame but it must also broadcast the PREQ frame. Likewise, if both DO and RF flags are set to zero, an intermediate node responds but it does not broadcast the request farther. Hence, the RF flag can limit the quantity of PREPs received by S-MP.

Whenever an I-MP node receives a PREQ, it learns a path back to S-MP. This path is the reverse path and it may be used later (in case this I-MP node is in the selected path) to forward RREP frames to S-MP. Response frames can be unicasted

[1] PREQ, PREP, PERR and RANN frames are management frames with the respective information element.

using this reverse path.

Both PREQ and PREP frames carry a metric field and each I-MP node must increment this metric field accordingly. That is how the destination node (D-MP) is able to choose a reverse unicast path among many possibilities (in a dense mesh) and this is also how the source node (S-MP) chooses the forward path at the end of the cycle.

Regarding the density of a mesh cloud, we should note that, in a wireless medium, coverage and high data rate are conflicting objectives, and increasing one will decrease the other. Broadcast and multicast frames are usually transmitted at low rates in order to reach most nodes, since distant nodes will have a greater probability of receiving them. On the other hand, those frames will take a longer time propagating through the cloud, which may be problematic in a dense environment.

Besides the on-demand path discovery mechanism, HWMP provides two different mechanisms for proactively building a forwarding table, as previously stated. The first is based on the PREQ frames and called “Proactive PREQ mechanism” and the second is based on the RANN frames, therefore named “Proactive RANN mechanism”.

In the proactive PREQ mechanism, when configured to work as a root MP, a node broadcasts a PREQ frame with DO and RF flags set to 1. This PREQ is sent periodically and every receiving MP updates the PREQ frame (decreasing the hop count and updating the path metric) and broadcasts the PREQ again, which eventually reaches all nodes in the mesh cloud.

Whether or not a node answers with a PREP frame upon receipt of a proactive PREQ depends in part on the setting of another flag, the “Proactive PREP”. If the root MP sets it on, all receiving nodes shall send a proactive PREP back to it. A node may send a PREP frame back if it has data to send to the root node and if it wants to establish a bidirectional link, even if the Proactive PREP is not set.

The proactive PREQ mechanism is clearly chatty, particularly in its proactive PREP version. An alternative method is presented by the proactive RANN mechanism. Here, instead of sending PREQs out, a root node can flood the mesh with `Root Announcement` frames. Nodes willing to form a path to the root MP answer with a PREQ frame. This PREQ is sent in unicast mode to the root MP, through the node by which the RANN frame was received, and is processed by intermediate nodes with the same rules applied to PREQ broadcasts in the reactive mode.

The root node answers each of the received PREQs with a respective PREP, thus forming a forward path from each MP to the root MP. At the end, the RANN mechanism introduces one additional step and may be advantageous if compared to the PREQ mechanism only if a small subset of MPs wants to establish paths with the root node.

Finally, it is worth to comment about the role of PERR frames in the mechanisms previously described. Whenever a frame cannot be forwarded by an intermediate node, this fact should be informed to the previous nodes in the path, until it reaches the original sender that will then start a new path discovery cycle. Thus, PERR frames are used for announcing a broken link to all traffic sources that have an active path over this broken link.

19.3.3.2 *Internetworking with 802.11s*

The multihop capabilities of an 802.11s mesh network would be not very useful without the ability to connect the mesh cloud to other networks such as the wired Internet, as illustrated in Fig. 19.6, which shows two examples of internetworking with mesh networks. As previously mentioned, the IEEE 802.11s draft names gateway nodes MPPs (Mesh Portal Points).

Fig. 19.6 (a) illustrates the use of MPPs to interconnect mesh clouds to other LAN networks, when they act like bridges and all nodes belong to the same subnet. Fig. 19.6 (b) depicts another scenario where MPPs act as gateways to different layer-three subnets. In a MANET where all nodes are potentially routers they are also potentially gateways to an infrastructured network.

An MPP basic characteristic is the fact that it is a mesh node (MP) that is also connected to another network, and this capability has to be announced for other MPs to benefit from its connectivity. Thus, once configured as an MPP, a node spreads the news sending a `Portal Announcement` (PANN) frame.

An MP that receives a PANN frame records the MPP MAC address and the associated path metric and then broadcasts the PANN frame again. Each mesh point in the cloud keeps a list of available MPPs and is able to choose among them when it needs to send traffic outside the mesh network limits.

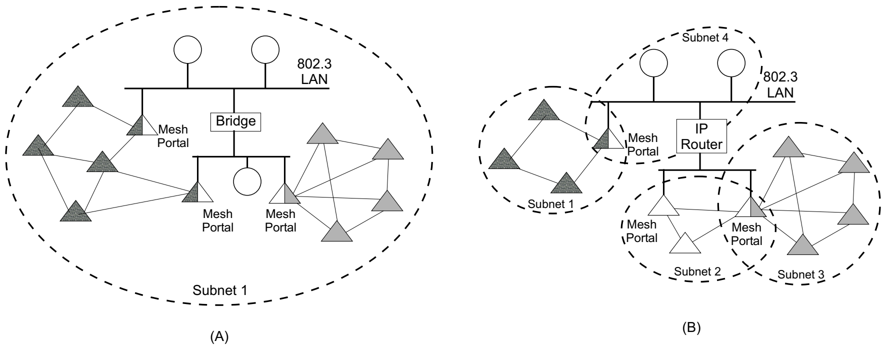


Fig. 19.6 802.11s Internetworking examples. (a) Layer 2 bridging. (b) Layer 3 internetworking.

A Mesh Portal Point may also interconnect mesh networks running different path selection protocols. It is also easy to design the interconnection of many wired 802.3 networks and mesh clouds in a big layer-two bridged network using protocols like 802.1D [IEEE (1998)].

19.3.4 *MAC Frame Structure and Syntax*

In order to allow multihop functions at the MAC layer, the IEEE 802.11s emerging standard extends the original 802.11 frame format and syntax. The new frame format supports four or six MAC addresses and new frame subtypes are introduced as it will be described in the following subsections.

19.3.4.1 *IEEE 802.11s Frame Format*

The first two octets of an 802.11 frame contain the Frame Control field and the third and fourth bits of this field identify the frame type, as shown in Fig. 19.7.

00 = management frames	01 = control frames
10 = data frames	11 = reserved

Fig. 19.7 802.11s frame types.

Besides those two bits, there are also four more bits devoted to a frame subtype. A beacon, for instance, is a management frame (0x0) of the beacon subtype (0x8), while an acknowledgement is a control frame (0x1) of subtype 0xD.

Since 802.11s is an amendment to 802.11, the frames it introduces must fall into the four pre-existing categories. Initially the reserved (0x3) type was considered for mesh traffic. Instead, it was decided to extend the data and management frames in the following ways:

- data exchanged between MPs are transported by `Mesh Data` frames, defined as data frames (type 0x2), where a mesh header is included in the frame body; and
- mesh-specific management frames, such as PREP or PREQ, belong to type 0x0 (management) and subtype 0xF, which was formerly reserved. This new subtype was named `Multihop Action` frames.

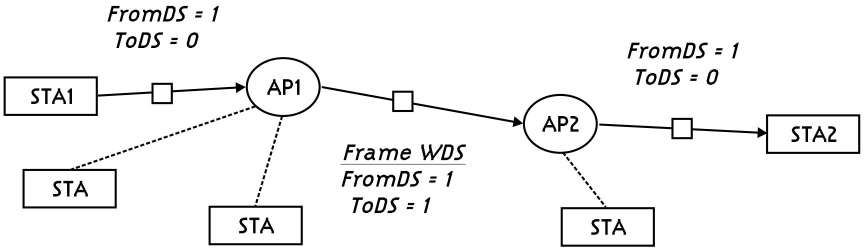


Fig. 19.8 802.11s layer-2 wireless distribution system.

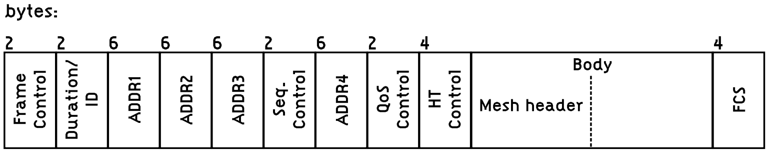
Another characteristic of the new frames is the use of the FromDS and ToDS flags. In 802.11, those bits marked frames as being originated from or destined to a distribution system, which is the infrastructure that interconnects access points. Fig. 19.8 depicts a wireless distribution system that connects two access points (AP1 and AP2) and allows two stations (STA1 and STA2) to exchange frames without the intervention of layer-three protocols. In other words, the distribution system provides bridging for the extended service set.

In a wireless distribution system, or WDS, the backhaul connecting the access points is, as the name implies, wireless. A WDS frame is used to exchange frames between them and has both FromDS and ToDS frames activated. Its original role is to allow transmissions between stations connected to two different access points in the same wireless local area network. IEEE 802.11s also sets FromDS and ToDS flags in frames transmitted inside a mesh cloud.

The IEEE 802.11 standard defines frames where FromDS and ToDS flags are set to 1 as "data frames using the four-address format". This definition will be changed to "A data frame using the four-address MAC header format, including but not limited to mesh data frames" when the "s" amendment is approved. The fact that WDS implementations are vendor specific may potentially raise up issues of compatibility with the emerging standard.

As we described the use of the DS flags, we should notice that both are set to zero in ad hoc 802.11 frames. In an ad hoc network, peer-to-peer transfers can happen opportunistically in a way that should not be confused with that proposed by a mesh network, where frame forwarding, i.e. multihop forwarding, capabilities are present.

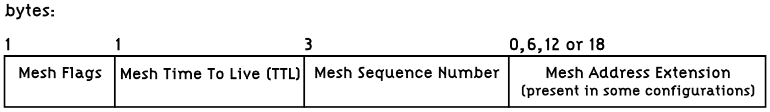
Fig. 19.9 shows the general structure of an IEEE 802.11 frame extended by a Mesh Header (included in the frame body). The Mesh Header is represented in Fig. 19.10 and contains four fields.



bytes:

2	2	6	6	6	2	6	2	4		4
Frame Control	Duration/ ID	ADDR1	ADDR2	ADDR3	Seq. Control	ADDR4	QoS Control	HT Control	Body Mesh header	FCS

Fig. 19.9 802.11s MAC frame structure.



bytes:

1	1	3	0,6,12 or 18
Mesh Flags	Mesh Time To Live (TTL)	Mesh Sequence Number	Mesh Address Extension (present in some configurations)

Fig. 19.10 802.11s MAC frame Mesh Header.

Currently, only the first two bits of the Mesh Flags field are defined. They inform the length of the last field in the header - the Mesh Address Extension field - and vary between zero and three, meaning the number of MAC addresses carried in the Mesh Address Extension field.

The Mesh TTL (Time To Live) field is decremented by each transmitting node, limiting the number of hops a frame is allowed to take in the mesh cloud and avoiding indefinite retransmissions in the case of a forwarding loop.

The three-octets-long Mesh Sequence Number identifies each frame and allows duplicate detection, preventing unnecessary retransmissions inside the mesh cloud. Finally, the aforementioned Mesh Address Extension field carries extra MAC addresses, since the mesh network might need up to six addresses as it will be discussed in the next section.

19.3.4.2 *STAs connectivity and frame addressing*

According to IEEE 802.11s, non-mesh nodes (STAs) can participate in the mesh network through a Mesh Point with Access Point capabilities - MAPs in Fig. 19.2. STAs communicating through the mesh cloud are proxied by their supporting MAPs and this scenario constitutes one example where the novel six-address frame format is employed.

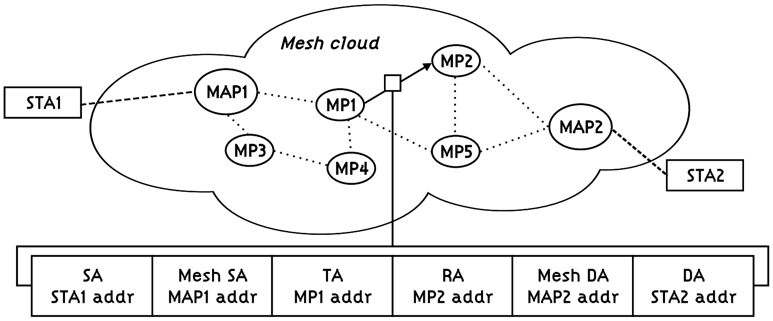
We start our discussion on frame addressing by the more general four-address frame format, which may be used for both data or management frames. The four MAC addresses in this case are:

- SA (source address) is the MAC address of the frame source - the node that generated the frame;
- DA (destination address) is the MAC address of the node that is the final destination of the frame;
- TA (transmitter address) is the MAC address of the node that transmitted the frame. It can be the same as the source address, or the address of any MP that forwards the frame on behalf of the source (any intermediate node); and
- RA (receiver address) is the MAC address of the node that receives the frame. It is the address of the next-hop node and, on the last hop to the destination, it becomes the same as DA.

In short, SA and DA are associated to the endpoints of a mesh path, while TA and RA are the endpoints of each single link. Four-address frames are originally supported by IEEE 802.11 for transmissions using a WDS (Wireless Distribution Systems) but, as mentioned before, they are not enough to implement all features described in the emerging standard.

As we exemplified above, if two non-mesh STAs are communicating through the mesh, two additional addresses will be necessary - the Mesh Source Address (Mesh SA) and the Mesh Destination Address (Mesh DA). In order to understand them, DA and SA entities are defined in a more general way:

- Mesh SA - In a six-address frame, the SA (source address) is the source communication endpoint, that is, the node outside the mesh cloud that originates the frame. Then, the Mesh SA is the node that introduces the frame in the mesh cloud (on behalf of the SA); and
- Mesh DA - Likewise, the DA is defined as the final destination of the frame, while the Mesh DA must be understood as the address of the last node of the mesh cloud that handles the frame.



SA	Mesh SA	TA	RA	Mesh DA	DA
STA1 addr	MAP1 addr	MP1 addr	MP2 addr	MAP2 addr	STA2 addr

Fig. 19.11 802.11s STA connectivity example through various MAPs.

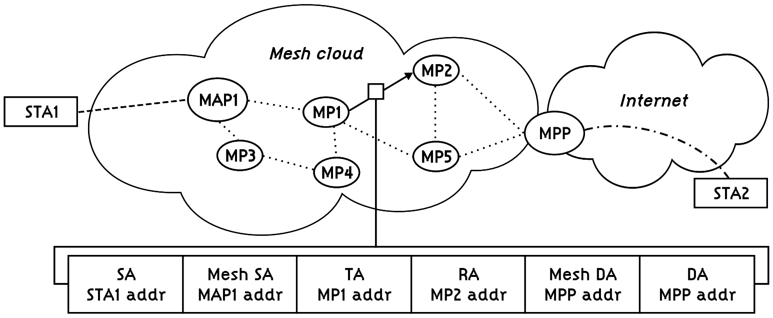
In Fig. 19.11 we depict a scenario where STA1 wants to communicate to STA2, which is associated to another MAP in the mesh cloud. During this transmission, if we analyze a frame while it is being forwarded from node MP1 to node MP2, the six-address scheme will be in use (addresses are shown in the figure).

Another case where the six address format is to be used comes from the HWMP tree-based mode, where two nodes can communicate through a root MP. In this scenario the complete path includes two sub-paths - one from the source MP to the root MP and another from the latter to the destination MP. Finally, mesh points can also communicate with the “outside world” through MPPs. In all those cases, more then four addresses are necessary.

In Fig. 19.12 we present a scenario where MAP2 is substituted by an MPP node. In this case five different addresses are necessary. The six-address frame format is employed again and both the Mesh DA and DA are set to the MPP MAC address. It is responsibility of the MPP to act as a gateway and forward the traffic to an STA outside the mesh cloud, possibly using layer-three traditional routing.

19.3.5 *Additional features*

The IEEE 802.11s standard covers much more ground than we could address in a book chapter. We tried to cover the most important points that touch the operation of a mesh network, but there are still some interesting aspects [Camp and Knightly



SA	Mesh SA	TA	RA	Mesh DA	DA
STA1 addr	MAP1 addr	MP1 addr	MP2 addr	MPP addr	MPP addr

Fig. 19.12 802.11s STA internetwork connectivity example through an MPP.

(2008)].

IEEE 802.11s introduces a medium access method called Mesh Deterministic Access (MDA), which helps reducing contention through the use of a new coordination function. This mechanism is optional and may be implemented by a subset of the MPs present in a mesh cloud. As a consequence, MDA-enabled Mesh Points must be able to interoperate with non-MDA MPs, potentially hurting the efficacy of the scheme.

The core idea of MDA is the introduction of periods of time, called MDAOPs (MDA Opportunities), during which MDA-capable nodes have the opportunity to access the medium with less contention (there may still be contention due to the presence of non-MDA nodes). MDA is implemented through five new action frames: `MDA Setup Request, MDA Setup Reply, MDAOP Advertisement Request, MDAOP Advertisements, MDAOP Set Teardown` [IEEE (2007)].

Congestion Control is only quickly addressed in the standard proposal. A congestion control mechanism must be selected for the whole network and will be also advertised in the `Mesh Configuration` element, along with the path selection protocol and metric. The draft describes the format of the `Congestion Control Notification` frame to be sent by an MP to its peer MP (or MPs) in order to indicate its congestion status. However, details on how congestion is detected or what triggers the announcement of congestion are considered beyond the scope of the future standard.

Power savings, on the other hand, received more attention in the draft. The main idea is that some capable nodes, named Power Save Supporting MPs, will buffer frames to other nodes, called Power Saving MPs, and transmit them only at negotiated times. It is a service similar to the one access points may provide to its associated nodes in IEEE 802.11 networks.

In terms of security, IEEE 802.11s describes mechanisms to provide both authentication and privacy. Security is based on Mesh Security Association (MSA) services that provide link security between two MPs and may operate even if there is no central authenticator, i.e. it also supports distributed authentication.

Once configured to enable security, an MP shall establish only secure peer links and renegotiate pre-existing unsecure links. The establishment of a secure peer link involves the exchange of extra frames (a four-way handshake) that will start immediately after the initial exchange of `Peer Link Open` and `Peer Link Confirm` frames.

The IEEE 802.1X [IEEE (2001)] standard is in the MSA core, but pre-shared keys (PSK) may also be employed, what seems viable only for centrally administered mesh networks.

19.4 Conclusions and Future Work

Handheld communication devices, such as PDAs, regular cell phones, smartphones, media players and many other gadgets yet to come, are not only near ubiquity, but converged into wireless devices that may account for most of the data traffic in a near future.

Although TCP/IP stacks are also incredibly universal, not all communication devices are IP devices or need to be one. Also, despite considerable advances in recent years, mobile devices are constrained in many ways if compared to their fixed equivalents. The price of mobility comprises reduced processing power, storage and memory capacity, due to weight and power-conservation issues.

In face of these factors, a layer-two network that is self sufficient in terms of data forwarding, i.e. a multihop layer-two network, seems to be a very appealing asset. It may support non-IP devices and it may be implemented in less capable ones. It may be less demanding, for instance, to port layer-two mesh functionalities to a network interface card, than to include an IP stack (on top of layer-two mechanisms).

An even bigger advantage though, might come from the fact that radio awareness is a natural capability of the link layer. And radio awareness is definitely important in a wireless network, where the communication medium is much more challenging than wired medium. Metrics based on the ever changing link conditions may be of vital importance in such deployments in order to find best multihop paths. One difficulty of layer-three routing protocols for wireless networks is measuring precise link quality based on layer-three packets instead of layer-two, as MAC retransmissions are usually not taken into account in those measures.

As the IEEE 802.11s draft indirectly implies in many instances, a mesh network need not to be homogeneous. More capable devices may have additional services or even support less capable devices in some activities. A Mesh Access Point is an example of such a capable device.

By not dictating every aspect of a mesh network, the future standard may extend its longevity. Its main goal should be to provide interoperability in a diverse and rapidly evolving environment. In that sense, an extensible framework for path selection or congestion control mechanisms might be a valid compromise between conciseness and completeness.

The first implementation of the IEEE 802.11s draft was brought to life by One Laptop Per Child [OLPC (2008)] in its innovative low-cost educational laptop, called XO. OLPC layer-two mesh network is in many aspects a simplified version of the early versions of the draft, what in many ways helped it being consistent with the evolving proposal. In the OLPC implementation there are no proactive path selection mechanisms (either PREQ-based or RANN-based), but only a reactive on-demand version of HWMP was implemented. MPPs are not announced in advance but discovered by the willing MP, which actively searches for a special anycast MAC address.

The whole implementation lives in the Marvell 88W8388 SoC, which includes an ARM9 low consumption processor, volatile and ROM memory and an 88W8015 radio chip. The radio subsystem is connected to the CPU via an USB bus and may remain powered even when the main CPU is not. An XO can participate in a mesh cloud and forward frames on behalf of other nodes without the use of the main CPU or a TCP/IP stack.

OLPC has also developed standalone active antennas, which host basically the same independent radio subsystem of the XO. These devices help improving the coverage of the mesh cloud and are a good example of non-IP communication devices.

Another implementation initiative of the future standard is the Open802.11s project [Open802.11s (2008)], which is sponsored by a consortium of companies and has the final goal of creating a totally free implementation of the IEEE 802.11s standard.

It is expected that IEEE 802.11s will be a relevant amendment to the all successful IEEE 802.11 family of standards through its multihop forwarding capabilities.

Acknowledgments

The authors would like to thank Javier Cardona from Cozybit and Michalis Bletsas from OLPC for their valuable comments regarding IEEE 802.11s implementation.

This work is supported in part by CNPq, CAPES, FAPERJ, FUNTTEL, and FUJB.

Problems

(1) What are the main differences between a WMN and a WLAN?
(2) Cite two examples of quality-aware routing metrics.
(3) Describe the main characteristics of ad-hoc, controlled-flooding, traffic-aware and opportunistic routing protocols.
(4) Describe the main functionalities of MAPs and MPPs in the IEEE 802.11s mesh network architecture.

(5) What is the (current) mandatory path selection protocol for IEEE 80211.s and what are its main characteristics?

(6) What is the (current) mandatory metric for IEEE 80211.s and what are its main characteristics?

(7) May a vendor implement its own path selection protocol and metric and still be compliant to IEEE 802.11s?

(8) What advantages and disadvantages may the layer-two approach proposed by the IEEE 802.11s bring when compared to traditional layer-three solutions?

(9) Suppose there is a path between two nodes in a mesh network. Is it safe to assume that the reverse and forward paths include the same intermediate nodes?

(10) Describe the six-address format used in the IEEE 802.11s mesh frame structure.

Bibliography

Aguayo, D., Bicket, J., Biswas, S., Judd, G. and Morris, R. (2004). Link-level measurements from an 802.11b mesh network, in *ACM SIGCOMM*, pp. 121–132.

Aguayo, D., Bicket, J. and Morris, R. (2005). SrcRR: A high throughput routing protocol for 802.11 mesh networks (DRAFT), Tech. rep., MIT.

Akyildiz, I. F. and Wang, X. (2005). A survey on wireless mesh networks, *IEEE Communications Magazine* **43**, 9, pp. S23–S30.

Akyildiz, I. F., Wang, X. and Wang, W. (2005). Wireless mesh networks: A survey, *Computer Networks* **47**, 4, pp. 445–487.

Bahr, M. (2006). Proposed routing for ieee 802.11s wlan mesh networks, in *WICON '06: Proceedings of the 2nd annual international workshop on Wireless internet* (ACM, New York, NY, USA), ISBN 1-59593-510-X, p. 5, doi:http://doi.acm.org/10.1145/1234161.1234166.

Biswas, S. and Morris, R. (2005). ExOR: Opportunistic multi-hop routing for wireless networks, in *ACM SIGCOMM*, pp. 133–144.

Bruno, R., Conti, M. and Gregori, E. (2005). Mesh networks: Commodity multihop ad hoc networks, *IEEE Communications Magazine* **43**, 3, pp. 123–131.

Camp, J. and Knightly, E. (2008). The IEEE 802.11s extended service set mesh networking standard, *IEEE Communications Magazine (to appear)* .

Campista, M. E. M., Esposito, P. M., Moraes, I. M., Costa, L. H. M. K., Duarte, O. C. M. B., Passos, D. G., Albuquerque, C. V. N., Muchaluat-Saade, D. C. and Rubinstein, M. G. (2008). Routing metrics and protocols for wireless mesh networks, *IEEE Network* **22**, 1, pp. 6–12.

Clausen, T. and Jacquet, P. (2003). Optimized link state routing protocol (OLSR), IETF Network Working Group RFC 3626.

Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., Qayyum, A. and Viennot, L. (2001). Optimized link state routing protocol, in *IEEE International Multi Topic Conference (INMIC)*, pp. 62–68.

Couto, D. S. J. D. (2004). *High-Throughput Routing for Multi-Hop Wireless Networks*, Ph.D. thesis, MIT.

Couto, D. S. J. D., Aguayo, D., Bicket, J. and Morris, R. (2003). A high-throughput path metric for multi-hop wireless routing, in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 134–146.

Cunha, D. O., Duarte, O. C. M. B. and Pujolle, G. (2008). An enhanced routing metric for fading wireless channels, in *IEEE Wireless Communications and Networking Conference (WCNC).*

Das, S. M., Pucha, H., Koutsonikolas, D., Hu, Y. C. and Peroulis, D. (2006). Dmesh: Incorporating practical directional antennas in multi-channel wireless mesh networks, *IEEE Journal on Selected Areas in Communications* **24**, 11, pp. 2028–2039.

David B. Johnson, D. A. M. and Broch, J. (2001). *Ad Hoc Networking*, chap. 5, DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks (Addison-Wesley), pp. 139–172.

Draves, R., Padhye, J. and Zill, B. (2004a). Comparison of routing metrics for static multi-hop wireless networks, in *ACM SIGCOMM*, pp. 133–144.

Draves, R., Padhye, J. and Zill, B. (2004b). Routing in multi-radio, multi-hop wireless mesh networks, in *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 114–128.

Faccin, S. M., Wijting, C., Kenckt, J. and Damle, A. (April 2006). Mesh wlan networks: concept and system design, *IEEE Wireless Communications Magazine* **13**, 2, pp. 10–17.

Iannone, L. and Fdida, S. (2005). MeshDV: A distance vector mobility-tolerant routing protocol for wireless mesh networks, in *IEEE ICPS Workshop on Multi-hop Ad hoc Networks: from theory to reality (REALMAN)*, pp. 103–110.

Iannone, L., Kabassanov, K. and Fdida, S. (2007). Evaluation of cross-layer rate-aware routing in a wireless mesh network test bed, *EURASIP Journal on Wireless Communications and Networking* **2007**, pp. 1–10.

IEEE (1998). IEEE 802.1d. media access control (MAC) bridges, Standard.

IEEE (2001). IEEE p802.1x.port-based network access control, Standard.

IEEE (2007). IEEE p802.11s;/d1.08, draft amendment to standard IEEE 802.11: ESS mesh networking, Standard.

Koksal, C. E. and Balakrishnan, H. (2006). Quality-aware routing metrics for time-varying wireless mesh networks, *IEEE Journal on Selected Areas in Communications* **24**, 11, pp. 1984–1994.

Liu, T. and Liao, W. (2008). On routing in multichannel wireless mesh networks: Challenges and solutions, *IEEE Network* **22**, 1, pp. 13–18.

MITRE Corporation (2006). http://wiki.uni.lu/secan-lab/MobileMesh.html.

Nelakuditi, S., Lee, S., Yu, Y., Wang, J., Zhong, Z., Lu, G.-H. and Zhang, Z.-L. (2005). Blacklist-aided forwarding in static multihop wireless networks, in *IEEE Conference on Sensor and Ad Hoc Communications and Networks (SECON'05)*, pp. 252–262.

OLPC (2008). One laptop per child project, URL `http://laptop.org/`.

Open802.11s (2008). Open 802.11s project, URL `http://open80211s.org`.

Passos, D., Teixeira, D. V., Muchaluat-Saade, D. C., Magalhães, L. C. S. and de Albuquerque, C. V. N. (2006). Mesh network performance measurements, in *International Information and Telecommunicatios Technologies Symposium (I2TS)*, pp. 48–55.

Perkins, C. and Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, in *ACM SIGCOMM*, pp. 234–244.

Perkins, C. E. and Royer, E. B. (1999). Ad hoc on-demand distance vector routing, in *IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100.

Ramachandran, K. N., Buddhikot, M. M., Chandranmenon, G., Miller, S., Belding-Royer, E. M. and Almeroth, K. C. (2005). On the design and implementation of infrastructure mesh networks, in *IEEE Workshop on Wireless Mesh Networks (WiMesh)*.

Raniwala, A. and Chiueh, T.-C. (2005). Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network, in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 2223–2234.

Subramanian, A. P., Buddhikot, M. M. and Miller, S. C. (2006). Interference aware routing in multi-radio wireless mesh networks, in *IEEE Workshop on Wireless Mesh Networks (WiMesh)*, pp. 55–63.

Wang, J., Lee, S., Zhong, Z. and Nelakuditi, S. (2005). Localized on-demand link state routing for fixed wireless networks, in *ACM SIGCOMM*.

Yang, Y., Wang, J. and Kravets, R. (2005). Designing routing metrics for mesh networks, in *IEEE Workshop on Wireless Mesh Networks (WiMesh)*.

Yuan, Y., Yang, H., Wong, S., Lu, S. and Arbaugh, W. (2005). ROMER: Resilient opportunistic mesh routing for wireless mesh networks, in *IEEE Workshop on Wireless Mesh Networks (WiMesh)*.

Zhang, Y., Luo, J. and Hu, H. (2007). *Wireless Mesh Networking Architectures, Protocols and Standards*, chap. 12, Wireless Networks and Mobile Communications Series (Auerbach Publications, Taylor & Francis Group), pp. 391–423.