Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s

Michael Bahr
Siemens Corporate Technology, Information & Communications
bahr@siemens.com

Abstract

HWMP, the default routing protocol of IEEE 802.11s has been revised during the comment resolution of the first letter ballot. The paper gives an update on three areas where major changes have been introduced to HWMP: support for interworking with other networks; revised concept for proactive routing trees to root MPs; and a better aligned extensible path selection framework.

1. Introduction

What is the difference between so-called Mobile Ad hoc Networks (MANETs) and so-called Wireless Mesh Networks (WMNs)? This question is often asked, and different people might have different answers to it. Both actually follow the same principle: communication between nodes over multiple wireless hops on a meshed network graph, even if they are not in direct wireless range. Efficient, self-organizing routing protocols provide paths through the wireless network and handle the dynamic changes of the topology caused by fluctuations in the radio environment or by the mobility of network nodes. Intermediate nodes forward the data packets to the destination. Both MANETs and WMNs promise greater flexibility, increased reliability, self-organized adaptability to changed network conditions, and improved performance. MANETs and WMNs have a large area of overlap sharing many of the same technical concepts.

An example for the conceptual similarity of MANETs and Wireless Mesh Networks is the upcoming IEEE 802.11s standard for WLAN mesh networking. It contains layer 2 adaptations of two routing protocols well-known from the area of Mobile Ad hoc Networks—AODV [1] and OLSR [2]. And it does not require specific device types: an IEEE 802.11s device can be static or mobile; it can be an infrastructure device, such as a wall-mounted access point, or an end customer device, such as a laptop.

Wireless mesh networks are often divided into backhaul meshes and client meshes. The former consist of infrastructure devices and provide a wireless access network. The latter consist of end customer devices. Combinations of the two are easily imaginable. A survey on WMNs can be found in [3]. Different aspects and mechanisms of wireless mesh networking are described in [4].

Research and development in the area of mobile ad hoc networks and wireless mesh networks are still going strong. The different standardization groups on wireless mesh networks, e.g. IEEE 802.11s, IEEE 802.15.5, and IEEE 802.16j, are progressing continuously. Mesh is a known term in the networking market by now. The most prominent usage scenario are currently WMNs for public wireless access. However, client mesh networks that provide flexible wireless multi-hop networking to end user devices are receiving more attention. For instance, the „One Laptop Per Child“ project uses IEEE 802.11s and HWMP for wireless mesh networking between the laptops [13].

This paper highlights important changes of the Hybrid Wireless Mesh Protocol (HWMP), the default routing protocol of IEEE 802.11s, compared to the very first draft [7]. The changes have been introduced as response to comments on the IEEE 802.11s draft. This paper is based on the current draft version D1.06 from July 2007 [12].

Note, that the standardization of WLAN mesh networks in the IEEE 802.11s task group is still work in progress. The task group is working on further improvements of HWMP, and future letter ballots might require further changes. Nevertheless, the general concepts seem to be quite stable as experience shows, but changes in details are likely.

The remainder of the paper is structured as follows. Section 2 provides a brief overview of IEEE 802.11s and HWMP. Sections 3 to 5 describe three areas in detail, where major changes to HWMP occurred: interworking with other IEEE 802 networks, proactive

1-4244-1455-5/07/$25.00 ©2007 IEEE

tree-routing, and extensible path selection framework. A brief outlook concludes the paper.

2. Overview of IEEE 802.11s and HWMP

The first meeting of the IEEE 802.11 task group „s“ (TGs) on WLAN mesh networking was in July 2004. The goal of the task group is the development of an extensible standard amendment for wireless mesh networks based on IEEE 802.11 [8] that can be used in a flexible way for many usage scenarios [6]. The PAR document [5] defines the scope of the standard development and certain requirements.

The first draft D0.01 for IEEE 802.11s had been produced in March 2006. The IEEE 802.11 working group commented on version D1.0 in December 2006. Currently, TGs is resolving these comments. This will further improve the IEEE 802.11s draft.

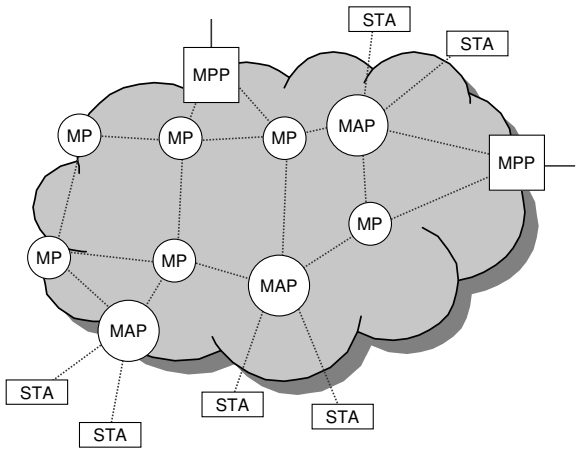

Figure 1: Example of IEEE 802.11s WLAN mesh network

The nodes of a wireless mesh network are called *mesh points (MPs)* in IEEE 802.11s. A mesh point is an IEEE 802.11 station that has mesh capabilities in addition to the basic station functionality. This means that it can participate in the mesh routing protocol and can forward data frames on behalf of other mesh points according to the IEEE 802.11s standard. In Figure 1, all nodes in the cloud are MPs and comprise the wireless mesh network. Mesh points can be end customer devices such as laptops as well as infrastructure devices such as access points.

Mesh points with additional access point functionality are called *mesh access points (mesh APs* or *MAPs)*. Conventional WLAN clients, which are *non-mesh IEEE 802.11 stations (STAs)*, can connect through the mesh APs to the wireless mesh network. Mesh points with additional portal functionality are called *mesh portals (MPPs)*. They can bridge data frames to other IEEE 802 networks, especially to a wired network such as an Ethernet.

IEEE 802.11s aims at WLAN mesh networks of up to 50 mesh points[1], indicating that a scalable solution for large networks with hundreds of MPs is not required by TGs.

IEEE 802.11s WLAN mesh networks will be applicable to a large variety of usage scenarios. The four most important usage scenarios identified by the task group [6] are:

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

The IEEE 802.11s draft can be split into four major parts—routing, MAC enhancements, security, and general IEEE 802.11 related topics. The key functionality is the wireless multi-hop routing and forwarding.

The IEEE 802.11s draft defines a default routing protocol, the *Hybrid Wireless Mesh Protocol (HWMP)*. Every IEEE 802.11s compliant device is required to implement HWMP and to be capable of using it. HWMP is located on layer 2, this means, it uses MAC addresses. The IEEE 802.11s task group decided to use the term *path selection* instead of routing in order to provide a clear terminology with as less potential for ambiguities as possible. This paper, however, uses path selection and routing interchangeably when possible.

HWMP is a hybrid routing protocol. It has both reactive components and proactive components. The foundation of HWMP is an adaptation of AODV [1] to radio-aware link metrics and MAC addresses. It is the basic, reactive component of HWMP. The on-demand path setup is achieved by a path discovery mechanism that is very similar to the one of AODV. If a mesh point needs a path to a destination, it broadcasts a *path request message (PREQ)* into the mesh network. MPs will rebroadcast the updated PREQ whenever the received PREQ corresponds to a newer or better path to the source. Similarly, the requested destination MP will respond with a *path reply message (PREP)* whenever a received PREQ corresponds to a newer or better path to the source. Intermediate MPs that have already a valid path to the requested destination, can respond with a PREP, if the *Destination Only* flag (DO flag) is not set. Depending on the new *Reply and Forward* flag

[1] The target size according to [5] is actually only 32 MPs, but this number is not a strict limit. Up to 50 MPs is a reasonable size for a WLAN mesh network

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

The proactive component of HWMP is the extension with a proactive routing tree to specially designated MPs. Any MP that is configured to be a root MP, will periodically broadcast *proactive PREQ messages* or *root announcement messages (RANNs)* into the wireless mesh network, which will create and maintain a tree of paths to the root MP. There are three different, configurable mechanisms for the proactive tree-building available in HWMP (cf. Section 4).

One of the design goals for a default path selection protocol is its applicability to a broad range of usage scenarios. The configurability of HWMP, those options are illustrated in Figure 2, supports this.

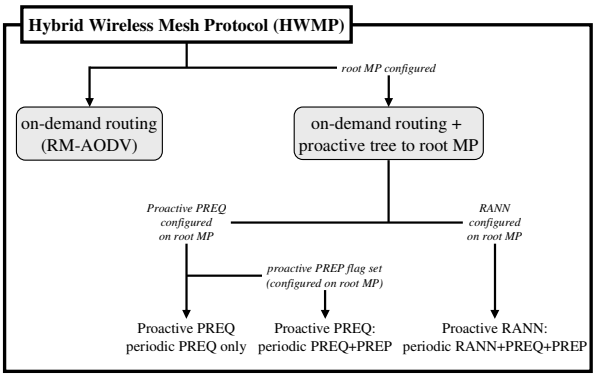

Figure 2: Configurability of HWMP

3. Interworking with HWMP

IEEE 802.11s WLAN mesh networks require connections to other wireless or wired networks. This is referred to as *interworking*.

HWMP runs only in the wireless mesh network. All other networks may have their own, different forwarding mechanism, which use different frame headers with a different number of addresses: The communication between IEEE 802.11 clients and access points uses 3 addresses, Ethernet uses only 2 addresses, and IEEE 802.11s mesh data frames use 4 addresses. However, all are MAC addresses following the same format, and there are devices that can translate between the different frame formats on MAC layer, for example, (mesh) access points and bridges.

An IEEE 802.11s WLAN mesh network can be connected by two kinds of devices to other networks at MAC level. Mesh APs connect conventional WLAN clients to the mesh network. Mesh portals connect the mesh network to other IEEE 802 based networks such as other IEEE 802.11s mesh networks or wired Ethernet segments.

IEEE 802.11s uses the 4-address frame format for data frames [5]. Two MAC addresses are source and destination. The other two MAC addresses are transmitter and receiver, the two MPs on both sides of the wireless link.

A WLAN mesh network might be connected to hundreds of clients and to thousands of devices located on a company Ethernet. All these devices can be source or destination of traffic going through a WLAN mesh network. In a wireless mesh network with layer 3 routing, the IP address indicates whether a node belongs to the mesh, since usually all mesh nodes and only mesh nodes belong to the same IP subnet. This is not possible with a routing protocol based on MAC addresses. They are usually assigned to devices statically by the vendor.

3.1. IEEE 802.11s data frame format

One solution is to integrate all non-mesh devices into the routing protocol and the mesh edge nodes perform an instance of the routing protocol on their behalf. However, such integration can lead to prohibitively huge routing tables, independent of the number of MPs.

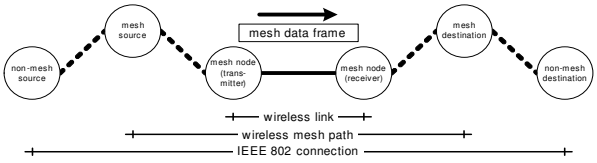

Figure 3: Different source/destination pairs

Another solution is to have only MPs being visible to the routing protocol. The source and destination address fields in a data frame will contain the MAC addresses of the MPs where the data frame enters or leaves the WLAN mesh network. The routing tables are now very small. For a non-mesh destination, however, the destination address field of the IEEE 802.11s data frame would contain the MAC address of the MP where the data frame will leave the mesh network towards the actual, non-mesh destination. The MAC address of the final destination would have been lost as the data frame entered the mesh network. Figure 3 illustrates the relationship between the different source-destination pairs.

IEEE 802.11s adopted a solution which introduces a fifth and sixth address to the data frame format (cf. Figure 4). These are the MAC addresses of the non-mesh destination and the non-mesh source respectively. They are only present if the data has a non-mesh source

and/or non-mesh destination. This is controlled by the *Address Extension* mode (AE mode). If only one of the IEEE 802 addresses is outside the mesh network, the other address 5/6 is the corresponding mesh source or mesh destination address [12].

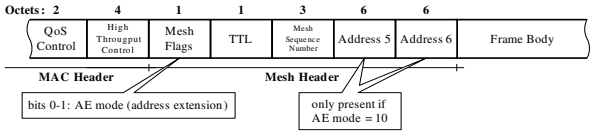

Figure 4: Mesh header of data frame

Mesh edge nodes are called proxy MPs [12], because they "proxy" data frames for non-mesh nodes. Mesh portals and mesh APs can be proxy MPs. The inclusion of MAPs supports a cleaner architecture for the interworking with IEEE 802.11s mesh networks.

The mesh sequence number has been extended to 24 bits in order to have a longer time until rollover.

3.2. Path discovery with non-mesh nodes

The principles illustrated in Figure 3 have to be reflected within HWMP [10]. The entries of the routing tables will be only for mesh points. The mesh source has to know to which mesh destination it has to send a data frame destined to a non-mesh destination. This is the corresponding proxy MP. This proxy information is stored in so-called proxy tables in the mesh edge nodes.

HWMP fills the proxy tables in a reactive manner, since not all proxy information is needed all the time. This allows combining the distribution of the proxy information with the path discovery of HWMP. Additionally, external sources such as association tables in mesh APs and bridge learning in mesh portals can provide proxy information.

A mesh edge node learns that it is proxying for a non-mesh source when it receives a data frame through its non-mesh interface. This proxy MP will be the mesh source. It may not have a path to the destination of the data frame; and it does not know whether the destination is part of the WLAN mesh network or beyond it. It is assumed that either the destination itself or its proxy MP responds to a corresponding PREQ.

Additionally, the proxy information about the non-mesh source has to be transmitted to the mesh destination, because the mesh destination has to know the proxy MP for the non-mesh source for the reverse path in bidirectional communications.

In order to achieve this, PREQ (Figure 5) and PREP (Figure 6) have been extended in a similar way as the IEEE 802.11s data frame. If a proxy MP is initiating a path discovery for a destination based on a data frame received from outside the mesh network, it sets the new *Address Extension* flag (AE flag) in the PREQ. This indicates that the PREQ contains two source addresses—the mesh source and the non-mesh source. This is the required proxy information.

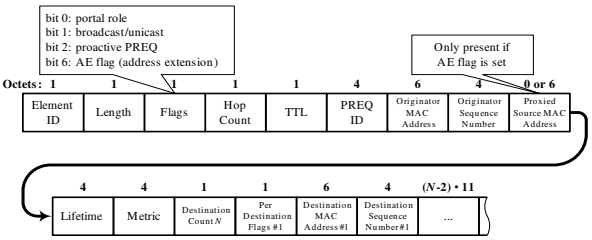

Figure 5: Path Request message (PREQ)

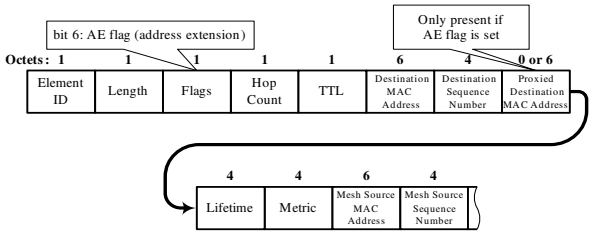

Figure 6: Path Reply message (PREP)

If the requested destination is outside the mesh, the proxy MP for this destination will respond with a PREP. This PREP does not only set up the forward path between both proxy MPs (mesh source and mesh destination), but it also provides the proxy information for the non-mesh destination to the mesh source. This is done by setting the new *Address Extension* flag (AE flag) in the PREP. This indicates that the PREP contains two destination addresses—the mesh destination and the non-mesh destination. This is the required proxy information.

4. Revised tree-based routing of HWMP

The proactive tree-building of HWMP to designated root MPs as described in [7] received a thorough revision [9][12]. There are now three different ways for proactive tree-building in HWMP (Sections 4.1 and 4.2). MPP announcement and root MP announcement have been separated (Section 4.3).

4.1. Proactive PREQ mechanism

The former non-registration mode [7] and parts of the former registration mode [7] are now realized with the *proactive PREQ mechanism* [9][12]. A proactive path request is a special PREQ message with the only

requested destination being the broadcast address (all 1's) and both DO flag and RF flag set.

If an MP is configured to be a root MP and to use the proactive PREQ mechanism, it will broadcast a proactive PREQ with increasing sequence number periodically. Any mesh point that receives a proactive PREQ will process it in a similar way it would process a PREQ during on-demand path discovery:

- The MP will create or update the path to the root MP in its routing table according to the update rules of the general PREQ processing.
- The MP will broadcast an updated PREQ (TTL, hopcount, path metric) to its neighbors if it refers to a better or newer path to the root MP. This propagates the proactive PREQ to all nodes in the wireless mesh network.

The generation of a PREP, however, follows special rules. The new *Proactive PREP* flag in the PREQ controls whether a PREP is sent in response to a proactive PREQ. The setting of the Proactive PREP flag is configured at the root MP. MPs that receive a proactive PREQ are not allowed to change its setting.

If the Proactive PREP flag is not set, no PREP is sent in response to the reception of a proactive PREQ. This corresponds to the former non-registration mode, where a tree of paths from all MPs to the announced root MP is set up but the MPs are not registered proactively at the root MP. If bidirectional communication is needed to the root MP, the source MP may send a gratuitous PREP before the first data frame in order to register its address with the root MP. The intention of the proactive PREQ mechanism with unset proactive PREP flag is a lightweight creation and maintenance of proactive paths to the root MP while the routing overhead is kept at a minimum.

If the Proactive PREP flag is set, the MP has to send a PREP in response to the reception of a proactive PREQ. This corresponds to the part of the former registration mode, where MPs register with the root MP by sending a route reply message in response to the root announcement message.

4.2. Proactive RANN mechanism

The proactive RANN mechanism is derived from the former registration mode [7].

Octets: 1	1	1	1	1	6	4	4
Element ID	Length	Flags	Hop Count	TTL	Root MP MAC Address	Root MP Sequence Number	Metric

Figure 7: Root MP Announcement (RANN)

If an MP is configured to be a root MP and to use the proactive RANN mechanism [9], it will broadcast a RANN (Figure 7) with increasing sequence number periodically. The sent RANNs are only used to disseminate metrics of paths to the root MP to all MPs of the mesh network, but they will not create or update any paths in the routing table. Any MP that receives a RANN will process it according to the special rules for RANN messages.

- If the MP has to create or to update a path to the root MP it will send a unicast PREQ with TTL=1 and set Destination Only flag, requesting a path to the root MP. This unicast PREQ is sent via the neighboring MP from which the MP received the RANN. The processing of the unicast PREQ and the response with a PREP follow the same processing rules as for the on-demand part of HWMP.
- The MP will broadcast an updated RANN (TTL, hopcount, path metric) to its neighbors after a given RANN propagation delay if it refers to a better or newer path to the root MP. Eventually, the information on the path metric to the root MP will be propagated to all nodes in the wireless mesh network.

4.3. Mesh portals and root MPs

MPP announcements and root MP announcements are now independent mechanisms [12]. Some usage scenarios benefit from proactively maintained routing trees to MPs that are not an MPP. On the other hand, it is useful to announce MPPs in a WLAN mesh network even if there will be no proactive routing tree to them.

Any MP, no matter whether an MPP or not, can be configured as a root MP. Multiple root MPs can be configured in a mesh network running HWMP. The proactive tree-building is done simultaneously by the different root MPs. The corresponding routing trees are uniquely identified by the MAC address of the root MP. A „super root MP“ does not need to be elected.

MPP announcements and announcements of root MPs are very similar. All the information of an MPP announcement is also contained in a proactive PREQ/ RANN for an MPP configured as root MP. Such an MPP can set the *Portal Role* flag in the proactive PREQ/ RANN and does not need to send MPP announcements to avoid flooding the same information twice into the wireless mesh network.

5. IEEE 802.11s extensibility framework

Research in mobile ad hoc networks has shown that there is no single path selection protocol that fits all possible usage scenarios for wireless mesh networks in an optimal way. On the other hand, interoperability is a major goal of a standard. In order to bring these two

requirements together, IEEE 802.11s defines an extensible path selection framework with default path selection protocol and default path selection metric [11].

This provides the flexibility to choose an optimal path selection protocol and to integrate future protocols and metrics. It allows implementing any path selection protocol with any path selection metric in an IEEE 802.11s WLAN mesh. However, only a single path selection protocol and only a single path selection metric will be active in a particular mesh network at a time.

The selected protocol and metric have to be compatible. The metric fields in the messages of the path selection protocol have to be able to carry all values of the metric. All other parameters (data type of metric field, operators for aggregation and comparison of metric values, initial value of path metric) can be derived from the active path selection metric.

A path selection protocol identifier and a path selection metric identifier are contained in the beacons of MPs. The identifiers announce the active path selection protocol and metric. An MP, that wants to join an existing IEEE 802.11s WLAN mesh network, has to be able to support the announced protocol and metric and has to select them as active protocol and active metric. Otherwise, the MP cannot join the mesh network.

The default path selection protocol (HWMP) and the default path selection metric (Airtime Link Metric [12]) provide interoperability of MPs. Every IEEE 802.11s compliant device is required to implement both the default protocol and the default metric. This ensures that every MP, no matter who the vendor is, can participate in a network that is configured to use HWMP and the Airtime Link Metric. The use of HWMP is encouraged by its broad applicability to many usage scenarios.

The description of HWMP has been revised in such a way, that HWMP can work with any path selection metric, as long as the values fit into the 4 bytes of the metric fields in the HWMP messages. Data type, operators, and initial value are described in a general way.

The MPP announcement has been taken out of HWMP. MPPs and their announcement are general concepts and have to be available to any active path selection protocol.

6. Outlook

The final approval of IEEE 802.11s is expected for 2009. TGs is making good progress with comment resolution and further improving the draft. HWMP has been getting more mature during this process.

The paper is based on draft version D1.06 [12]. More versions with further changes and improvements to HWMP can be expected as well as feedback from simulations and first implementations.

7. References

[1] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", *IETF Experimental RFC 3561*, Jul. 2003.

[2] T.H. Clausen and P. Jacquet, eds., "Optimized Link State Routing Protocol (OLSR)", *IETF Experimental RFC 3626*, Oct. 2003.

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

[4] Zhang, Y., J. Luo, and H. Hu, eds., *Wireless Mesh Networking: Architectures, Protocols and Standards*, Auerbach Publications, Boca Raton, 2007.

[5] D. Eastlake, "Modified 802.11 TGs PAR and 5C", *IEEE P802.11 Wireless LANs, Document 11-07/0149r5*, Jan. 2007.

[6] W.S. Conner, "IEEE 802.11 TGs Usage Models", *IEEE P802.11 Wireless LANs, Document IEEE 802.11-04/0662r16*, Jan. 2005.

[7] M. Bahr, "Proposed Routing for IEEE 802.11s WLAN Mesh Networks", *2nd Annual International Wireless Internet Conference (WICON)*, Boston, MA, USA., Aug. 2006.

[8] IEEE Std. 802.11™-2007, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *IEEE Computer Society*, Jun. 2007

[9] A. Joshi, et al., "HWMP Specification", *IEEE P802.11 Wireless LANs, document IEEE 802.11-06/1778r1*, Nov. 2006

[10] H. Gossain, et al., "Proxy Frame Forwarding", *IEEE P802.11 Wireless LANs, document IEEE 802.11-07/0337r1*, Mar. 2007

[11] M. Bahr, G. Strutt, and W.S. Conner, "Path selection metric framework", *IEEE P802.11 Wireless LANs, document IEEE 802.11-07/0239r1*, May 2007

[12] IEEE P802.11s™/D1.06, draft amendment to standard IEEE 802.11™: Mesh Networking. *IEEE*, May 2007, work in progress.

[13] J. Cardona, M. Bletsas, and J. Watlington, "Mesh Network Details – OLPCWiki", *http://wiki.laptop.org/go/Mesh_Network_Details*, May 22, 2007.