IEEE 802.11s Multihop MAC: A Tutorial

Ricardo C. Carrano, Luiz C. S. Magalhães, Débora C. Muchaluat Saade and Célio V. N. Albuquerque

***Abstract*—Recently, IEEE started a task group to investigate adding wireless mesh capabilities to its ubiquitous IEEE 802.11 wireless local area networks standard. The proposal is specified as the IEEE 802.11s amendment. Although the IEEE802.11s amendment is still a draft, some implementations based on it may already be found. The first and most widespread of these implementations is the one developed by One Laptop per Child (OLPC) for its educational laptop - the XO.**

One notable feature of IEEE 802.11s is the fact that the mesh network is implemented at the link layer, relying on MAC addresses rather than IP addresses for its mechanisms. This feature enables the design and development of new CPU-free network devices that provide layer-2 multihop communication.

This tutorial describes the main characteristics of the IEEE 802.11s proposal illustrating the advantages and disadvantages of the MAC layer approach in comparison to the traditional layer three paradigm to multihop wireless networks. To achieve this, this work provides a detailed analysis of 802.11s traffic captured in a real testbed, with special attention to the path discovery mechanism. The step by step explanation of the mesh mechanisms highlights how some of the design choices may impact on the scalability and reliability of such networks.

***Index Terms*—IEEE 802.11s, multihop wireless networks, MANETS, wireless mesh networks, HWMP.**

I. Introduction

THE IEEE 802 family of standards is dedicated to the construction of Local Area Networks (LANs) and Metropolitan Area Networks (MANs). Distinguished members of this group are the IEEE 802.3 (Ethernet) and the now almost forgotten 802.5 (Token Ring) but most of the emerging standards in this family deals with networking over the wireless medium [1].

The 802.15, of which Bluetooth is part of, is designed to interconnect personal devices over a short range Wireless Personal Area Network (WPAN). For the creation of the wireless equivalent of a LAN (i.e. a Wireless Local Area Network or WLAN), the IEEE proposed the 802.11 standard; while the 802.16 (a.k.a WiMax) addresses the problem of city-wide networks or WMANs (Wireless Metropolitan Area Networks).

Those three standards have in common the fact that they are strongly based on some sort of infrastructure. In a WPAN - a master device concentrates all traffic. For a WLAN, the access point plays a central role, by relaying all traffic between participating nodes. And, finally, WiMax is also infrastructure bound - its central node is a powerful and resourceful base station.

Manuscript received 9 April 2009; revised 21 August 2009, 14 October 2009, and 23 October 2009.

L. Magalhães is with the Telecommunications Department and R. Carrano, C. Albuquerque and D. Saade are with the Computing Institute, MídiaCom Labs, Universidade Federal Fluminense, Brazil, (e-mail: {carrano, schara, debora, celio}@midiacom.uff.br).

Digital Object Identifier 10.1109/SURV.2011.040210.00037

Though still easy to deploy when compared to their wired counterparts, those technologies are not viable in scenarios where no infrastructure at all is available. The classical example is a disaster area where a natural catastrophe or terrorist attack completely destroyed any infrastructure.

But there is a much more common scenario where infrastructure-free networks are needed - the developing and economically challenged regions where no investments exist to build or maintain a working infrastructure. A non-infrastructure or ad hoc network may be the powerful digital inclusion tool needed to reduce poverty by means of extending access to information and educational contents.

An ad hoc network is a self-forming, self-configuring network that dispenses any infrastructure, even an access point. In such a network a node is able to communicate with any other node within range and also with nodes out of immediate radio range. To implement the latter, an ad hoc network relies on the nodes to relay traffic for the benefit of other nodes. Another important category of multihop wireless networks is generally called “mesh" network. In a “mesh" network some of the nodes are dedicated to the forwarding of traffic of the other nodes, forming a wireless backhaul that may be considered its “infrastructure". A survey of such mechanisms can be found in [2] and a description of the routing protocols and metrics typically used can be found in [3].

The first multihop wireless networks used layer three mechanisms to relay packets from the source to the destination and although network layer implementations are still prevalent in ad hoc networks, there are recent efforts to incorporate the missing multihop capabilities in the three aforementioned IEEE wireless technologies. This tutorial presents the proposal of a “*mesh*" network with 802.11 devices - a goal being pursued by the IEEE 802.11 Task Group “*s*", namely IEEE 802.11s [4]–[6]. It is worth noticing that for this IEEE task group the terms mesh and ad hoc are interchangeable.

The main contributions of this tutorial are a detailed description of some features of the future standard and a step-by-step analysis of real multihop MAC traffic, as well as the highlighting of advantages and disadvantages of the layer two over the layer three approach to the wireless multihop networks.

The remaining of the text is structured as follows. In the second section the main aspects of IEEE 802.11 are covered, since this is the base standard on which all of this work stands on. Section III presents the general analysis of the Mobile ad hoc Networks (MANETs) including their taxonomy, routing protocols and metrics. A more detailed description of the emerging standard IEEE 802.11s is presented in Section IV. The particularities of an example implementation by One Laptop per Child (OLPC), followed by the analysis of a real

TABLE I
IEEE 802.11 AMENDMENTS

Standard or Amendment	Description
802.11-1997	Original standard (from 1997) which described the MAC layer and the FHSS and DSSS modulation techniques (1 and 2Mbps).
802.11a	Approved in 1999 - introduces a new physical layer - OFDM (Orthogonal frequency-division multiplexing).
802.11b	Approved in 1999 - introduces a new physical layer - HR/DSS (High Rate/Direct Sequence Spread Spectrum).
802.11g	Approved in 2003 - introduces a new physical layer - ERP (Extended Rate PHY).
802.11d	Approved in 2001 - introduces support compatibility with international regulations.
802.11e	Approved in 2005 - introduces quality of service (QoS).
802.11h	Approved in 2004 - adapts 802.11a to European Union regulations.
802.11i	Approved in 2004 - introduces new security mechanisms.
802.11j	Approved in 2004 - adapts 802.11 to Japanese regulations.
802.11-2007	Incorporates amendments “a", “b", “d", “e", “g", “h", “i" e “j" to IEEE802.11-1997.
802.11n (draft)	Task Group “n" (TGn) proposes techniques to achieve bands superior to 100Mbps (MIMO or Multiple Input, Multiple Output is possibly the most popular of these techniques).
802.11r (draft)	Task Group “r" (TGr) works on handoff mechanisms, particularly for fast moving devices (vehicles, for instance).
802.11s (draft)	Task Group “s" (TGs) is proposing a mesh network for 802.11 devices.

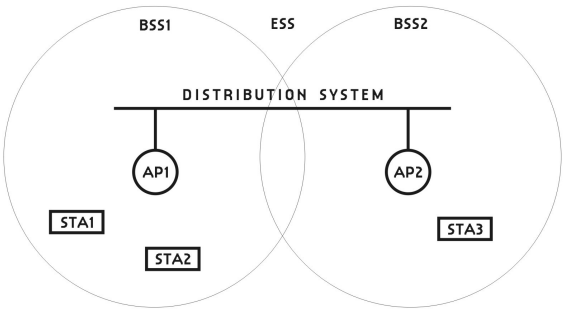


Fig. 1. An Extended Service Set formed by two Basic Service Sets and a Distribution System.

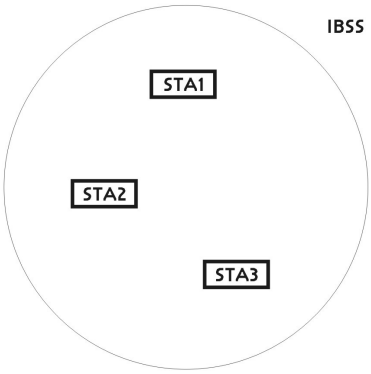


Fig. 2. An Independent Basic Service Set.

case mesh traffic is given in Section V. Concluding remarks are presented in the closing Section VI.

II. IEEE 802.11 WLAN STANDARD OVERVIEW

Among all the wireless network technologies available today, none was so successful in extending local area networks to wireless nodes than those derived from IEEE 802.11 [7]. This standard describes the physical layer and the MAC layer for wireless communication frequencies in the ranges of 2.4GHz and 5GHz. Since its release in 1997, IEEE 802.11 was amended many times to introduce new capabilities or to include different physical layers. Table I provides a list of the most popular past and present amendments.

The IEEE 802.11 standard was augmented to improve bandwidth (IEEE 802.11a, b and g, or the recent draft n); to make them more secure (IEEE 802.11i); to improve support for mobility (draft r); or to introduce quality of service mechanisms (IEEE 802.11e). Recently, a new proposal (IEEE 802.11s) provides multihop capabilities that are discussed in this tutorial.

The IEEE 802.11 standard describes two distinct types of networks, or modes, depending on whether there is or there is not the participation of the specialized node called Access Point. The first, and by far most common, is called infrastructure mode, in reference to the presence of an access point who will mediate all the communications between the nodes which are associated to it. Normally, the access point is also connected to a wired network to which it will extend access to the wireless nodes.

Figure 1 shows a wireless local network (WLAN) where access points are interconnected via a wired distribution system (DS). A group of nodes connected to a same access point defines a BSS (Basic Service Set), while the union of all interconnected access points, bridged due to the presence of the distribution system, is called an ESS (Extended Service Set). It is not uncommon to find distribution systems implemented through wireless links. Wireless Distribution Systems (WDS) are shipped by vendors with proprietary protocols. And some implementations where each member of the distribution system encapsulates and sends its traffic to all of its WDS peers tend to be inneficient.

Associated stations will be able to exchange frames through the access point, to other nodes connected to the same BSS and to other nodes outside the BSS if the access point is connected to a wired network or if it is part of an ESS.

The second type of IEEE 802.11 networks consists only of stations (no access points) that connect to each other in a point to point, on demand fashion, in what is called ad hoc mode (Figure 2). In ad hoc mode there is no provision for multihop paths and nodes are only capable of communicating to peers to which an ad hoc connection was established.

Based on the non-infrastructure approach of the ad hoc mode, a variety of mechanisms was proposed to add routing capabilities to the nodes and surpass the lacking multihop communication. The first implementations employed traditional network layer routing protocols, such as OLSR [8] and AODV [9], which deployed multihop communications through wireless routers as depicted in Figure 3. After a decade of research in ad hoc networks, the amendment “s" is the first to propose a multihop mechanism to be implemented at the MAC layer. In the context of the IEEE standard, the next

section will briefly describe concepts of the most important implementations of multihop ad hoc networks in layer three. These concepts will be explored by the IEEE's proposal of a layer two implementation, described in more detail in the subsequent section.

III. MANETs

A. Introduction

Multihop wireless networks fall into many categories. Sensor networks [10] are an increasingly important class of multihop wireless network. Its main goal is the consolidation of information collected from distributed nodes - the sensors - spread over a given area. The sensor might be mobile – and connectivity might be intermittent [11] – like the collars attached to coyotes in UCSC's CARNIVORE Project [12] or to zebras in Princeton's ZebraNet [13], projects designed to study wildlife; or fixed, like the ones installed in floaters or tree tops to collect environmental data, as temperature or the incidence of light, just to cite a few among many applications of sensor networks. Vehicular Ad Hoc Networks, or VANETs, are a new class of wireless ad hoc networks that is recently receiving considerable attention. The VANET goal is to provide communications among moving vehicles and also between vehicles and fixed equipment. A survey on VANETs can be found in [14].

Probably the most widespread multihop wireless network category is the Wireless Mesh Networks (WMN). A WMN (Figure 3) is basically a collection of fixed nodes, most of the times consisting of regular wireless routers running adapted software. Its main goal is to provide an inexpensive and easily deployable wireless backhaul that will connect distant LANs or WLANs.

Operational WMNs can be found around the world and are mostly based on traditional network layer routing. Some examples are the FunkFeuer Net in Austria [15], MIT's RoofNet [16], VMesh in Greece [17], UCSB's MeshNet [18], CUWin in Urbana [19], Microsoft Mesh [20], [21], among others [22]. In Brazil, Universidade Federal Fluminense (UFF) has deployed the ReMesh Network in the city of Niterói [23] that has been operational since March 2006. There are also propositions for building indoor WMNs, using off the shelf access points, like HomeMesh [24].

A WMN is not necessarily an ad hoc network, in the sense that it can benefit from ahead planning on the position of the nodes (the case of UFF's ReMesh). Nonetheless, nothing prevents it from growing organically like the FunkFeuer Network, in Austria, or the Meraki Public Network in San Francisco [25].

Another category of wireless mobile networks, and the one that we are most interested in, is the Mobile Ad hoc Network, or MANET. These networks are designed to provide connectivity to mobile computing devices without the aid of an infrastructure. In this text, a mesh network, or a mesh cloud, is a MANET.

Differently from a WMN, a MANET is a self-configuring network where there are no fixed routers. In a MANET, routers are free to move and the topology of the network can change dramatically and quickly. Traffic routing functions

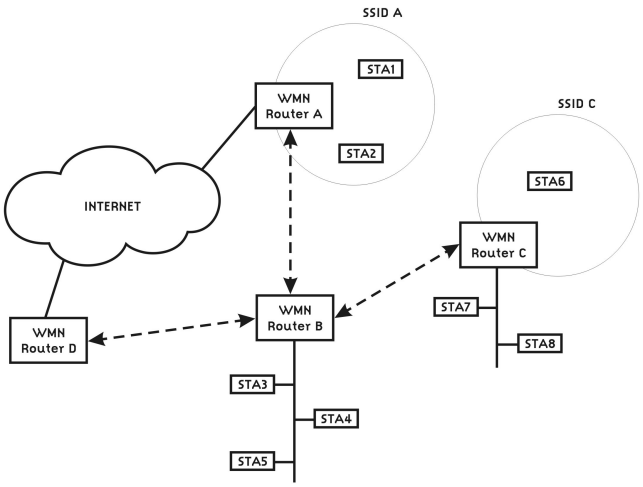


Fig. 3. In a WMN routers provide a wireless backhaul that interconnects wired and wireless stations.

will be carried on by some or all of the participating nodes. Moreover, differently from a sensor network, there may be no clear concentration of traffic to a given node. Though some concentration may happen if one node offers an attractive service to the mesh cloud - like gateway provisions to the Internet - any two nodes might want to communicate. IEEE 802.11s was clearly designed with MANETs in mind, and a relatively small one, of up to 32 nodes [4].

MANETs pose a lot of challenges to routing protocols as they must be able to cope with the specific conditions of wireless networks, particularly when the nodes are mobile: quickly changing characteristics of the radio environment, complex medium access contention, rapidly changing topology, interference and not infrequently, unreliable links.

As the problem of routing is not a new one, there is a natural tendency that the first protocols designed for MANETs are based, in varying degrees, on preexistent routing protocols.

The traditional approach 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 the routing protocols. But when it comes to wireless networks, the choice of layer two to implement the routing protocol is being considered by IEEE.

B. Routing protocols

One of the most common ways of classifying routing protocols for multihop wireless networks is based on the way a route discovery is triggered. There are two opposed approaches, called proactive and reactive, and some attempts to combine both, in hybrid mechanisms.

In the proactive approach, the collection of route information happens in a scheduled manner, independently of the transmission needs. In a proactive protocol, routers are constantly exchanging information. Based on this information, forwarding tables are calculated so, whenever a node has traffic to send out, the routing information will be readily available.

The obvious drawback of this approach is the overhead traffic posed to the network. Routing information is to be

exchanged whether or not they are necessary. Because wireless networks are dynamic in nature (even if the nodes are not mobile, but even more if they are), routing tables may age rapidly and there is the need of constant update messages, which means the reduction of the already relatively scarce bandwidth available for user applications. Examples of proactive protocols specific for wireless networks are the Optimized Link State Routing (OLSR) [26] and the Destination-Sequenced Distance-Vector Routing (DSDV) [27].

In reactive protocols, path discovery mechanisms are activated only when necessary. Nodes will have to wait until the information is gathered, what means a somehow delayed beginning of the transmission. Here, again, paths can rapidly and constantly become unavailable what means that path maintenance mechanisms may be activated many times during a transmission. Examples of reactive protocols are the Dynamic Source Routing (DSR) [28] and the Ad hoc On-Demand Distance Vector (AODV) [9].

In trying to gather the advantages of both proactive and reactive approaches, hybrid proposals have emerged [29]. The Hybrid Wireless Mesh Protocol (HWMP) [30] at layer two, which is part of the IEEE 802.11s draft and will be explained in subsection IV-B, is an example of a hybrid protocol, another example is the Zone Routing Protocol [31] at layer three.

C. Metrics

An important characteristic on which routing decisions can be based is the metric they use. In a network in which nodes move quickly, the links will break and form continuously and the routing protocol must be able to converge to the new topology in a short interval. In such an environment, hop count seems to be a natural choice, particularly if we assume that traffic seems to flow to and from gateways connecting the mesh network to the wired Internet. But it is important to observe that 802.11 networks are multirate networks. It is common for a node to support more than ten transmission rates and, typically, higher rates mean shorter range. For that reason, hop count might not always be the best option. In today's multihop wireless networks, the medium is the scarcest resource and it makes sense to privilege the higher rates, as they consume less airtime, even if this results in longer paths.

One of the earliest proposed quality-aware metrics - the Expected Transmission Count (ETX) [32] - computes the expected number of times a packet would have to be transmitted to successfully reach a neighbor. An evolution of ETX is the ETT metric [20], where the number of tries is replaced by the expected time a node would need to successfully forward a frame. This way, the metric accounts for the different rates at which nodes can transmit in a wireless network.

Recent WMNs implementations may take advantage of some more advanced techniques as the simultaneous use of orthogonal radio channels. This brings new demands in terms of metrics - they will have to account for intra-flow interference (when two nodes transmitting packets from the same flow interfere with each other) and inter-flow interference (when it happens among concurrent flows). An example metric that deals with inter-flow interference is the Weighted Cumulative ETT (WCETT) [20], while the Metric of Interference and Channel-switching (MIC) [33] and iAWARE [34] are designed to deal with both inter and intra flow interferences.

The quick and unpredictable variation of the link quality is another phenomenon to take into consideration when determining an effective metric for wireless networks. Some metrics take the standard deviation in addition to link quality average values. Examples of instability-aware metrics are the modified ETX (mETX) and the Effective Number of Transmissions (ENT) [35].

Another increasingly popular approach is the use of power-aware metrics [3], which accounts for the battery power available for a given node in a mesh. Power aware metrics are more keen to MANETs where the routing nodes are mobile (and thus battery powered) than to WMNs, where routing nodes may in general be AC powered.

The next section discusses the IEEE 802.11 Task Group "s" metric called the Airtime Link Metric, whose main goal is to save the medium, by taking into account not only the datarates that a given link can support, but also the probability of success on the transmission of frames.

IV. 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 3.02) [4], 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 it is important to keep in mind that this is still a work in progress. Nevertheless, implementations of this draft are already available in some wireless devices, like the XO laptop.

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). A MAC layer solution fits that purpose, since it is lightweight in contrast to a full implementation of ad hoc routing.

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.

Originally, two path selection mechanisms were proposed in the draft, RA-OLSR (Radio-Aware Optimized Link State Routing) [36] and HWMP (Hybrid Wireless Mesh Protocol). RA-OLSR is a proactive controlled-flooding protocol based on OLSR but adapted to work at layer-two instead of three. HWMP is a hybrid protocol, based on AODV, which is actually the mandatory protocol and the only one remaining in the current proposal (version 3.02). 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, it is important to discuss the mesh creation mechanisms and describe the architecture proposed by the emerging standard.

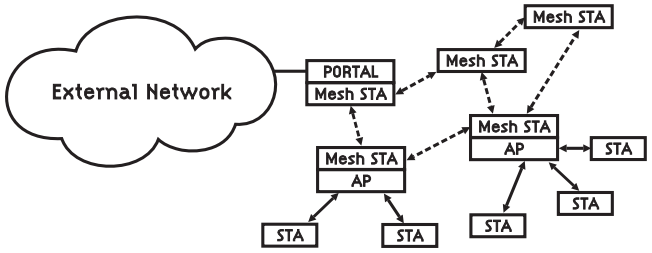


Fig. 4. The 802.11s network architecture.

A. 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 Figure 4:

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

Figure 4 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 (Mesh APs).

In this topology example, there is only one Portal, 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.

Figure 4 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 a Portal may be 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 Portals. These announcement mechanisms will be described later in this text.

1) Mesh Creation: In infrastructured wireless networks, a Service Set Identifier (SSID) is used to distinguish the set of access points, which maintain 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 networks. To avoid misleading a non-mesh station when trying to associate to a mesh network, Mesh STAs 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 STA may support different profiles, but all nodes in a mesh cloud, at a given moment, must share the same profile.

The IEEE 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 Mesh STAs find neighbors that share the same profile. The neighbor discovery mechanism is similar to what is currently proposed by the IEEE 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.

Another important point to be highlighted is the establishment of the Peer links - the edges of a mesh graph. A Mesh STA shall create and maintain peer links to its neighbors that share its active profile (as previously mentioned, a Mesh STA may keep many profiles, but only one is active at a given moment). Once a neighbor candidate is found, through active or passive scanning, a Mesh STA uses the Mesh Peer Link Management protocol 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 Mesh STAs in order to minimize reuse in short time intervals.

To establish a peer link, both Mesh STAs exchange Peer Link Open and Peer Link Confirm frames as depicted in Figure 5. Whenever a Mesh STA wants to close a peer link it should send a Peer Link Close frame to the peer Mesh STA.

2) Internetworking with IEEE 802.11s: The multihop capabilities of an IEEE 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 Figure 6, which shows two examples of internetworking with mesh networks. As previously mentioned, the IEEE 802.11s draft names gateway nodes Portals.

Figure 6(a) illustrates the use of Portals to interconnect mesh clouds to other LAN networks, when they act like bridges and all nodes belong to the same subnet. Figure 6(b) depicts another scenario where Portals 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.

A Portal basic characteristic is the fact that it is a Mesh STA that is also connected to another network, and this capability

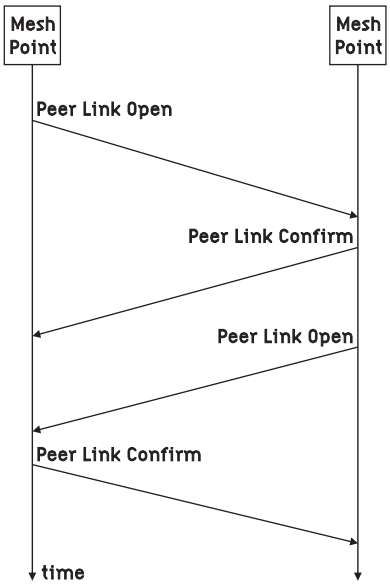


Fig. 5. The establishment of a peer link in 802.11s

has to be announced for other Mesh STAs to benefit from its connectivity. Thus, once configured as a Portal, a node spreads the news sending a Portal Announcement (PANN) frame. A Mesh STA that receives a PANN frame registers the Portal 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 Portals and is able to choose among them when it needs to send traffic outside the mesh network limits.

A Portal may also interconnect mesh networks running different path selection protocols. It is also easy to design the interconnection of many wired IEEE 802.3 networks and mesh clouds in a big layer-two bridged network using protocols like 802.1D [37].

B. Path Selection Mechanisms

IEEE 802.11s proposes a mandatory path selection protocol: a hybrid (proactive/reactive) 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 the configuration parameters, a Mesh Configuration element is transported by beacon frames, Peer Link Open frames and Peer Link Confirm frames. The Mesh Configuration element contains, among other sub-fields, an Active Path Selection Protocol Identifier and an Active Path Selection Metric Identifier.

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 [9] and on its extension AODV-ST [38].

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 Mesh

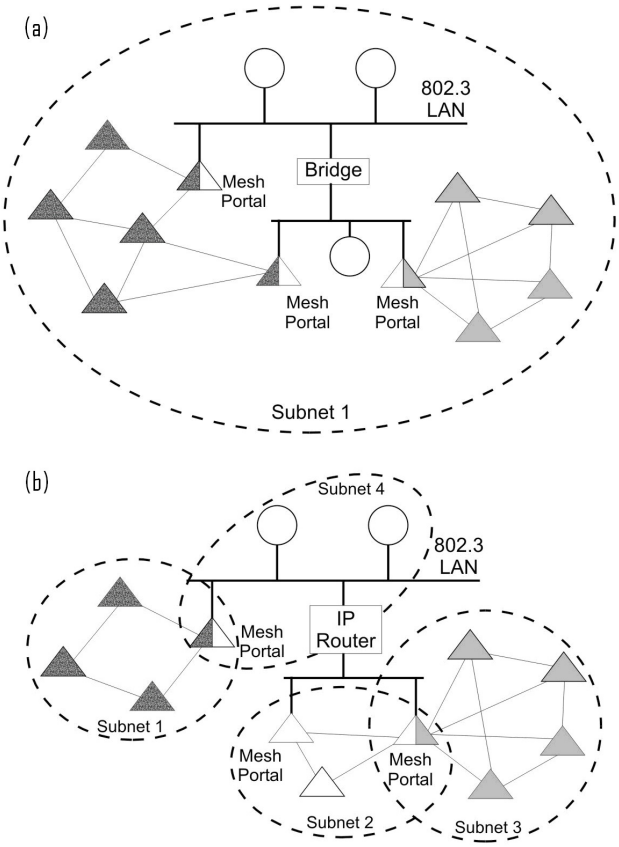


Fig. 6. IEEE802.11s internetworking scenarios. Triangles are Mesh Points (some are Portals), circles are non-Mesh STAs (a) Layer 2 bridging (b) Layer 3 internetworking.

STAs in a peer-to-peer basis; while in proactive mode, a tree-based topology is calculated once a Mesh STA announces itself as a root. The tree-based approach can improve path selection efficiency when there is a tendency for forwarding significant portions of network traffic to some specific nodes, for instance to a Portal serving as the root of the tree.

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 IEEE 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 link error rate. The draft does not specify how to calculate the frame loss probability, leaving this choice to the implementation. Nodes transmitting

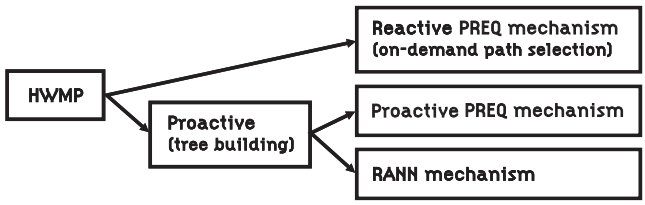


Fig. 7. Path selection mechanisms in 802.11s

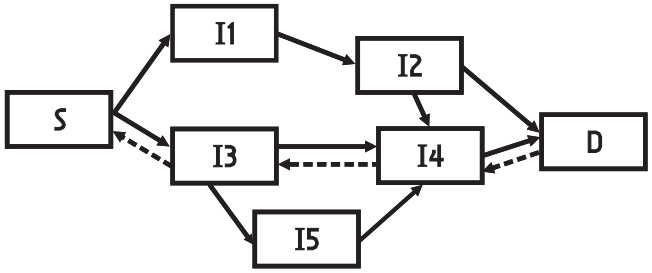


Fig. 8. On demand path discovery where S wants to find a path to D

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:

$$c_a = \left[O + \frac{B_t}{r}\right] \frac{1}{1 - e_f}, \quad (1)$$

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 Mesh STA 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 STA that wants to discover a path to a destination Mesh STA;
- `Path Reply` (PREP) elements are sent from the destination Mesh STA back to the source Mesh STA, in response to a PREQ. Occasionally, PREP elements can be sent from intermediate nodes that already know the path to the destination Mesh STA;
- `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).

The above-listed frames are employed in all of the three mechanisms HWMP provides. The mechanisms are summarized in Figure 7. The first one, which is reactive, is called on-demand path selection. The other two are proactive and are named PREQ and RANN mechanisms.

Figure 8 displays an example for the on-demand path discovery mechanism. The Source Mesh STA (S) needs to find a path to the Destination Mesh STA (D) and in order to do so, S needs the cooperation of Intermediate Mesh STAs (I1-I5).

The mechanism works as follows. First, S broadcasts a PREQ frame. Whenever an I node receives a PREQ, it checks to see if it already knows a path to D. If this is the case, this I node issues a PREP frame back to S. Node S can prevent intermediate nodes from answering PREQs by setting a DO (Destination Only) flag in the PREQ frame. In that case, only D is allowed to respond with a PREP frame. Therefore, when receiving a PREQ with DO set to "1", any I node may broadcast the PREQ frame again and the process repeats until the request eventually reaches D. Only if the DO flag is not set, an I node (that knows a path to D) may answer PREQ with a PREP frame. Solid-line arrows in Figure 8 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.

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

Both PREQ and PREP frames carry a metric field and each I node must increment this metric field accordingly. That is how the destination node (D) is able to choose a reverse unicast path among many possibilities (in a dense mesh) and this is also how the source node (S) 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, a node broadcasts a PREQ frame with DO and RF flags set to 1. This PREQ is sent periodically and every receiving Mesh STAs updates the PREQ frame (decreasing the time to live and updating the path metric) and broadcasts the PREQ again, which eventually reaches all nodes in the mesh cloud.

TABLE II
IEEE 802.11 FRAME TYPES

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

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 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 answer with a PREQ frame. This PREQ is sent in unicast mode to the root, 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 Mesh STA to the root. 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 Mesh STAs wants to establish paths with the root node.

After a path is formed, whenever a frame cannot be forwarded by an intermediate node this fact should be informed to the previous nodes in the path. The PERR frames are used for such purpose, announcing a broken link in the path. The PERR will be sent to all traffic sources that have an active path over this broken link. Each sender that still needs to use the path will then start a new path discovery cycle.

C. 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 present section.

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 Table II.

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 acknowledgment is a control frame (0x1) of subtype 0xD.

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

- data exchanged between Mesh STAs 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 0xD (action frames). There is also a new subtype called Multihop Action frame. This new subtype refers to action frames with four MAC addresses.

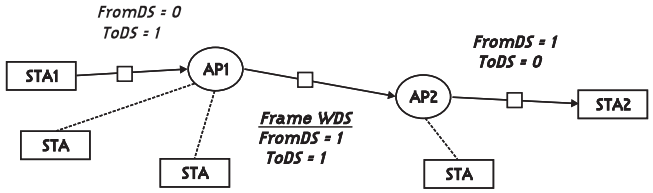


Fig. 9. A frame travels through a Wireless Distribution System

Another characteristic of the new frames is the use of the FromDS and ToDS flags. In IEEE 802.11, those bits marked frames as being originated from or destined to a distribution system, which is the infrastructure that interconnects access points.

Figure 9 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. Similarly, 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 rise up issues of compatibility with the emerging standard.

Notice that both flags (FromDS and ToDS) are set to zero in ad hoc IEEE 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.

Figure 10 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 Figure 11 and contains four fields.

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

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

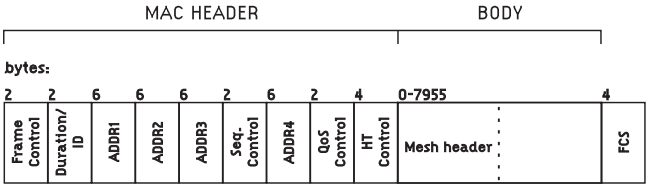


Fig. 10. 802.11 frame format

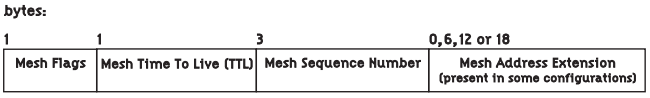


Fig. 11. Mesh Header introduced by 802.11s

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 as follows.

According to IEEE 802.11s, non-mesh nodes (STAs) can participate in the mesh network through a Mesh STA with Access Point capabilities - see Figure 4. STAs communicating through the mesh cloud are proxied by their supporting Mesh APs and this scenario constitutes one example where the novel six-address frame format is employed.

In the more general four-address frame format, which may be used for both data or management frames, the four MAC addresses 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 Mesh STA 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 wireless link. Four-address frames are originally supported by IEEE 802.11 for transmissions using a WDS (Wireless Distribution Systems). In order to support non-mesh stations though, IEEE 802.11s frames need six MAC addresses as shown in Figures 12 and 13.

As previously mentioned, 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

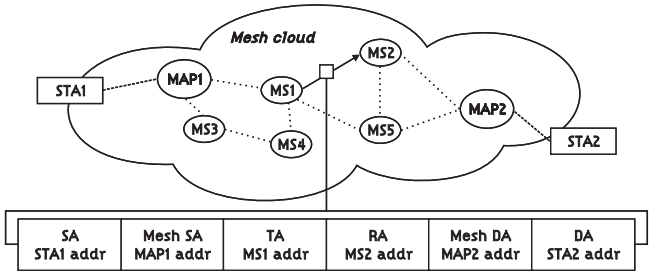


Fig. 12. The six MAC addresses in a frame sent from STA1 and destined to STA2. Note: The address order in the figure does not follow the address order in the frame. The order in the figure was chosen for being more elucidative.

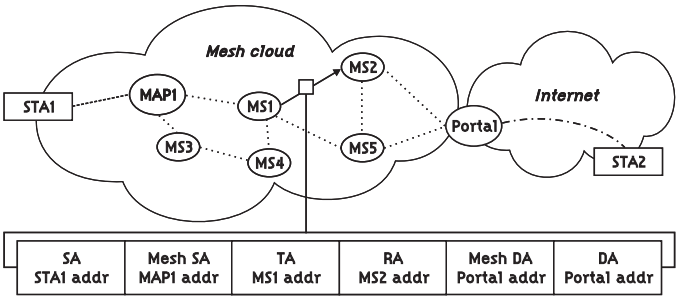


Fig. 13. The six MAC addresses in a frame sent from STA1 and destined to STA2, via a Portal. Note: The address order in the figure does not follow the address order in the frame. The order in the figure was chosen for being more elucidative.

- `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.

Figure 12 presents a scenario where STA1 wants to communicate to STA2, which is associated to another Mesh AP in the mesh cloud. During this transmission, a frame being forwarded from node MS1 to node MS2, uses the six-address scheme (addresses are shown in the figure).

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

Figure 13 shows a scenario where Mesh AP2 is substituted by a Portal 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 Portal MAC address. It is responsibility of the Portal to act as a gateway and forward the traffic to an STA outside the mesh cloud, possibly using layer-three traditional routing.

D. Additional features

The previous sections covered the most important points that touch the operation of an IEEE 802.11s network, but there are still some interesting aspects of the emerging standard to be highlighted.

IEEE 802.11s introduces a medium access method called Mesh Coordinated Channel Access (MCCA), 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 Mesh STAs present in a mesh cloud. As a consequence, MCCA-enabled Mesh STAs must be able to interoperate with non-MCCA Mesh STAs, potentially hurting the efficacy of the scheme.

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

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 a Mesh STA to its peer Mesh STAs 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 Mesh STAs, will buffer frames to other nodes, called Power Saving Mesh STAs, 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 Mesh STAs and may operate even if there is no central authenticator, i.e. it also supports distributed authentication.

Once configured to enable security, a Mesh STA shall establish only secure peer links and renegotiate pre-existing unsecured 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 [39] standard is in the MSA core, but pre-shared keys (PSK) may also be employed, what seems viable only for centrally administrated mesh networks.

V. Multihop MAC example scenario

Empirical analyzes of IEEE802.11s are not easy to obtain since there are no full implementations of the draft. The first IEEE 802.11s based network and the only one actually shipped in real world devices is the one implemented by OLPC (One Laptop per Child) [40]. Recently the Open 802.11s [41], an almost complete implementation of the draft, was released and incorporated in the mainline Linux kernel version 2.6.26. Although it lacks access control and encryption, mesh-wide synchronization and power saving mechanisms, Open 802.11s already implements the airtime metrics and the active (not the proactive components) of HWMP, among other features, but the stack is supported only by Zydas (zd1211rw) and Broadcom (b43) chips.

The analysis in this section is based on version 0.01 of the IEEE 802.11s draft implemented by OLPC. This implementation is embedded in OLPC's educational laptop - the XO or the "one-hundred dollars" laptop - that is now present in more than half a million devices deployed all over the world, in countries like Peru, Uruguay, Mongolia and Rwanda, where the layer-two mesh paradigm is being put to prove everyday by students and teachers.

A. The OLPC-Mesh

OLPC's XO was the first device to implement a mesh network based on the IEEE 802.11s, but the implementation has its own particular characteristics and diverges from the current state of the IEEE 802.11s draft at some points. This subsection explains exactly what these differences are and presents the mesh mechanisms in more detail.

1) Path asymmetry: In IEEE 802.11s HWMP, whenever the on-demand path selection is used, the result will be a bidirectional end-to-end path between the originator (S) and the target Mesh STA (D), meaning that a good path between S and D is assumed to be also a good path between D and S.

Differently from the IEEE proposal, in OLPC's implementation a new path discovery mechanism will be started to find a path between D and S. In one hand, radio links are known to be asymmetrical - the fact that a node A successfully decodes a frame from B does not imply that the opposite is correct. A and B will suffer different interference and contention levels by the mere fact that they are in different positions - a phenomenon perfectly negligible in wired networks, but typical of radio transmissions.

On the other hand, though accounting for path asymmetry may result in more robust forwarding, it is also true that an additional path discovery cycle will increase route acquisition time. This approach may be considered advantageous if (1) path acquisition time is not critical or (2) most paths are asymmetric.

2) Metrics: The calculation of link cost is one item where the IEEE proposal and the OLPC implementation are significantly different. The first introduces the Airtime link metric that reflects the time necessary for the frame to be successfully transmitted, and this time calculation takes the error probability into account. For OLPC, the cost for a given link will be derived exclusively from the data rate at each of the PREQs that reaches the destination. There is no account for the error probability other than the successful reception of the PREQ frame at a given data rate.

To start the path discovery to a given destination, an XO will send a set of PREQs consisting of four frames sent at different transmission rates, here and after called a PREQ cluster. The data rates are 54Mbps, 36Mbps, 11Mbps and 1Mbps, as seen in Figure 14a. The default associated cost for each of these rates is 13, 28, 42 and 64, respectively - a lower rate will have a higher (hence worse) cost.

3) The path discovery mechanism in detail: After the initial cluster of PREQs is broadcasted, intermediary nodes will begin to rebroadcast them and flood the entire mesh cloud - a process called Network Wide Broadcast [42], or NWB - in an attempt to reach the destination. In figure 14b node I1 broadcasts a new cluster of PREQs after receiving the PREQ cluster from node S. In the current implementation, the first PREQ received by an intermediary node will be immediately rebroadcasted, but a delay time will be respected before additional PREQs are forwarded. During this delay time, the node may receive multiple PREQs, not only with different metrics, but also from different transmitters, but only the PREQ with the best metric will be rebroadcasted after this time expires. This mechanism will avoid unnecessary consumption of airtime. After all, reactive protocols can be extremely bursty and rebroadcasting every single PREQ a node receives would make things even worse.

Since broadcast frames are not acknowledged, they lack any retransmission mechanism and this fact alone advocates for some level of redundancy as necessary or many path discovery cycles would not succeed. On the other hand, another means for improving broadcast/multicast reliability is reducing the transmission data rate for multicast/broadcast frames. But since lower transmission rates mean longer transmission times, there is a clear tension between coverage/reliability on one side and spectrum efficiency on the other.

After the PREQ delay period is finished (by default this time is 10ms, but it is adjustable), a new timer will be fired, as the intermediary node may still receive additional PREQs. In this case, the node will retransmit only the best PREQ received during this second period.

An intermediary node will not simply rebroadcast a single PREQ, it must actually make a new PREQ cluster based on the first PREQ received and also for every best PREQ received over the delay time period. This means that an intermediary node will rebroadcast at least a complete cluster (4 frames) and maybe more, depending on the configured delay time and on the mesh density. It is an inherent characteristic of a dense cloud that an intermediary node will receive many PREQs coming from different paths, with different metrics and hop counts. It is not impossible that PREQs with lower costs (better metrics) are received after PREQs with higher metrics. Thus, in a dense mesh, a short delay time will pose a higher control overhead on the cloud.

It is also worth noticing that there is no DO or RF flags present in the XO path discovery frames. In fact, there is an implicit DO flag, since an intermediary node will not respond to PREQs. In short, a description of the path discovery mechanism implemented in the XO follows:

Step 0 - S wants to discover a path to D.

Step 1 - S will check its forwarding table for a valid path to D. A valid path is one not expired. Route expiration time defaults to 10 seconds, currently.

Step 2 - If step 1 fails, S will broadcast a cluster of PREQs, consisting of four frames sent back to back at the data rates of 54, 36, 11 and 1Mbps. Each of these frames will have an associated cost (13, 28, 42 and 64).

Step 3 - All intermediary nodes will rebroadcast the first PREQ received in a new cluster. If, for example, the intermediary node successfully decodes the 54Mbps PREQ from S, it will immediately broadcast a new cluster with values 13+13, 13+28, 13+42 and 13+64 for PREQs at 54, 36, 11 and 1Mbps, respectively.

Step 4 - An intermediary node will wait a configurable time - the rreqdelay - before relaying another PREQ cluster if a PREQ with a better associated cost is received later. Note that it is perfectly possible for a node to listen to the 11Mbps PREQ from S (with cost 42) and only then receive another PREQ transmitted at 54Mbps, relayed by another intermediary node with a lower total cost of 26 (after two hops). Figure 14 illustrates this scenario.

All but the first PREQ received will be stored for rreqdelay before being retransmitted. And the intermediary node will only retransmit the best PREQ received during this period. The rreqdelay currently defaults to 10ms.

Step 5 - A number of PREQs will eventually hit the destination node D that will respond with a PREP relative to the path with the lowest cost. At this point, the procedure is the same of what is described in the IEEE 802.11s proposal, besides the fact that if D needs to send traffic back to A, a new path discovery will start.

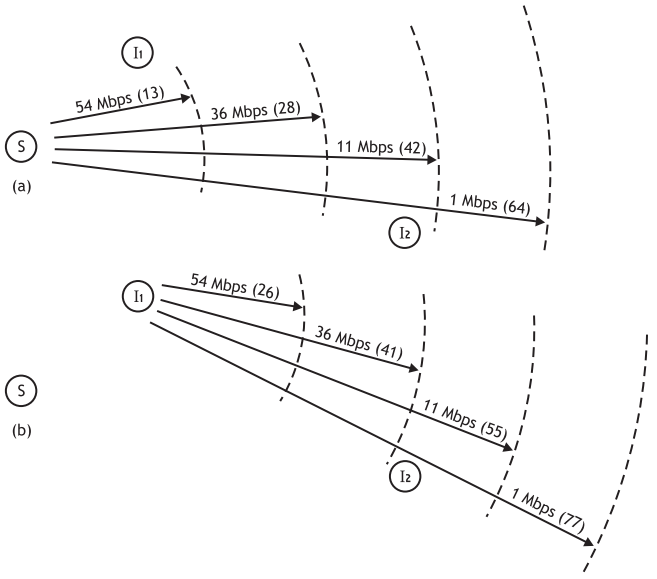


Fig. 14. I2 receives PREQs directly from S and also with one additional hop, from I1

B. Non-implemented features

Some features described in the 802.11s draft are not implemented in OLPC's mesh and this is mainly for two reasons. First, when the first prototypes of the XOs started being tested, the 802.11s draft was in its very first version (0.01) and many points of the proposal were still being discussed.

The second reason is simplicity. The XO is projected to consume low power - about five percent of what a regular laptop would do - and this led to the use of the Marvell 8388

SoC, primarily designed for cell phone use and thus limited in memory and processing power. For this reason every aspect of the draft that is not fundamental was not implemented. A little gain in efficiency on the path discovery mechanism or in the mesh operation could mean a lot of extra complexity and computer power requirements and, in this case, the simpler approach was preferred.

1) Link establishment: For OLPC, there is no idea of a link as being established. There are no Peer Link Open, Peer Link Confirm or Peer Link Close elements and no periodic messages to keep or check if a link is still active (as the Hello messages in AODV). An active neighbor will be a one hop distant neighbor for whom there is an active path in the forwarding table, and nothing else.

2) Security: Currently no security mechanism is implemented at the link layer. Security is left to be implemented at higher layers (examples: network IPsec, SSL transport, application), though it is true that none of these mechanisms would prevent authentication issues or spoofing, for instance. Traditional techniques for secure MANETs are discussed in [43], [44]. On the other hand, security is one of the topics that are still under heavy debate in the draft.

3) Other features: An XO will contend for the medium using the Distributed Coordination Function (DCF) as described in the 802.11 standard. The MDA, proposed in IEEE 802.11s is not implemented. Also Congestion Control and the Power Saving mode are not implemented. Actually, none of these three features are implemented either by OLPC or in open80211s.

C. Example

A path discovery mechanism for an ad hoc wireless network, irrespective of the layer in which it is implemented, is considerably more complex than that of a wired network or even that of a wireless network operating in infrastructure mode.

The following example illustrates the connectivity problem seen from the perspective of layers two and three and underlines the complex and time consuming routines involved, with a particular emphasis on its brute-force approach aimed at providing the necessary network robustness.

In the experiment, the traffic resulting from a ping session carried on by two nodes that are not directly connected and must rely on a mesh cloud to forward the traffic was captured and analyzed.

The experiment was performed with 6 XOs forced into a given topology that is represented in Figure 15. To achieve this, each XO was set, through the use of a feature known as “blinding table", to discard all traffic but the one coming from a subset of the other XOs (for instance, node A will discard frames if the transmitter is not B or E).

The devices under test were placed close together (less than two meters separating any two nodes) and the monitoring station was a commercial laptop with a Cacetech Airpcap USB adapter, which recorded the session traffic in tcpdump format, via the Wireshark Utility [45].

Though a very simple set up, the underlying complexity of operations in a mesh cloud becomes quickly evident. The

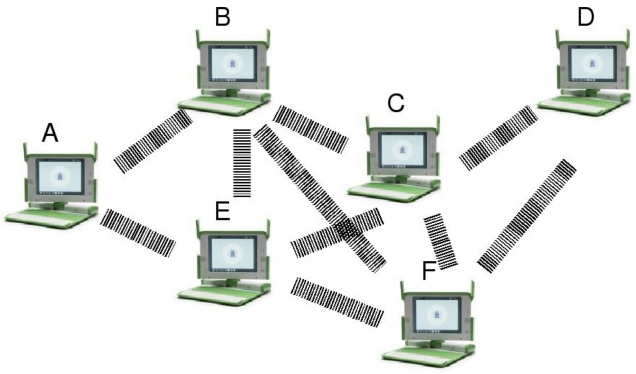


Fig. 15. The testbed topology

test consists of a ping session from node A to node D. The first ping from A will trigger an ARP (Address Resolution Protocol) resolution to find the MAC address of D. In order to better analyze the whole process, the test was divided in five sections that account for the initial ARP and path resolution and the eventual sending of the ICMP traffic itself.

The test conditions were near ideal, since there was no detectable Wi-Fi network operating in the same channel in the vicinity (as inspected by a station running Kismet [46]) and the noise level was verified to be less than -95dBm (as checked with a station equipped with a Wispy [47] spectrum analyzer).

The captured traffic will be presented in tables, with one line for each frame. For clarity and conciseness, acknowledgment frames were omitted from the tables. Likewise, periodic management traffic, such as beacons and probe requests and responds were also eliminated. All times are relative to the monitoring station, that is, in itself, a radio device subject to the limitations of this class of devices, possibly missing occasional frames or being subject to phenomena like the capture effect [48].

The traffic analyzes is made in five phases, each described separately. In phase 1, A wants to ping D and sends out ARP requests for the MAC of node D. In phase 2, as the ARP requests reach D, the latter has to start a path discovery to node A. Once D knows a path to A, it may send his ARP response, and this is covered in phase 3. At this point, A has the MAC address of D and must start a Path Discovery to reach it, as explained in phase 4. Finally, in phase 5, the ICMP traffic may start, closing the experiment.

1) A sends out ARP requests for the MAC of node D: The experiment begins with the ping application in node A, requesting the sending of an ICMP echo request to node D. As the MAC address of D is still unknown, this will trigger an ARP resolution. This first ARP request marks the start of our time line, and is displayed in line 1 of Table III, at time zero.

As an ARP request is a broadcast frame, the mesh cloud must be flooded so that each of its participating nodes receives the request. This is seen in the last 4 lines of Table III. First, nodes B and E will rebroadcast the ARP request, and then nodes C and D will do the same. The fact that a rebroadcast of the ARP request coming from node E was not captured may be explained by the simple fact that the monitoring station missed

TABLE III
A SENDS AN ARP REQUEST TO GET THE IP OF THE DESTINATION NODE D

No.	Time	Source	Destination
1	0.000000	mac[A]	Broadcast
2	0.001195	mac[B]	Broadcast
3	0.002442	mac[C]	Broadcast
4	0.003172	mac[F]	Broadcast
5	0.003719	mac[D]	Broadcast

it. This is because, in the current implementation, an XO will retransmit a broadcast frame at least one time, meaning that node E at least tried to transmit it once.

This brute-force approach to flood the network (a method sometimes referred to as simple flooding [42]) is wasteful and also accounts for the unnecessary retransmission of the ARP request by its final destination. This is a consequence of the multilayer design where layer two is in charge of the rebroadcasting mechanism that will flood the mesh cloud and will do it before and irrespective of the layer three processing of the ARP request. For instance, in Table III, notice that node D also rebroadcasted the ARP request addressed to itself. This is the side effect of the independence between layer two processing, performed by the wireless NIC and the IP processing performed by the main CPU in the XO - the wireless NIC ignores the host IP address and rebroadcasts the ARP request.

After a little longer than three milliseconds, the ARP request reached D. It is interesting to analyze further the fact that the ARP request from E was lost. Besides the fact that the monitoring station might have missed it, previous experiments with larger testbeds [49], involving more nodes, demonstrated that the flooding of a large and particularly dense mesh cloud, i.e. one in which all/most nodes are within the same transmission range, with a brute-force algorithm is a problematic approach as it triggers many simultaneous retransmissions that will increase the probability of collisions.

2) Path discovery to node A: Once D receives the ARP request for its MAC address, it needs a path to A in order to be able to respond it with an ARP reply. Since the ARP reply is a unicast frame, the flooding mechanism will not be used to transport it. And since, in this case, D does not know a path to A, it needs to start a path discovery cycle, that will actually result in a network flooding.

At about 4.2 ms after the start of the experiment, D will start broadcasting a PREQ cluster, consisting of four PREQ frames sent at different data rates and with different associated metrics. The four frames will be sent back to back in an operation that will take about 1.22 milliseconds, where the transmission of the 1Mbps PREQ will account for most of this time (0.88 ms).

The idea behind the transmission of the low rate PREQ is that this will increase the coverage of the mesh cloud, as low rate signals are better decoded by distant nodes than its faster counterparts. The obvious disadvantage is the consumption of airtime, particularly because each of the participating nodes will rebroadcast a complete cluster of Path Request frames.

Therefore, for the path discovery mechanism, the need for an airtime efficient network-wide broadcast is even more important. As it can be seen in frames 10 to 16 of Table IV, nodes

TABLE IV
D STARTS A PATH DISCOVERY TO A, IN ORDER TO BE ABLE TO RESPOND TO THE ARP REQUEST

No.	Time	Source MAC	Destination MAC	Data Rate (Mbps)	Action type
6	0.004235	mac[D]	Broadcast	54.0	PREQ
7	0.004431	mac[D]	Broadcast	36.0	PREQ
8	0.004786	mac[D]	Broadcast	11.0	PREQ
9	0.005652	mac[D]	Broadcast	1.0	PREQ
10	0.005844	mac[C]	Broadcast	54.0	PREQ
11	0.005968	mac[C]	Broadcast	36.0	PREQ
12	0.006066	mac[F]	Broadcast	54.0	PREQ
13	0.006520	mac[C]	Broadcast	11.0	PREQ
14	0.007448	mac[C]	Broadcast	1.0	PREQ
15	0.007594	mac[F]	Broadcast	36.0	PREQ
16	0.008094	mac[F]	Broadcast	11.0	PREQ
17	0.008238	mac[E]	Broadcast	54.0	PREQ
18	0.008443	mac[E]	Broadcast	36.0	PREQ
19	0.009498	mac[F]	Broadcast	1.0	PREQ
20	0.009632	mac[B]	Broadcast	54.0	PREQ
21	0.009965	mac[E]	Broadcast	11.0	PREQ
22	0.010066	mac[B]	Broadcast	36.0	PREQ
23	0.010454	mac[B]	Broadcast	11.0	PREQ
24	0.011422	mac[B]	Broadcast	1.0	PREQ
25	0.030176	mac[A]	mac[E]	1.0	PREP
26	0.032253	mac[E]	mac[C]	1.0	PREP
27	0.034438	mac[C]	mac[D]	1.0	PREP

C and F will contend for the transmission of their Path Request Clusters and, after that, a second wave of retransmissions will be carried on by nodes B and E. Although 15 of the 16 PREQ retransmissions expected to captured (four for each of the four intermediary nodes) were indeed registered, other experiments showed again that in denser environments, collisions will render many of the retransmission useless, and as the PREQ frames are broadcast frames, the sending node will not try to retransmit it. A path discovery traffic storm was observed in testbeds with more than 10 XOs [49].

Differently from the ARP request, and because the path discovery mechanism is implemented at layer two, node A will not wastefully retransmit a path request to its own MAC address. It will, instead, respond the Path Request with a Path Response unicast frame (frame 25, Table IV), that will follow the reverse path back to D, in the example, through E (frame 26) and C (frame 27).

While PREQs will be transmitted at four different data rates, forming the PREQ cluster, PREPs will use solely the robust data rate of 1Mbps. Adding the fact that PREPs are unicast frames, and therefore acknowledged, this may be considered a conservative design choice.

In this experiment, the path discovery cycle took a little longer than 30ms to resolve, but some additional steps are still necessary before the ICMP packets begin to flow. The next phase is the ARP response.

3) ARP response from D: Before roughly 35ms, D is ready to respond the ARP request from A. A two-hop path is now formed from D to A, and the ARP reply from D must be forwarded through this path until it reaches A, as shown in Table V. In this capture, three frames were enough to complete such task, but this is the best case scenario.

In a busier spectrum, with contending nodes, other networks sharing the same spectrum or even sources of interference,

TABLE V
D RESPONDS THE ARP REQUEST FROM A

No.	Time	Transmitter	Receiver	Source	Destination
28	0.036099	mac[D]	mac[C]	mac[D]	mac[A]
29	0.037472	mac[C]	mac[E]	mac[D]	mac[A]
30	0.038822	mac[E]	mac[A]	mac[D]	mac[A]

TABLE VI
A STARTS A PATH DISCOVERY TO D

No.	Time	Source MAC	Destination MAC	Rate	Action type
31	0.040387	mac[A]	Broadcast	54.0	PREQ
32	0.040536	mac[A]	Broadcast	36.0	PREQ
33	0.041006	mac[A]	Broadcast	11.0	PREQ
34	0.042000	mac[A]	Broadcast	1.0	PREQ
35	0.042094	mac[B]	Broadcast	54.0	PREQ
36	0.042308	mac[B]	Broadcast	36.0	PREQ
37	0.042652	mac[B]	Broadcast	11.0	PREQ
38	0.043546	mac[B]	Broadcast	1.0	PREQ
39	0.043958	mac[E]	Broadcast	54.0	PREQ
40	0.044095	mac[E]	Broadcast	36.0	PREQ
41	0.044535	mac[E]	Broadcast	11.0	PREQ
42	0.044753	mac[C]	Broadcast	54.0	PREQ
43	0.045591	mac[E]	Broadcast	1.0	PREQ
44	0.045722	mac[C]	Broadcast	36.0	PREQ
45	0.046184	mac[C]	Broadcast	11.0	PREQ
46	0.046299	mac[F]	Broadcast	36.0	PREQ
47	0.047099	mac[C]	Broadcast	1.0	PREQ
48	0.047496	mac[F]	Broadcast	11.0	PREQ
49	0.048415	mac[F]	Broadcast	1.0	PREQ
50	0.067391	mac[D]	mac[C]	1.0	PREP
51	0.069748	mac[C]	mac[B]	1.0	PREP
52	0.072003	mac[B]	mac[A]	1.0	PREP

there may be the need of retransmissions in some of even all of the links that constitute the path.

4) Path discovery to node D: Contrary to the IEEE 802.11s the XO-Mesh implementation accommodates for path asymmetry, and the path from A to D may be different from the path from D to A. This happens, of course, at the cost of an increased path acquisition time. In this experiment, the acquisition of a return path for the ping traffic took about 32ms (the time elapsed between frames 31 and 52 of Table VI) and the resulting path is indeed different than the path formed from D to A. The path from A to D is through B and C, while the chosen intermediary nodes for the path from D to A, were C and E, as frames 50 to 52 in Table VI and frames 25 to 27 in Table IV show.

5) Pinging: At last the ICMP traffic itself can start. Table VII shows the frames relative to the ICMP traffic. After about 75ms the first frame (number 53) transporting the ICMP echo request from A to D is transmitted. In this experiment, the first ICMP request (the one with ICMP sequence number one) was not lost, because it could be buffered in node A's send buffer for the necessary time (the path acquisition time). For a more demanding application or in a less favorable environment this may not be the case, and the first datagrams of a data flow may be lost.

Moreover, only frame 77 is a retransmission, a rather efficient instance of a multihop wireless traffic. This comes from the fact that the ping traffic is lightweight, with relatively small frames (154 bytes in total) sent every second only. Typically,

TABLE VII
A PINGS D, AND D RESPONDS

No.	Time	IP addrs		MAC addrs				ICMP type
		source	destination	receiver	transmitter	destination	source	
53	0.074525	A	D	B	A	D	A	request
54	0.076321	A	D	C	B	D	A	request
55	0.077116	A	D	D	C	D	A	request
56	0.078627	D	A	C	D	A	D	reply
57	0.079474	D	A	E	C	A	D	reply
58	0.080234	D	A	A	E	A	D	reply
59	0.988336	A	D	B	A	D	A	request
60	0.989139	A	D	C	B	D	A	request
61	0.989864	A	D	D	C	D	A	request
62	0.991235	D	A	C	D	A	D	reply
63	0.991896	D	A	E	C	A	D	reply
64	0.992589	D	A	A	E	A	D	reply
65	1.988273	A	D	B	A	D	A	request
66	1.988937	A	D	C	B	D	A	request
67	1.989564	A	D	D	C	D	A	request
68	1.990836	D	A	C	D	A	D	reply
69	1.991510	D	A	E	C	A	D	reply
70	1.992170	D	A	A	E	A	D	reply
71	2.989359	A	D	B	A	D	A	request
72	2.990008	A	D	C	B	D	A	request
73	2.990662	A	D	D	C	D	A	request
74	2.992033	D	A	C	D	A	D	reply
75	2.992818	D	A	E	C	A	D	reply
76	2.993504	D	A	A	E	A	D	reply
77	2.994021	D	A	A	E	A	D	reply
78	3.989751	A	D	B	A	D	A	request
79	3.990402	A	D	C	B	D	A	request
80	3.991075	A	D	D	C	D	A	request
81	3.992403	D	A	C	D	A	D	reply
82	3.993056	D	A	E	C	A	D	reply
83	3.993723	D	A	A	E	A	D	reply
84	4.989830	A	D	B	A	D	A	request
85	4.990480	A	D	C	B	D	A	request
86	4.991139	A	D	D	C	D	A	request
87	4.992420	D	A	C	D	A	D	reply
88	4.993056	D	A	E	C	A	D	reply
89	4.993781	D	A	A	E	A	D	reply

a file transfer over TCP will pose a significantly higher load and retransmissions will happen much more frequently. The frame loss probability increases with frame size and as the number of retransmissions increase, congestion gets worse. Since this is a tutorial, the authors decided not to show results for a congested scenario and focus on an instructive frame-by-frame analysis of the implemented mechanisms. Performance measurements of congested IEEE 802.11s networks can be found in [49].

The overhead posed by the path discovery mechanism could be reduced by either considering that the paths are symmetric or through the use of the route caches in intermediary nodes, as implemented in AODV, for instance. The latter would nonetheless make the implementation of the path discovery mechanism a little more complex.

VI. CONCLUDING REMARKS

Implementing a path discovery mechanism at layer two is advantageous in terms of a closer relationship between the mechanism and the link layer information readily available. A wireless link is sufficiently more challenging as a medium than

a cable to help supporting that idea. Hence, making decisions based on spectrum conditions, interference, error rates and congestion may be crucial. On the other hand, one can argue that exposing these parameters to upper layers would suffice.

Having a Network Interface Card (NIC) capable of forwarding mesh traffic without the need of implementing a full TCP/IP stack and without the intervention of the host CPU brings some interesting possibilities. In the XO, the main CPU may sleep while the independent wireless NIC, where the mesh code is implemented, will still be able to contribute to the mesh cloud, by forwarding other nodes' frames. The same principle allowed OLPC to build "standalone antennae", which are inexpensive and low power consumption devices that contain only a wireless NIC and are able to perform all the functions of a mesh point, including acting as a Mesh AP or a Portal if connected to a host.

The critics of the layer two approach will point out that IEEE is trying to bring to the link layer functionalities that belong, as they see it, to the network layer. But as we have been watching in the last decades, there is advantage in implementing some functionalities in varied layers, as cryptography for example and, more interestingly, cases where a feature is implemented in more than one layer, as the automatic retransmissions that are usually performed in layer two for wireless links even if the upper layer protocols like TCP or application protocols also retransmit unacknowledged data.

Another issue to consider is whether the added complexity will be a burden to the wireless NICs. They will have to be more capable in terms of processing power and memory requirements - an issue that, as history proves, is expected to fade out with time but, nonetheless, is currently pertinent.

As it is still a draft, there is not much to say about the future adoption of IEEE 802.11s or even its release. There seems to be little agreement on the security model to be implemented and the proposal has gone through important changes. Firstly, mesh frames were demoved from the status of a frame type (using the only lasting reserved type 4) to that of a subtype. Later, the proactive mechanism, described as a Radio Aware version of OLSR (RA-OLSR) was completely removed.

In the WMN landscape it seems that IEEE 802.11s is increasingly irrelevant as OLSR and other proactive protocols mature. The IEEE standard is actually designed to small groups, of less than thirty two nodes [4], of mobile devices that are sufficiently close to each other to permit connectivity with the low penetration wavelength and power levels used by 802.11 interfaces. If distance grows and the mesh network becomes too sparse, there will be no connectivity whatsoever. If the network is too dense, then one can argue that it is better to switch to infrastructure mode and connect to an access point without the overhead of a path discovery mechanism.

Unless such path discovery overhead is dramatically reduced by increasing the efficiency of the flooding mechanisms implemented by vendors (which is not part of IEEE 802.11s), the new standard may be interesting only to a small set of scenarios. The more tempting scenario is probably the infrastructure free deployment represented by a mesh cloud formed by mobile devices - a MANET. This use may foster connectivity in under served areas and help bridging the digital divide [50] in these regions (with distance constraints cited above). Whether all the features described in this tutorial should necessarily be implemented in layer two or in layer three is a debatable matter.

ACKNOWLEDGMENT

This work is partially supported by CAPES, CNPq and FAPERJ. The authors would also like to thank Michail Bletsas and Javier Cardona for their invaluable support during the development of the tests and the writing of this tutorial.

REFERENCES

[1] M. S. Kuran and T. Tugcu, "A survey on emerging broadband wireless access technologies," *Comput. Netw.*, vol. 51, no. 11, pp. 3013–3046, 2007.

[2] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23–S30, Sept. 2005.

[3] M. E. M. Campista, P. M. Esposito, I. M. Moraes, L. H. M. K. Costa, O. C. M. B. Duarte, D. G. Passos, C. V. N. Albuquerque, D. C. Muchaluat-Saade, and M. G. Rubinstein, "Routing metrics and protocols for wireless mesh networks," *IEEE Netw.*, vol. 22, no. 1, pp. 6–12, Jan. 2008.

[4] IEEE, "P802.11s draft d3.02, draft amendment to standard IEEE 802.11: ESS mesh networking," 2008, standard.

[5] J. Camp and E. Knightly, "The IEEE 802.11s extended service set mesh networking standard," *Commun. Mag., IEEE*, vol. 46, no. 8, pp. 120–126, Aug. 2008.

[6] R. Carrano, D. C. Muchaluat-Saade, M. E. M. Campista, I. M. Moraes, C. V. N. de Albuquerque, L. C. S. Magalhães, M. G. Rubinstein, L. H. M. K. Costa, and O. C. M. B. Duarte, *Multihop MAC: IEEE 802.11s Wireless Mesh Networks, Encyclopedia on Ad Hoc and Ubiquituous Computing*. World Scientific, 2009, ch. 19.

[7] IEEE, "802.11 standard: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," 2007, standard.

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

[9] C. E. Perkins and E. B. Royer, "Ad hoc on-demand distance vector routing," in *IEEE Workshop Mobile Comput. Syst. Applications*, Feb. 1999, pp. 90–100.

[10] I. Akyildiz, W. Su, and E. Sankarasubramaniam, Y. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, pp. 102–114, 2002.

[11] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in *ACM SIGCOMM*. New York, NY, USA: ACM, 2004, pp. 145–158.

[12] C. Project, "Movement of top predators: Combining sensor technology and biology," 2009. [Online]. Available: http://www.steps.ucsc.edu/collabs.html

[13] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet," in *ASPLOS*, 2002.

[14] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 2008.

[15] FunkFeuer, "Funkfeuer project," 2009. [Online]. Available: http://www.funkfeuer.at/

[16] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, "Architecture and evaluation of an unplanned 802.11b mesh network," in *ACM International Conf. Mobile Comput. Netw. (MobiCom)*. New York, NY, USA: ACM, 2005, pp. 31–42.

[17] N. Tsarmpopoulos, I. Kalavros, and S. Lalis, "A low cost and simple-to-deploy peer-to-peer wireless network based on open source linux routers," in *IEEE First International Conf. Testbeds Research Infrastructures Development Netw. Communities (TRIDENTCOM)*, 2005, pp. 92–97.

[18] C. C. Ho, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "A scalable framework for wireless network monitoring," in *WMASH '04: Proc. 2nd ACM International Workshop Wireless Mobile Appl. Services WLAN Hotspots*. New York, NY, USA: ACM, 2004, pp. 93–101.

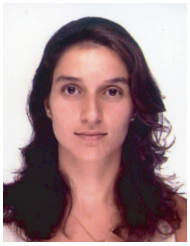
[19] M. Lad, S. Bhatti, S. Hailes, and P. Kirstein, "Enabling coalition-based community networking," in *London Commun. Symp. (LCS)*, Sept. 2005.

[20] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *ACM International Conf. Mobile Comput. Netw. (MobiCom)*. New York, NY, USA: ACM, 2004, pp. 114–128.

[21] ——, "Comparison of routing metrics for static multi-hop wireless networks," in *ACM SIGCOMM*. New York, NY, USA: ACM, 2004, pp. 133–144.
[22] S. Weber, V. Cahill, S. Clarke, and M. Haahr, "Wireless ad hoc network for Dublin: A large-scale ad hoc network test-bed," in *ERCIM News*, vol. 54, 2003.
[23] D. Passos, D. Teixeira, D. Muchaluat-Saade, L. Magalhães, and C. Albuquerque, "Mesh network performance measurements," in *International Inf. Telecomm. Technol. Symp. (I2TS)*, 2006.
[24] T. He, S.-H. Chan, and C.-F. Wong, "Homemesh: A low-cost indoor wireless mesh for home networking," *Commun. Mag., IEEE*, vol. 46, no. 12, pp. 79–85, Dec. 2008.
[25] Meraki, "Meraki public network in San Francisco," 2009. [Online]. Available: http://sf.meraki.com/map
[26] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," IETF Netw. Working Group RFC 3626, Oct. 2003.
[27] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM*, Aug. 1994, pp. 234–244.
[28] D. B. Johnson, D. A. Maltz, and J. Broch, *Ad Hoc Networking*, ser. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. Addison-Wesley, 2001, ch. 5, pp. 139–172.
[29] H. Cheng and J. Cao, "A design framework and taxonomy for hybrid routing protocols in mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 62–73, 2008.
[30] M. Bahr, "Proposed routing for IEEE 802.11s WLAN mesh networks," in *WICON '06: Proc. 2nd Annual International Workshop Wireless Internet*. New York, NY, USA: ACM, 2006, p. 5.
[31] Z. Haas, "A new routing protocol for the reconfigurable wireless networks," in *IEEE 6th International Conf. Universal Personal Commun. Record*, vol. 2. IEEE, 1997, pp. 562–566.
[32] D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *ACM International Conf. Mobile Comput. Netw. (MobiCom)*, Sept. 2003, pp. 134–146.
[33] Y. Yang, J. Wang, and R. Kravets, "Designing routing metrics for mesh networks," in *IEEE Workshop Wireless Mesh Netw. (WiMesh)*, Sept. 2005.
[34] A. P. Subramanian, M. M. Buddhikot, and S. C. Miller, "Interference aware routing in multi-radio wireless mesh networks," in *IEEE Workshop Wireless Mesh Netw. (WiMesh)*, Sept. 2006, pp. 55–63.
[35] C. E. Koksal and H. Balakrishnan, "Quality-aware routing metrics for time-varying wireless mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 11, pp. 1984–1994, Nov. 2006.
[36] Y. Zhang, J. Luo, and H. Hu, "Radio aware optimized link state routing protocol," in *Wireless Mesh Netw. Architectures, Protocols Standards*. Auerbach Publications, Taylor & Francis Group, 2007, pp. 391–423.
[37] IEEE, "802.1D standard: Media access control (MAC) bridges," 1998, standard.
[38] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, "On the design and implementation of infrastructure mesh networks"," Sept. 2005.
[39] IEEE, "802.1x standard: Port-based network access control," 2001, standard.
[40] OLPC, "One laptop per child project," 2008. [Online]. Available: http://laptop.org/
[41] Open802.11s, "Open 802.11s project," 2008. [Online]. Available: http://open80211s.org
[42] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," in *ACM International Symp. Mobile Ad Hoc Netw. Computing (MobiHoc)*. New York, NY, USA: ACM, 2002, pp. 194–205.
[43] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 4, pp. 78–93, 2008.
[44] M. Lima, A. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 66–77, 2009.
[45] A. Orebaugh, G. Ramirez, and J. Burke, *Wireshark & Ethereal network Protocol Analyzer Toolkit*. Syngress Media Inc, 2007.
[46] Kismet, "Kismet: an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system," 2009. [Online]. Available: http://www.kismetwireless.net/
[47] MetaGeek, "Metageek's wispy spectrum analyzer," 2009. [Online]. Available: http://www.metageek.net/Products/Wi-Spy/
[48] L. G. Roberts, "Aloha packet system with and without slots and capture," *SIGCOMM Comput. Commun. Rev.*, vol. 5, no. 2, pp. 28–42, 1975.
[49] R. Carrano, "Improving the scalability and reliability of the XO mesh network," Master's thesis, UFF, 2008.
[50] R. Carrano and L. Magalhães, "Mesh networks for digital inclusion - testing olpc's xo mesh implementation," in *FISL 8th Workshop Free Software*, 2007.

Ricardo Campanha Carrano received his B.S and M.Sc degrees in telecommunications engineering from Universidade Federal Fluminense, Brazil, in 1995 and 2008. He is a PhD student in Computer Science and a Professor at the Science and Technology Department of Puro/UFF. His current research interests include energy conservation and ad hoc networks. He has contributed to the OLPC mesh network development and testing team from 2007 to 2009.

Luiz Claudio Schara Magalhães has a PhD in Computer Science from the University of Illinois at Urbana-Champaign. He has been a professor at the Telecommunications Department at Universidade Federal Fluminense since 1994, instructor at UIUC, Visiting Scholar at HP-Labs in Palo Alto and is currently working for the Brazilian government on the deployment of mesh-network capable educational laptops. His main research interests lie in the area of mobility, large scale infrastructure to support mobile nodes, hiperconnectivity (high-redundancy last mile access) and device environment awareness and cooperation.



Débora Christina Muchaluat Saade received a computer engineering degree, and M.Sc. and D.Sc. degrees in computer science from PUC-Rio, Rio de Janeiro, Brazil, in 1992, 1996, and 2003, respectively. Since 2002, she has been an Associate Professor at Universidade Federal Fluminense, from 2002 to 2009 at the Telecommunications Engineering Departament, and currently at the Computer Science Department. Her major research interests are mesh networks, ad hoc routing protocols, QoS, multicast, multimedia communications, multimedia authoring languages, digital TV and telemedicine applications.

Célio Albuquerque (S'94-M'00) received the B.S. and M.S. degrees in electrical and electronics engineering from Universidade Federal do Rio de Janeiro, Brazil, in 1993 and 1995, and the M.S. and Ph.D. degrees in information and computer science from the University of California at Irvine in 1997 and 2000, respectively. From 2000 to 2003, he served as the networking architect for Magis Networks, designing high-speed wireless medium access control. Since 2004 he has been an Associate Professor at the Computer Science Department of Universidade Federal Fluminense, Brazil. His research interests include wireless networks, Internet architectures and protocols, multicast and multimedia services, and traffic control mechanisms.