IEEE 802.11s wireless mesh networks: Framework and challenges

Xudong Wang a,*, Azman O. Lim b

a Kiyon, Inc., San Diego, CA 92121, United States
b National Institute of Information and Communication Technology, Kyoto, Japan

Received 5 June 2007; accepted 11 September 2007
Available online 22 October 2007

Abstract

Wireless mesh networking based on 802.11 wireless local area network (WLAN) has been actively explored for a few years. To improve the performance of WLAN mesh networks, a few new communication protocols have been developed in recent years. However, these solutions are usually proprietary and prevent WLAN mesh networks from interworking with each other. Thus, a standard becomes indispensable for WLAN mesh networks. To meet this need, an IEEE 802.11 task group, i.e., 802.11s, is specifying a standard for WLAN mesh networks. Although several standard drafts have been released by 802.11s, many issues still remain to be resolved. In order to understand what performance can be expected from the existing framework of 802.11s standard and what functionalities shall be added to 802.11s standard to improve performance, a detailed study on the existing 802.11s standard is given in this paper. The existing framework of 802.11s standard is first presented, followed by pointing out the challenging research issues that still exist in the current 802.11 standard. The purpose of this paper is to motivate other researchers to develop new scalable protocols for 802.11 wireless mesh networks.
© 2007 Elsevier B.V. All rights reserved.

Keywords: Wireless mesh networks; IEEE 802.11s standard; Protocol; Layer-2 routing

1. Introduction

In a traditional setup of 802.11 wireless LANs, basic service sets (BSSs) are connected via Ethernet LANs. Such a fixed network architecture limits the flexibility of network deployment and increases cost. Thus, the mobility of BSS and multihop networking are needed.

Starting from the first IEEE 802.11 standard, ad hoc networking has been specified in the independent basic service set (IBSS) mode. In this mode, stations (STAs) can connect to each other without any central coordinator like access point (AP). Moreover, there is no access or connection to the distributed system (DS). Thus, STAs are totally self-contained as an ad hoc network. Such an operation mode has been researched in the field of ad hoc networking. However, it has been realized for a long time, especially in industry, that the IBSS mode is not enough for many interesting application
scenarios where ad hoc networking is needed but Internet access and support of client nodes are also necessary. Thus, both infrastructure mode and IBSS mode shall be integrated in a new type of multihop networks.

To meet the above requirements, wireless mesh networking [1] is needed for 802.11 wireless networks. For years, many companies have developed their proprietary solutions to build 802.11 based wireless mesh networks (WMNs). Such solutions share the following common features:

- The network usually includes three types of nodes: mesh routers, clients, and gateways.
- An ad hoc routing protocol is implemented in mesh routers to work together with 802.11 MAC. Certain radio aware functions may be included in the routing protocol.
- 802.11 MAC driver is enhanced in mesh routers to improve multihop performance. Typical examples include fine-tuning CSMA/CA parameters, developing algorithms for multi-radio or directional antennas, etc.
- Certain network configurations are needed to support client access, Internet access, roaming, and so on.

In spite of the similarities, the proprietary solutions are usually not inter-operable. In order to resolve such an issue and meet the ever-increasing demands of 802.11 mesh networks, it is critical to develop a standard for 802.11 mesh networks.

Before the establishment of the IEEE 802.11s task group, many companies had formed a study group to push a standard for 802.11 WMNs. At the beginning, many proposals were submitted to resolve different issues involved in mesh networking. These proposals were finally consolidated and merged into one proposal in early 2006, which provides the basic framework for the current 802.11s standard draft. Since then the 802.11 task group has been working hard to resolve issues in the framework. Draft 1.0 of 802.11s standard released in November 2006 [2] went through a letter ballot, but it failed in this process because many issues still remain. Currently participants of 802.11s task group are working actively to resolve comments raised by 802.11 voters. Although a lot of progress has been made and a few new drafts have been released recently, there exist many issues that demand enhanced or even new solutions to 802.11s mesh networking. Otherwise, performance of 802.11s WMNs can be unsatisfactory. However, to the best of our knowledge, there is no sign that the 802.11s task group is taking the challenge of enhancing adopted solutions or developing new solutions for 802.11s mesh networking. Without putting efforts along this direction, it is quite possible that voters will continue to raise comments and fail the letter ballot. Consequently, the releasing date of an official 802.11s standard becomes unpredictable. More importantly, even if an official standard is released someday, its mediocre performance will prevent it from surviving in a competitive market with so many alternative mesh networking technologies.

In this article we give a detailed analysis of 802.11s framework. Firstly, the major functionalities of 802.11s WMNs are presented. We then point out the gap between these functionalities and those required by a scalable WMN. Our aim is to provide a better understanding of the following questions for the emerging 802.11s standard: what performance can be expected from 802.11s WMNs, what problems still exist in 802.11s WMNs, and what direction can be taken to improve 802.11s mesh networking. We hope our analysis will stimulate the development of scalable mesh networking protocols that can lead to expedited standardization of 802.11s WMNs with scalable network performance.

2. Network architecture of 802.11s WMNs

In order to understand the network architecture of 802.11s, we first need to explain 802.11 extended service set (ESS) and its difference from IBSS.

An 802.11 ESS consists of multiple BSSs connected through a DS and integrated with wired LANs [3]. The DS service (DSS) is provided by the DS for transporting MAC service data units (MSDUs) between APs, between APs and portals, and between stations within the same BSS that choose to involve DSS. The portal is a logical point for letting MSDUs from a non-802.11 LAN to enter the DS. The ESS appears as single BSS to the logical link control layer at any station associated with one of the BSSs. The 802.11 standard has pointed out the difference between IBSS and ESS. IBSS actually has one BSS and does not contain a portal or an integrated wired LANs since no physical DS is available. Thus, an IBSS cannot meet the needs of client support or Internet access, while the ESS architecture can. However, IBSS has its advantage of self-configuration and ad hoc networking. Thus, it is a good strategy to develop schemes to combine
the advantages of ESS and IBSS. The solution being specified by IEEE 802.11s is one of such schemes. In 802.11s, a meshed wireless LAN is formed via ESS mesh networking. In other words, BSSs in the DS do not need to be connected by wired LANs. Instead, they are connected via wireless mesh networking possibly with multiple hops in between. Portals are still needed to interconnect 802.11 wireless LANs and wired LANs. Based on such a concept, the network architecture of 802.11s is illustrated in Fig. 1. There are three new nodes in this architecture. A mesh point (MP) is an 802.11 entity that can support wireless LAN mesh services. A mesh access point (MAP) is an MP but can also work as an access point. A mesh portal (MPP) is a logical point where MSDUs enter/exit the mesh network from/to other networks such as a traditional 802.11 LAN or a non-802.11 network. An MPP includes the functionality of MP and can be co-located with an 802.11 portal.

Because MPs do not have AP functionality but can work as relaying nodes, the meshed wireless LAN is not an ESS anymore. Thus, in a recent 802.11 standard meeting, suggestion of changing the project authorization request (PAR) of 802.11s was made so that the title of 802.11s will be just “Mesh Networking” rather than “ESS Mesh Networking”.

The protocol stacks of these three types of nodes are illustrated in Fig. 2. The 802.11s MAC is developed based on existing 802.11 MAC, and the mesh routing protocol resides in the MAC layer. In an MPP, a layer-3 routing protocol is also needed for path selection from the mesh network to external network or vice versa.

3. Framework of 802.11s WMNs

The upcoming 802.11s standard includes the following critical components:

- **Topology formation and discovery:** This includes the specifications of how a mesh network is created and how other mesh nodes\(^1\) join or leave the network. Both single-channel or multi-channel operations shall be supported.
- **Routing in the MAC layer:** Since the routing protocol is specified in the MAC layer, MAC address routing is needed and shall be radio aware. In addition, support of legacy nodes needs to be specified in the routing framework.
- **MAC:** Many functionalities need to be specified for the MAC protocol, including MAC enhancement, MAC layer congestion control, power management, multi-channel operation, synchronization, and so on.

\(^1\) A mesh node can be either an MP or a MAP.
• **Interworking:** Mechanisms for interconnecting the mesh network with other wired or wireless networks shall be specified.
• **Security:** Secure links shall be maintained among mesh nodes as well as between mesh nodes and legacy nodes.

To support these new functionalities, the frame format must be extended for mesh operation. This includes adding new information elements to the existing frames and also defining new frames.

### 3.1. Topology formation and discovery

1. **Discovery and formation of mesh networks:**
   When a new mesh node powers up, it may use passive or active scanning to discover a mesh network. In 802.11s, a new ID, called mesh ID, is used to identify a mesh network. The mesh ID is attached in beacon and probe response frames as a new information element for passive and active scanning, respectively.

   The function of mesh ID is similar to SSID, but SSID cannot be used for identifying a mesh network. One of the reasons is that the mesh ID can prevent STAs from being associated with MPs without AP functionality. For the same reason, for a non-AP MP the beacon should not include a valid SSID or a wildcard value is used for SSID information element in the beacon.

   Before a new mesh node associated with a mesh network identified by a mesh ID, it needs to check if its mesh profile matches the established mesh network. In 802.11s, each mesh device must support at least one mesh profile consisting of a mesh ID, a path selection protocol identifier, and a path selection metric identifier. If such mesh capability information in a mesh node matches that of an established mesh network, it will start association. Security procedures is also involved in this association process. If a new mesh node cannot find an established mesh network, it needs to create a mesh network.

---

**Fig. 2.** Protocol stack of 802.11s.
2. Mesh peer link establishment: Once a mesh node has joined a mesh network, it needs to establish peer links with its neighbors before it can start send packets. In 802.11s, state machines and detailed procedures have been specified for setting up peer links. Once this step is completed, it is also necessary to establish a measure of link quality for each peer link. This requires a link quality measurement scheme and a procedure of propagating such information among neighbors. When it is necessary, a procedure to ensure symmetrical link quality information is needed. It should be noted that the link quality information of each peer link is also used as one of the routing metrics for the routing protocol.

3. Multi-channel topology formation: In the single-channel mode, a mesh node selects one channel during the discovery process. In the multi-channel case, a mesh node with multiple radios needs to select a different channel for each radio, while a mesh node with single-radio has to switch channels.

In order to manage the topology in a multi-channel mesh network, a unified channel graph (UCG) concept is adopted. In the same UCG, all mesh devices\(^2\) are interconnected using one common channel. As a result, in a single-channel mesh network, the entire network has only one UCG. For a multi-channel WMN, it may consist of multiple UCGs depending on network self-organization. To coordinate different UCGs, a channel precedence value is attached in mesh channel switch announcement element for coalescing or switching channels in UCGs. In the same UCG, the channel precedence value is the same for all mesh devices, but it must be different in different UCGs.

A simple channel unification protocol and a simple channel graph switching protocol are specified in the current 802.11s standard draft. However, such mechanisms are only applicable to simple scenarios where only slow channel switching is demanded. If dynamic and fast channel switching is needed, the UCG concept and its supporting procedures in the current 802.11s draft is insufficient.

3.2. Routing in the MAC layer

It is a widely accepted concept that it is beneficial to have layer-2 routing for WMNs. However, IEEE 802.11s is probably the first standard that actually specifies routing in the MAC layer. Among many other reasons, interoperability is the most obvious motivation to do so. Previously many proprietary 802.11 mesh networks are built using different routing protocols, which result in difficulty of interoperation.

In 802.11s, the framework for routing is extensible. More specifically, different routing protocols can be supported by following the same framework, but the mandatory protocol shall be implemented for interoperability.

The routing mechanism in 802.11s handles packet forwarding for MPs, MAPs, and associated STAs. Unicast, multicast, and broadcast frames are all supported in the same framework. Since routing is performed in the MAC layer, packet forwarding is carried out via MAC addresses, which requires the MAC header contains at least four MAC addresses. Compared to a conventional MAC protocol, two additional MAC addresses are required for the MAC addresses of the source and the destination of an end-to-end traffic flow.

In a routing protocol, nodes usually need to exchange routing messages for the purpose of finding link status, collecting neighbor information, requesting routing path, and so on. Thus, many control messages are involved. In 802.11s, such messages are sent in various mesh action frames as information elements.

Before draft 1.06 of 802.11s, one mandatory routing protocol and one optional routing protocol have been specified. The mandatory routing protocol is called hybrid wireless mesh protocol (HWMP), which is a hybrid routing protocol of on-demand routing and proactive tree-based routing. The optional routing protocol is based on link state routing and is called radio aware optimized link state routing (RA-OLSR). Starting from draft 1.07, the optional routing protocol is removed from 802.11s.

1. **HWMP**: The network infrastructure of 802.11 WMNs tends to have minimal mobility and most of the traffic is to/from the Internet. However, some nodes such as handset devices, laptops, etc. can be an MP but definitely need mobility support. In order to meet diverse requirements
by making the routing protocol be efficient for different scenarios, HWMP is being specified in 802.11s. In HWMP, on-demand routing protocol is adopted for mesh nodes that experience a changing environment, while proactive tree-based routing protocol is an efficient choice for mesh nodes in a fixed network topology. In this routing protocol, the mandatory routing metric is airtime cost that measures the quality of links. The extensible framework supports other types of metrics such as QoS parameters, traffic load, power consumption, and so on. However, in the same mesh only one metric shall be used.

The on-demand routing protocol is specified based on radio-metric ad hoc on-demand distance vector (AODV) routing. The basic features of AODV [5] are adopted, but extensions are made for 802.11s. The proactive tree-based routing is applied when a root node is configured in the mesh network. With this root, a distance vector tree can be built and maintained for other nodes, which can avoid unnecessary routing overhead for routing path discovery and recovery. It should be noted that the on-demand routing and tree-based routing can run simultaneously.

Four information elements are specified for HWMP: root announcement (RANN), path request (PREQ), path reply (PREP), and path error (PERR). Except for PERR, all other information elements of HWMP contain three important fields: destination sequence number (DSN), time-to-live (TTL), and metric. DSN and TTL can prevent the counting to infinity problem, and the metric field helps to find a better routing path than just using hop count.

In the on-demand routing mode, an PREQ is broadcast by a source MP with an aim to set up a path to a destination MP. When an intermediate MP receives this element, it creates/updates a path to the source if the sequence number of the PREQ is greater than the previous one or the sequence number is the same but the metric is better. If the intermediate MP has no path to the destination MP, it just forwards the PREQ element further. Otherwise, there are different cases depending on two flags, i.e., destination-only (DO) flag and reply-and-forward (RF) flag:

1. **The DO flag is set to 1.** This is a default case. The intermediate MP does nothing but just forwards the PREQ to the next-hop MP until the destination MP. Once the destination MP gets this element, it sends a unicast PREP back to the source MP. All intermediate MPs create a route to the destination MP when receiving this PREP element. Thus, in this case the routing protocol just ignores the existing route from the intermediate MP to the destination MP and creates a new one. The RF flag has no effect on the routing protocol in this case.

2. **Both flags are set to 0.** In this case the intermediate MP sends a unicast PREP to the source MP and does not forward PREQ. Thus, the routing protocol uses the existing route from the intermediate MP to the destination MP.

3. **The DO flag is set 0 but the RF flag is set to 1.** In this case the intermediate MP sends a unicast PREP to the source MP; additionally, it needs to change the DO flag to 1 and then forwards the PREQ element to the destination MP. By doing so, all the subsequent intermediate MPs will not send PREP elements to the source MP.

In maintenance PREQ, the DO flag is always set to 1, i.e., the first case must be used. It should be noted that the third case exists only when the source MP has no valid route and also wants to create a new route to the destination MP. The difference between the second case and the third one is that the third case cannot only quickly set up a routing path via an intermediate MP but can also create a new path from the intermediate MP to the destination MP.

As we can see, the above procedures are different from the original AODV protocol and are designed specifically for HWMP.

In the proactive tree-based routing mode, there are two mechanisms. One is based on proactive PREQ and the other is based on proactive RANN. In the proactive PREQ mechanism, the root node\(^3\) periodically broadcasts an PREQ element. An MP in the network receiving the PREQ creates/updates the path to the root, records the metric and hop count to the root, updates the PREQ with such information, and then forwards PREQ. Thus, the presence of the root and the distance vector to the root can be disseminated to all MPs in the mesh. If the proactive PREP bit in the proactive PREQ element is set to 1,

---

\(^3\) The root node can be an MP, MAP, or MPP for proactive RANN, and can be either an MP or a MAP for proactive PREQ.
then the receiving MP sends a gratuitous PREP to the root so that a route from the root to this MP is established. On the other hand, if the proactive PREP bit is set to 0, the gratuitous PREP is sent only when there is data to send between the MP and the root with a bidirectional route. In the proactive RANN mechanism, the root node periodically flood an RANN element into the network. When an MP receives the RANN and also needs to create/refresh a route to the root, it sends a unicast PREQ to the root. When the root receives this unicast PREQ, it replies with a PREP to the MP. Thus, the unicast PREQ forms the reverse route from the root to the originating MP, while the unicast PREP creates the forward route from the originating MP to the root.

2. RA-OLSR: RA-OLSR is a proactive link state routing protocol that is developed based on OLSR [4]. However, in order to reduce flooding overhead, several extensions are made. Firstly, only a subset of one-hop neighbors of an MP is selected to relay control messages. Such neighbor MPs are called multipoint relays (MPRs). The MPRs are selected such that control messages relayed by them can reach all two-hop neighbors of the selecting MP. The MPR selection is performed through periodic HELLO messages between MPs. In addition, the message exchange frequency can be controlled based on fisheye scopes as defined in fisheye state routing protocol [6]. Secondly, to provide shortest routes, RA-OLSR requires only partial link state information to be flooded. The minimum set of links consists of those between the MPRs and their selectors.

Since RA-OLSR continuously maintains routes to all destinations in the network, it is specially beneficial when source-destination pairs are very dynamic or the mesh network is large and dense. RA-OLSR is a distributed protocol, without a requirement of reliable delivery of control messages. It can also support both single-interface or multiple-interface MPs.

The mechanisms for supporting non-mesh STAs are specified for RA-OLSR. However, the overhead of these mechanisms are still extremely high, in particular when the number of STAs is large.

3. Support of legacy nodes: For packets transmitted between legacy nodes via a WMN, the routing protocol inside the mesh needs the source MAC and the destination MAC addresses of a legacy node. Based on such MAC addresses, a MAC can find the right legacy node for each packet. Thus, two additional MAC addresses are added into the MAC header, as specified in the 6-address mechanism in 802.11s. However, each MAP needs to store the MAC addresses of all legacy nodes including those associated with other MAPs. In this way, a MAP can correctly find out what is the MAC address of the given destination legacy nodes. In HWMP of 802.11s, the MAC addresses of legacy nodes can be sent in proxied MAC address fields of PREQ, PREP, and proxy update (PU) information elements.

3.3. MAC

The basic operation mechanism of 802.11s MAC is the enhanced distributed channel access (EDCA) specified in 802.11e. Other features of 802.11e such as hybrid coordination function controlled channel access (HCCA) are not considered in 802.11s. In this sense, the QoS of 802.11s in its current form is still far from enough for many multimedia services. Moreover, EDCA does not work well for mesh networks, since its prioritization mechanism does not perform well in a multihop mesh environment. Nevertheless, the current 802.11s MAC protocol is built on top of EDCA with various enhancements.

1. Beaconing and synchronization: Beaconing procedures for unsynchronizing and synchronizing MPs are defined in 802.11s. A mechanism to avoid beacon collisions is also specified in the mesh beacon collision avoidance (MBCA) mechanism. Also, an MP can be designated as a beacon broadcaster for a defined period of time while all other MPs defer their transmission of beacons.

Based on beacon or probe response frames, synchronization is performed for MPs. In 802.11s, the synchronization is similar to the timing synchronization function (TSF) of the original 802.11 standard [7]. The differences are two folds. One is that the MPs are not all synchronized and their beacon intervals are not necessarily the same. The other is that not only a TSF timer but also an offset is needed for synchronization. Whether or not an MP supports synchronization is identified by synchronization capability field of the WLAN mesh capability information element.
When an MP does not need synchronization, it maintains its own TSF timer and does not update it when receiving beacons or probe responses. However, for a synchronizing MP, it needs to maintain a mesh TSF time that is common to all synchronizing MPs. The mesh TSF time is equal to the sum of the TSF timer and the offset on the synchronizing MP. Because of using the offset, the TSF timers of synchronized MPs can be different. On the other hand, when receiving beacons or probe responses that contain the sender’s TSF timer and the offset, an MP follows a synchronization procedure similar to that for IBSS mode of 802.11 networks. More specifically, the MP performs the following calculation:

\[
\text{Calculated time stamp} = \frac{\text{received TSF value} + \text{received offset}}{C_0} - \text{the MP's own offset}.
\]

If the calculated time stamp is later (or faster) than the MP’s local TSF value, then the TSF timer is updated with this calculated time stamp. Otherwise, this step is ignored. Optionally, the MP can update its own offset rather than the TSF timer as follows. If the sum of the received TSF value and the received offset is larger than the sum of the MP’s TSF value and self offset, then the self offset is updated as follows:

\[
\text{The MP's new offset} = \frac{\text{received TSF value} + \text{received offset}}{\text{the MP's TSF value}} - \text{the MP's own offset}.
\]

Otherwise, no updating is needed.

It should be noted that updating TSF timer and updating offset cannot be used at the same time.

2. **Multi-channel operation**: Multi-channel operation is so important to WMNs. However, no mechanism has been specified in 802.11s. In the beginning, a proposal called common channel framework (CCF) was adopted into earlier versions of the draft (before draft 1.0). However, because of many problems that were not resolved effectively, the proposal was removed from the draft. Nevertheless, we still introduce the mechanism of CCF here.

In CCF, mesh nodes that want to use multi-channel operation need to negotiate its channel in a common channel. Thus, the common channel is known to all mesh nodes in the mesh network. A transmitter first sends an *request to switch (RTX)* message to request a channel. The receiver sends back a *clear to switch (CTX)* to confirm the requested channel. If RTX–CTX is successful, then a channel is selected for these two mesh nodes. Thus, both mesh nodes switch to the selected channel and exchange data following the data/acknowledgment procedure. Once this step is done, both mesh nodes switch back to the common channel. Such a mechanism is applied to all mesh nodes that can support CCF. In the common channel, in addition to RTX–CTX messages, packets for nodes that do not support CCF can be sent. The major problems of CCF are discussed in Section 4.

3. **Mesh deterministic access**: The mesh deterministic access (MDA) mechanism allows MPs to access a certain period with lower contention than other periods without using MDA. Such a period is called MDA opportunity (MDAOP). Before using MDAOP to access the medium, the owner of this MDAOP, i.e., the transmitter needs to set up the MDAOP with its receiver.

In a multihop network, the interference between nodes that are more than one hop away should be considered. Thus, in the MDA mechanism, two types of time periods are defined. The neighborhood MDAOP times of an MP are the transmitting/receiving (RX/TX) times during which the MP and its neighbors are either a transmitter or receiver of these MDAOPs. The neighborhood MDAOP times during which the MP is not a transmitter or receiver are called neighbor MDAOP interfering times. No MDAOP can be set up with this MP during such interfering times; otherwise, the MDAOP for this MP will experience interference.

When a transmitter wants to set up a new MDAOP to an intended receiver, it needs to check its neighborhood MDAOP times, the TX–RX times of its frames, and the neighbor MDAOP interfering times for the intended receiver. If no overlapping occurs and the MDA limit is not reached, then the transmitter sends an MDAOP setup request to the receiver. The receiver will do the same check. If the check is passed, the receiver accepts the MDAOP; otherwise, it rejects. Once the MDAOP is setup, both the transmitter and the receiver will start to advertise their new MDAOP time in the MDAOP advertisement information element. Both the transmitter and the receiver can initiate the teardown
process to release the MDAOP time period. The teardown is complete once the initiator is acknowledged by the receiver.

During an MDAOP period, the transmitter and the receiver follow a different procedure. If this period is accessed by the transmitter, i.e., the owner of MDAOP, it attempts to use CSMA/CA but new backoff parameters (e.g. MAD maximum contention window \( MDACW_{\text{max}} \), MDA minimum contention window \( MDACW_{\text{min}} \), and MDA arbitration interframe space number \( MDAI_{\text{FSN}} \)) to set up a TXOP. However, for a non-owner of the TXOP, it has to defer its access by setting its network allocation vector (NAV) to the end of the MDOAP or using a carrier sensing scheme.

4. Intra-mesh congestion control: An 802.11 mesh usually involves multiple hops. The transmission of one hop may impact its previous hop, the next hops, or any links in the neighbors. One problem from such an interaction is that links may be congested, and thus a node with congested links may receive more packets than that can be sent out. The transport layer protocol such as TCP can help mitigate this problem, but research has shown that it is not effective enough in a wireless multihop network. On the other hand, contention resolution can also help reduce congestion. However, in a WMN the contention level experienced by different nodes varies, which makes a contention resolution protocol ineffective. To resolve congestion in the MAC layer, an intra-mesh congestion mechanism is specified in 802.11s.

The intra-mesh congestion control is a hop-by-hop scheme. Nodes in the neighbor need to exchange congestion information and control message in order to resolve congestion in the network. Thus, the scheme consists of three modules: local congestion monitoring, congestion control signaling, and local rate control.

In the current draft of 802.11s, some local congestion monitoring schemes are suggested. For example, congestion can be monitored by comparing the transmitting rate and the receiving rate of packets that need to be forwarded. Queue size can also be used to monitor congestion. Once congestion is detected, the congested node will inform its previous hop nodes by sending a unicast congestion control request message in the mesh action frame. The node that receives this message shall adjust its transmission rate according to the local rate control algorithm. The congested node also send a broadcast message neighborhood congestion announcement to all its neighbors so that neighbors also regulate their transmission rate.

Congestion control signaling can be triggered periodically or non-periodically. In either case, in order to carry out local rate control, the target rate must be computed by the congested node and sent to the upstream node. The target rate is computed for each traffic category as defined in 802.11e rather than one link. Such information is attached as an information element in the congestion control request message. When the upstream node receives the congestion control message, it controls its transmission rate according to the target rate to the congested node. The upstream node shall also send a congestion control response message to tell the congested node about its offer traffic load. The local rate control at node when receiving the neighborhood congestion announcement has not been discussed in 802.11s.

Although congestion control can help improve the mesh network performance, unfortunately the critical part of this mechanism such as target rate computation and local rate control have not been clearly specified yet; only simple conceptual discussions are available in the draft of 802.11s.

5. Power management: Many nodes in 802.11s mesh networks always work in an active state since they either need to be an AP or forward traffic for other nodes. However, there are still other nodes that need to work in power save mode. Typically these nodes are the lightweight MPs or MPs that do not forward traffic for other nodes. Of course, STAs associated with a MAP may also work in power save mode, but the mechanism for these nodes is the same as that in the original 802.11 standards and is thus out of scope of 802.11s standard.

For a lightweight MP, it needs to check if its neighbors can also be in power save mode. If the answer is negative, it may choose to enter power save mode or communicate with neighbors without entering power save mode. In the former case, the MP may not be able to communicate with nodes that do not support power save mode. Thus, whether or not a lightweight MP goes into power save mode is determined by considering the tradeoff between power and communication constraints. In some cases, a lightweight MP
can just operate as a STA, so its power management is carried out through an AP. However, mostly the power management can be done via an announcement traffic indication message (ATIM) based mechanism.

In the ATIM-window based power management scheme, an MP works in two states: doze or wake state. The MP in power save mode needs to wake up during the ATIM window to receive or send control messages including beacons. The ATIM window repeats every one delivery traffic indication message (DTIM) interval. DTIM is usually equal to multiple beacon intervals. An MP may also wake up in a scheduled time period negotiated with other MPs. In the power save mode, packets in an MP need to be buffered and wait for being sent during the wake state.

To initiate the power management in a mesh network, the following procedure shall be used:

- An unsynchronizing MP shall set the values of DTIM, ATIM window, beacon interval, and power management mode. Such information is sent in beacon frames.
- When a synchronizing MP creates a mesh or when it joins a mesh where all neighbors are unsynchronized MPs, the same operation as the previous item is needed.
- When a synchronizing MP joins a mesh where there are synchronizing neighbor MPs, it needs to set the beacon interval and power management mode and update its ATIM window and DTIM interval according to the values in the received beacons of synchronizing MPs.
- The ATIM window shall start from the target beacon transmission time (TBTT) within each beacon interval.

It should be noted that an MP that has established peer links with other MPs cannot transition to power save mode unless 1. It can support power save mode and 2. All its neighbor MPs can send packets to MPs working in power save mode. Moreover, the MPs in power save mode shall be coordinated with the neighbor discovery mechanism and the route discovery mechanism. Otherwise, these MPs can experience low performance and degrade the performance of the entire mesh network.

3.4. Interworking

The interworking between mesh networks and other LAN segments is carried out through the bridging function in MPPs in a manner compatible with IEEE 802.1D.

In order to inform MPs of its presence, an MPP needs to send an MPP announcement. The MPP announcement protocol works as follows. An MPP sends an announcement information element in management frames. When an MP gets a management frame with a valid MPP announcement element, it checks the destination sequence number in the MPP announcement element. If it is smaller than that of a previous MPP announcement element, the current MPP element shall be discarded. Otherwise, it needs to forward the MPP announcement element to other MPs after the portal propagation delay has expired and also the TTL value is still greater than zero. In addition, it needs to record the MAC address and routing metric to this MPP.

When an MP has packets to send, it first follows the data forwarding procedure as defined in the routing protocol. If an intra-mesh route to the destination MAC address cannot be found, then the MP shall forward all packets to the all active MPPs in the mesh.

At an MPP, both egress and ingress messages need to be handled. An egress message is generated by an MP inside the mesh. If the MPP knows the destination node is inside the mesh, it will forward the message to the destination node. If the destination is outside mesh, it will forward the message to the external network. However, if the destination node is unknown to the MPP, the MPP shall forward the message to both the external network and the mesh network. An ingress message is a packet received by MPP from the external network. If the destination node inside mesh is known to the MPP, the message is simply forwarded by the MPP. Otherwise, the MPP can have two options: establish a route to the destination or broadcast the message within the mesh network.

Node mobility is also considered in 802.11s. There are four scenarios of node mobility. If a node moves within the mesh, then the routing protocol will take care of the mobility. If a node moves from the LAN outside the mesh to another LAN outside the mesh, no special action is needed for the mesh network, because 802.1D bridging functionality will handle this scenario [8]. In the third scenario where a node moves from inside the mesh to outside the mesh, the routing protocol needs to repair routing path after
detecting the route is changed. When a node moves from outside the mesh to inside the mesh, the MPP and the routing protocol cooperate to build a new routing path for the node.

MPP plays a critical role in interworking. From above procedures, we know it needs to support 802.1D bridging functionality. Moreover, MPP also needs to support virtual LAN (VLAN) functionality. In other words, the VLAN tag information defined in IEEE 802.1Q must be carried between MPs and MPPs. 802.1Q defines two header formats: Ethernet-encoded formats and SNAP-encoded header [9]. If the former is considered, a change to the 802.11 MAC header is needed in order to add the VLAN tag information. The latter one does not need such a change.

3.5. Security

The security specification in the current 802.11s standard draft is dedicated to secure links between MPs. The security in routing or forwarding functionality in a mesh network is not specified.

To provide secure links, mesh security association (MSA) services are specified in 802.11s. MSA inherits lots of work from 802.11i [10] and also adopts 802.1X [11] for initial authentication. MSA services extend the robust security network association (RSNA) framework of 802.11i to fit the mesh networking environment.

There are two types of MSA key holders in the network: mesh authenticator (MA) and mesh key distributor (MKD). A role negotiation protocol is available in 802.11s to determine if an MP shall be an MA, both an MA and an MKD, or neither. An MP without MA or MKD functionality shall work as a supplicant MP. Once this step is successful, both the MA and the supplicant MP open their controlled ports so that data traffic are allowed to exchange using the selected ciphersuites.

4. Challenging issues in 802.11s WMNs

Many issues still exist in the current 802.11s standard draft. Instead of discussing meticulous problems/errors, here we point out major ones that can dramatically degrade the performance of 802.11 WMNs.

4.1. Topology formation for multi-rate operation and physical rate control

In order to support routing, MAC and other functionalities, the network topology needs to be maintained. 802.11s has specified such a framework in which the peer-link setup takes into account the link quality measurement. However, such kind of mechanism is not flexible for a mesh network with multi-rate operation. As of today most physical layer technologies for wireless networks including 802.11 support multiple rates depending on the selection of different modulation and coding schemes. For such kind of multi-rate network, the topology is very sensitive to the transmission rate that is being used. For example, if a high rate is used, the communication range (and usually the interference range) is reduced too. Normally the physical rate on a node is controlled automatically by a rate control per packet. Mostly the control/signalng messages are sent using the lowest transmission rate to improve reliability. Thus, topology
being built up based on such messages is not consistent with the network topology that is seen by other packets. Such inconsistency will cause problems to any topology related protocols such as routing and MAC.

Since change of rate results in different communication range and interference range, it may be also beneficial to consider tradeoff between number of hops and the physical rate. For example, in order to connect two nodes, we can use one-hop communication with a very low transmission rate. We can also use multihop communications with a very high transmission rate. The end-to-end throughput for these two cases may be different, and so is the interference to other nodes. Unfortunately, the framework of topology formation in 802.11s is not flexible to support optimization between the rate and the number of hops.

4.2. Link quality measurement and routing metrics

Link quality is an important parameter for multiple modules of 802.11s, including the routing protocol. In 802.11s, the link quality measurement is based on the transmission rate and transmission error rate. However, such a scheme lacks three important mechanisms. Firstly, what packets can be sent and how to send them are not specified. Without a careful design, the link quality measurement can be inaccurate. For example, the frequency of measurement packets and their transmission rate impact the result of airtime cost. Secondly, the packet error rate due to transmission error does not actually reflect the link quality. For example, the packet error rate can be due to collisions, which is totally dynamic depending on the traffic activities and the behavior of routing and MAC protocols. Thus, the airtime cost varies a lot from time to time, which cannot provide a good metric for link quality. Routing based on such a metric may have a stability issue. Consequently, a more reliable and stable metric for link quality measurement and routing protocol is still desired.

4.3. Routing protocol

As a routing protocol, both HWMP and RA-OLSR have several shortcomings. First of all, the scalability of both routing protocols is limited. In HWMP, the proactive tree-based routing is totally centralized and constrained by the root node. Even if there is a short path between two MPs, the proactive routing mode still routes the packets via the root node, which results in a bottleneck at the root node and wastes precious wireless resources due to non-optimized routing path. Meanwhile, the on-demand routing mode still initiates a path discovery process to look for an optimized routing path before the packets are sent out, which results in a broadcast storm problem and wastes power resources on other MPs. Thus, the hybrid routing protocol in 802.11s still cannot support route optimization between two MPs. For RA-OLSR, the overhead of control messages is too high although fisheye scope mechanism is adopted.

Secondly, for both HWMP and RA-OLSR, although they are being specified as a routing module in the MAC layer, their interactions with other MAC functionality, especially the medium access mechanism, are not considered. Thus, such a strategy actually lose one important advantage of layer-2 routing, i.e., MAC-routing cross-layer design. Radio-metric routing in HWMP or radio aware routing in RA-OLSR has considered a simple interaction between routing and MAC/PHY layer. However, such interaction is far from enough. For example, for both mechanisms, how to use the routing metric based on airtime cost to find a better routing path is not specified. However, such a scheme critically determines the performance of the routing protocol. In another example, if intra-mesh congestion control is used, the routing protocol shall cooperate with the congestion control algorithm by a mechanism of considering the target rate; otherwise, the effectiveness of congestion control can be compromised. When multi-channel operation comes into picture, the cross-layer design becomes much more necessary.

Thirdly, supporting legacy nodes is still an ongoing effort for MAPs. Since legacy nodes do not participate in the HWMP routing protocol, the legacy nodes have to be associated with MAPs in order to gain access to the Internet through the backbone of the WMN. In 802.11s, the mechanism of locating a destination MAP for a given destination legacy node is not specified. In the Internet, the destination legacy node is identified by its destination IP address. Even though the MAP of the source legacy node has collected MAC addresses of all legacy nodes, it needs to find out which MAC address is mapped to the given IP address. Such mapping is usually done by an address resolution protocol (ARP). However, no mechanism is specified in 802.11s to perform ARP in a multihop network.
Furthermore, in case the legacy nodes move away from the communication range of the MAP to which it is associated, it should be disassociated from the MAP and re-associated from the new MAP in range. In order to support the dynamic movement of legacy nodes, a handover function needs to be specified in the current default routing protocol. On the other hand, a basic functionality of associating the legacy nodes is specified in the RA-OLSR routing protocol. However, the procedures in RA-OLSR can result in a very high percentage of overhead, which also limits the scalability of the routing protocol. Additionally, the current RA-OLSR has not considered the scenario when the legacy nodes are roaming between MAPs.

Lastly, in the current framework, although multiple routing metrics can be supported, only one metric is supported in the same mesh. However, in many application scenarios, different traffic types may need different routing metrics. Thus, multiple metrics need to be integrated into the same mesh in order to achieve optimized performance. Obviously, the current framework is not extensible to support such a feature.

For RA-OLSR, it has one more shortcoming: no portal mechanism is specified. Thus, if RA-OLSR is selected as a routing protocol, 802.11s WMNs cannot interwork with an outside network.

4.4. Multi-channel operation

In 802.11s, for multiradio MPs, only a simple UCG mechanism is used to unify the network using different channels. So far there is no MAC mechanism defined for multi-channel operation for single-channel radios. The original proposal of CCF has several obvious problems. CCF needs packet-level channel switching. However, since the duration of channel switching is larger than the time of sending a regular packet, the channel switching cause a huge percent of overhead. Moreover, the RTX–CTX mechanism in the common channel has no way to avoid possible collisions from non-CCF nodes in a new channel that the CCF node wants to switch to. Thus, when CCF node switches to the new channel, its performance is not guaranteed, and may cause some co-existence issues. Since RTX–CTX messages are always sent in the common channel that is shared by other non-CCF nodes, such messages can be congested and result in a slow process of getting a new channel. Moreover, CCF lacks a scheme to determine channel selection.

In fact the above problems can happen to any multi-channel MAC protocol if it is not carefully designed. To the best of our knowledge, the scheme of multi-channel TDMA MAC overlaying CSMA/CA [12] is the only multi-channel MAC protocol that has avoided these problems.

4.5. Congestion control

Several problems exist in the intra-mesh congestion control mechanism of 802.11s. Firstly, it does not have an effective mechanism for congestion monitoring. Congestion based on queue size may not work since the queue size is also impacted by higher layer protocol such as TCP. Whenever congestion happens, the congestion monitoring scheme may need to take some time to get a reliable measurement. For example, the time window shall be large enough in order to avoid false alarm. Such a time window may already cause TCP to take action and have adjusted the traffic rate. No matter what performance TCP congestion control can be, the status of congestion may have changed, and thus congestion may not accurately captured at the MAC layer.

In target rate computation, a mesh node must obtain traffic load information from all neighbors including one-hop and two-hop ones. Otherwise, the computed target rate can be so arbitrary and degrade the performance of congestion control. However, in 802.11s standard draft no mechanism is specified to exchange traffic load related information among one-hop and two-hop neighbors. How to determine the target rate based on neighbor information is not specified either.

Moreover, there is no scheme specified in 802.11s for the local rate control. Simply adjusting EDCA parameters cannot achieve the goal because EDCA is more effective for traffic prioritization rather than ensuring a certain traffic rate. The above problems render the current framework for congestion control useless in a multihop mesh environment.

4.6. MDA

MDA aims to reduce the contention in a 802.11s mesh. However, such a mechanism can cause an interoperability issue. In the same 802.11s mesh network, if there have both non-MDA and MDA nodes, the performance of either type of nodes can be degraded. An MDA node has no way to prevent
a non-MDA node from accessing the MDA TXOP. On the other hand, the non-MDA node may experience difficulty in accessing the medium due to the existence of MDA TXOP.

The MDA mechanism relies on timely information of neighbor MDAOP interfering times and neighborhood MDAOP times to determine an MDAOP. This means frequent message exchange is needed between MPs, which causes a large overhead. Moreover, such information can be propagated over multiple hops, but no filtering mechanism is specified in MDA, which further increases overhead.

4.7. QoS

Although 802.11s adopted the EDCA mechanism, no QoS can be guaranteed. First of all, EDCA is only a mechanism of achieving “soft” QoS, i.e., traffic prioritization. Such a mechanism is good for traffic classes with different priorities. For the nodes with the same class of traffic, no priority is provided. Such a problem is more severe in a multihop environment.

Other mechanisms such as MDA or intra-mesh congestion control at most provide some improvement of QoS locally, because such mechanisms still contain many problems in a multihop environment as explained before.

For end-to-end QoS of a traffic flow, a reservation scheme is usually needed. However, no such a mechanism is specified in 802.11s.

4.8. Security

802.11s inherits security framework from 802.11i with certain extensions. Thus, whatever security problems exist in 802.11i will also occur in 802.11s. Moreover, due to the multihop mesh network architecture, security becomes a more challenging issue. For example, in WLAN environment, it is reasonable to assume there is a trustworthy channel between AS and authenticator. However, in a mesh network, the multihop wireless link between AS and MKD or MA does not always provide a trustworthy channel between AS and MKD or MA.

On the other hand, all security procedures of 802.11s only take care of the potential security attacks in network association and secure link establishment. How to make sure the routing protocol is secure is not specified. Routing security is usually considered as out-of-scope work for an IEEE 802.11 standard. However, for 802.11s, since the routing functionality is specified in the link layer, it becomes imperative to specify a security mechanism for routing protocols in 802.11s standard.

4.9. Mobility and fast handoff

In 802.11s, non-mesh clients are supported through an MAP. For such kind of nodes, when they move within the mesh, the handoff delay can be large due to channel scanning, security, authentication, and other necessary operation procedures. On the other hand, real-time services such as voice over Internet protocol (VoIP) are killer applications of 802.11s WMNs. In order to support real-time services in 802.11s WMNs, fast handoff schemes need to be developed. A possible solution for 802.11s is to develop a fast handoff mechanism based on radio resource measurement as specified in 802.11k [13]. However, for certain scenarios, MAPs or MPs can be mobile, the fast handoff issue becomes more challenging and demands more an efficient solution.

4.10. Multiple MPPs

In the current framework of 802.11s, single MPP is assumed. However, in a relatively large scale WMNs, e.g., an enterprise network, multiple MPPs are needed in order to provide enough backhaul capacity to the Internet. When multiple MPPs are available, many functionalities such as interworking and routing protocols in the current 802.11s draft need to be modified accordingly.

5. Conclusion

The network architecture and major functionalities of the upcoming standard of 802.11s WMNs were investigated in this article. In particular, the issues that degrade the performance of 802.11s WMNs were analyzed. Although the IEEE 802.11s task group is working hard to resolve comments raised by voters, no sign is shown that the issues discussed in this article will be resolved on this task group’s agenda. We admit that a WMN built up according to the current framework of 802.11s specification will probably work. However, there is no doubt that the performance of such a WMN is extremely low. To ensure scalable performance in a future 802.11s WMN, it is indispensable to develop new protocols to resolve issues pointed out in this article.
Acknowledgements

The authors would like to acknowledge Bing Zhang and Youiti Kado at NICT, Japan, and Weilin Wang and Michael Nova at Kiyon, Inc., for their valuable discussions and suggestions.

References