The IEEE 802.11s Extended Service Set Mesh Networking Standard

Joseph D. Camp and Edward W. Knightly
Electrical and Computer Engineering, Rice University, Houston, TX
{camp, knightly}@ece.rice.edu

***Abstract*— Today, municipalities are planning to deploy metro-scale two-tier wireless mesh networks at a rapid pace. Fittingly, the IEEE 802.11s standard is being developed to allow inter-operability between heterogeneous mesh network devices. In this article, we describe and discuss how the initial standard addresses key factors for standardization of these networks: (i) efficient allocation of mesh resources at the routing and MAC layers, (ii) protection and conservation of the network resources via security and energy efficiency, and (iii) assurance of fairness and elimination of spatial bias via mesh congestion control. We draw upon examples from existing two-tier deployments, simulations, and analytical models to motivate these enhancements within the standard.**

I. Introduction

Wireless mesh networks provide reduced infrastructure costs for access networks spanning up to hundreds of square miles by reducing the use of costly wired entry points that supply access to the Internet [1]. Moreover, multiple, redundant wireless routes are able to route around network faults to self-heal (refer to Fig. 1). We define such networks as two-tier mesh networks, consisting of a backhaul tier (mesh node to mesh node) and an access tier (mesh node to client): Instead of the typical wireline backhaul, the wireless mesh nodes forward data to and from wireline entry points. Clients or access nodes throughout the coverage area then connect to local mesh nodes to receive connectivity back to the wireline network.

City-wide two-tier mesh networks are becoming attractive for metropolitan areas of all sizes and thereby, reshaping the traditional roles of municipal access networks. Many cities have already deployed mesh networks to assist public service and safety personnel, e.g., New Orleans, San Mateo, and Chaska[1]. Other cities, such as Philadelphia[2], Houston[3], and San Francisco, plan city-wide two-tier mesh deployments to additionally provide public broadband Internet access. A two-tier mesh testbed on the East End of Houston provides Internet access to residents of a low-income neighborhood spanning two square miles [2]. Moreover, a number of single-tier networks such as in Champaign-Urbana[4] have been deployed via "organic growth" via volunteers vs. planned large-scale two-tier deployments for city-wide coverage.

These planned and existing deployments have been facilitated by the IEEE 802.11 providing standardized modulation types (802.11a, b, and g) and service differentiation (802.11e). Further, the security amendments to the standard (802.11i) and multi-input, multi-output (MIMO) communication by Task Group n (TGn) can signficantly enhance mesh operation. In IETF, the Mobile Ad Hoc Network (MANET) work group has standardized many multihop routing protocols such as Ad Hoc On-demand Distant Vector Routing (AODV), Dynamic Source Routing (DSR), and Optimized Link State Routing (OLSR). Now, the increasing demand for mesh networks necessitates a new standard by which networking manufacturers can extend the interoperability of hardware and software for multi-vendor mesh network deployments. In 2004, a task group (TGs) was formed to define the Extended Service Set (ESS) Mesh Networking Standard. To date, the standard draft amendment (802.11s) exists as a single proposal comprised of select proposal characteristics from various organizations [3]. IETF has no such group for mesh networking.

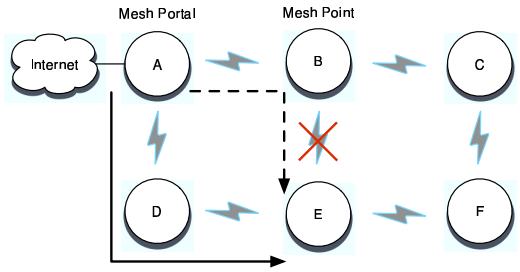

Fig. 1. In a mesh network, there are redundant routes which allows connectivity even when wireless links fail. Here, the wireless link from B to E fails so the initial route (dotted arrow) changes to route around the failure (solid arrow). For a full definition of IEEE 802.11s terms refer to II-A.

There are three technical challenges that the IEEE 802.11s mesh standard must solve so that current and future deployments can effectively provide bandwidth over large coverage areas: (i) the efficient use of limited resources (capacity and time) since intermediate mesh nodes are used both to source and forward data over the mesh, (ii) the protection and conservation of resources–both in securing data for sensitive applications and conserving power for long-term operation of mobile wireless devices, and (iii) providing fairness via elimination of spatial bias, i.e., assurance that mesh nodes closer to the gateway nodes do not achieve higher throughput than mesh nodes of greater hop count. While others have created a survey of the existing literature on mesh networks [4], in this

[1]http://www.tropos.com/applications
[2]http://www.phila.gov/wireless
[3]http://www.houstontx.gov/it/wirelessrfp.html
[4]http://www.cuwireless.net

article, we motivate each of the three aforementioned technical challenges through examples from existing mesh deployments, simulation, and analytical models. We also describe how each challenge is addressed in the initial IEEE 802.11s standard.

The organization of the article is as follows. We first provide an overview of the work and define key terms of IEEE 802.11s mesh networks in Section II. We present the proposed IEEE 802.11s routing and MAC layer enhancements in Section III and IV, respectively. We present the 802.11s methods to protect data in terms of security in Section V and power management in Section VI. Next, we address the elimination of spatial bias through the 802.11s congestion control mechanism in Section VII. Finally, we conclude in Section VIII.

II. Overview: IEEE 802.11s Mesh Networks

In this section, we define the IEEE 802.11s draft standard terms, MAC frames, channel selection, topology discovery, and interworking mechanisms.

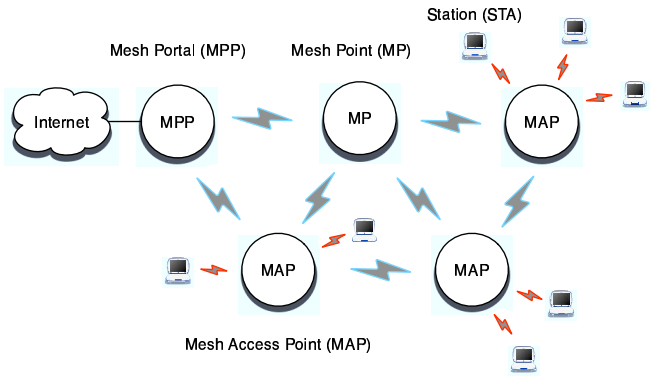

Fig. 2. IEEE 802.11s terms: A Mesh Portal (MPP) connects to the wired Internet, a Mesh Point (MP) just forwards mesh traffic, and a Mesh Access Point (MAP) additionally allows stations (STA) to associate with it.

A. Key Terms

The draft standard defines a mesh network as two or more nodes that are interconnected via IEEE 802.11 links which communicate via mesh services and comprise an IEEE 802.11-based Wireless Distribution System (WDS). A mesh link is shared by two nodes who can directly communicate to one another via the wireless medium. A pair of nodes which share a link are neighbors. Any node that supports the mesh services of control, management, and operation of the mesh is a Mesh Point (MP). If the node additionally supports access to client stations (STAs) or non-mesh nodes, it is called a Mesh Access Point (MAP). A Mesh Portal (MPP) is an MP that has a non-802.11 connection to the Internet and serves as an entry point for MAC Service Data Units (MSDUs) to enter or exit the mesh (refer to Fig. 2). An MPP and MAP may be collocated on one device. The draft standard additionally defines options for power-constrained MPs to be lightweight, in which nodes are able to communicate only with their neighbors and do not use the distribution system (DS) or provide congestion control services. It additionally defines a non-forwarding MP for leaf nodes that can fully operate within the mesh even if no MAPs are available (which a STA could not do). A mesh network can have one operating channel or multiple operating channels. A Unified Channel Graph (UCG) is a set of nodes that are interconnected on the same channel within a mesh network.

B. Channel Selection

After initialization, a node uses the Simple Channel Unification Protocol where the MP performs active or passive scanning of the neighbors. If no neighboring MPs are found, the MP can establish itself as the initiator of a mesh network by selecting a channel precedence value based upon the boot time of the mesh point plus a random number. If two disjoint mesh networks are discovered (i.e., they are on different channels), the channel is chosen according to the highest precedence value. If the mesh is in the 5 GHz band, the mesh is required to conform to the regulatory requirements of the dynamic frequency selection (DFS) and radar avoidance to conform with FCC UNII-R regulation.

C. Topology Discovery and Link State

Mesh Points (MPs) that are not yet members of the mesh must first perform neighbor discovery to connect to the network. A node scans neighboring nodes for beacons which contain at least one matching profile, where a profile consists of a mesh ID, path selection protocol identifier, and link metric identifier. If the beacon contains a mesh capacity element that contains a nonzero peer link value (r and e_{pt}, refer to Section III-A) then the link can be established through a secure protocol.

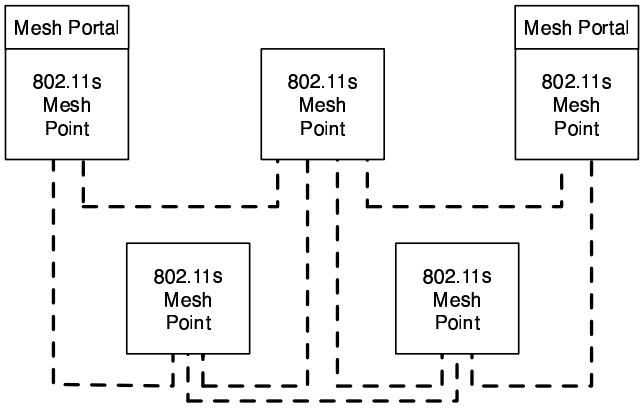

Fig. 3. Reference Model for WLAN Mesh Interworking.

D. Interworking

Mesh Portals bridge the wireless and wired networks. MPPs function as if on a single loop-free logical layer 2 and interconnected layer 3 for both the internal mesh and the external LAN segments. For layer 2, the MPPs use the IEEE 802.1D bridging standard, and at layer 3, routing must be performed in a similar fashion to IP gateway routers.

III. Path Selection and Routing

Mesh traffic is predominantly forwarded to and from wireline gateway nodes forming a logical tree structure. The Hybrid Wireless Mesh Protocol (HWMP) within the IEEE 802.11s draft standard uses hierarchical routing to exploit this tree-like logical structure and an on-demand routing protocol to address mobility. The on-demand routing protocol is based upon AODV which uses a simple hop count routing metric [5]. HWMP is the default routing protocol and therefore must be implemented on all MPs. The draft standard also defines an optional Radio Aware-Optimized Link State Routing (RA-OLSR) that uses multipoint relays, a subset of nodes that flood a radio aware link metric, thereby, reducing control overhead of the routing protocol. In this section, we define the radio-aware metric and the HWMP routing protocol within the draft standard. We then relate the standard's mechanisms to prior routing research in ad hoc and mesh networks.

A. 802.11s Radio Aware Link Metric

IEEE 802.11s defines a default link metric and also provides for the use of alternate link metrics for a UCG. All nodes must employ a radio-aware path selection metric to ensure a routing metric is can be agreed upon. The Airtime Link Metric is used to calculate each pairwise link within the mesh and is defined to be the amount of channel resources consumed by transmitting the frame over a particular link. The airtime cost c_a is defined in terms of the modulation rate r and bit error rate e_{pt} for a test frame of size B_t,

$$c_a = \left(O_{ca} + O_p + \frac{B_t}{r} \right) \frac{1}{1 - e_{pt}} \tag{1}$$

where the channel access overhead O_{ca}, protocol overhead O_p, and B_t are defined constants for each 802.11 modulation type (see Table I).

Parameter	802.11a	802.11b	Description
O_{ca}	75 μs	335 μs	Channel access overhead
O_p	110 μs	364 μs	Protocol overhead
B_t	8224	8224	Number of bits in test frame

TABLE I
Airtime Link Metric Constants

B. Hybrid Wireless Mesh Protocol

The IEEE 802.11s draft standard uses the Hybrid Wireless Mesh Protocol (HWMP) to provide both on-demand routing for predominantly mobile topologies and proactive tree-based routing for predominantly fixed infrastructure networks. The hybrid protocol is used in the case that an MP does not have an on-demand route to another MP and sends the first packet to the root. Subsequent packets can be sent along a shorter path that is found directly.

1) On Demand Routing: With an on-demand routing protocol, the network is not required to use routes through the root node (or even have a root node). Specifically, IEEE 802.11s MPs can use a Route Request (RREQ) and Route Reply (RREP) mechanism to discover link metric information from source to destination. To maintain the route, nodes send periodic RREQs where the time between two different RREQs transmitted at the same source is known as a refresh-round. Sequence numbers are used per refresh-round to ensure loop-free operation. To avoid updating poor routes too quickly, hysteresis is used to maintain operation of the better route in the case that the updated RREQ from the original route is lost or the RREQ from along another route is delivered first in a particular round. Each best candidate route is cached for later use in case loss occurs on a newly selected route.

2) Tree Based Routing: When a Mesh Portal (MPP) exists within the topology, the network can use proactive, distance vector routing through the root to find and maintain routes. The root announcement is broadcast by the root MPP with a sequence number assigned to each broadcast round. Each node updates the metric as the announcements are received and rebroadcasted. The MP chooses the best parent and caches other potential parents. Periodic RREQs are sent to parents to maintain the path to the root. If the connection to the parent is lost (3 consecutive RREQs), the MP will notify its children, find a new parent, and send a gratuitous RREP to the root, which all intermediate nodes use to update their next-hop information about the source.

C. Related Work

The logical tree structure has been expoited within multicast and broadcast routing mechanisms for wireless networks [6] but not for unicast delivery. There have been many on-demand routing protocols for ad hoc networks, most notably DSR and AODV which were directly compared in [7]. However, there has been very few known works that incorporates both on-demand routing with the advantages of a logical tree structure for efficient unicast delivery of packets. As for link metrics, the expected transmission count (ETX) was studied on a single tier mesh testbed [8]. In a comparison of the route metrics of ETX, per-hop RTT, and per-hop packet pair, ETX had the best performance for static networks, but when the sender had mobility the simple hop count metric outperformed ETX as it was not able to react quickly enough to account for link quality changes [9].

IV. Medium Access Control

Due to multihop forwarding, flows of equivalent throughput but differing hop count from the gateway consume different amounts of network resources according to the distance from the portal node. Therefore, the available resources must be efficiently allocated for the network to effectively serve a large coverage area. In this section, we discuss the MAC layer enhancements of synchronization and EDCA optimizations within the 802.11s draft standard that enable efficient allocation of mesh resources in respect to both capacity and time.

For each, we discuss related work for such medium access control enhancements.

A. Synchronization

1) Proposed 802.11s Synchronization: Synchronization is an optional feature for MPs. With synchronization, each MP updates its timers with time stamp and offset information received in beacons and probe responses from other MPs, thereby maintaining a common Mesh TSF time. The self time stamp τ_s from the perspective of the receiving MP is in terms of the received time stamp τ_{rd} plus received offset δ_{rd} minus the receiver offset δ_{rx}:

$$\tau_s = \tau_{rd} + \delta_{rd} - \delta_{rx}. \quad (2)$$

Otherwise, synchronizing MPs may choose to update their offsets instead of the timers. The new self offset value $\delta_{s'}$ is updated when the τ_{rd} plus δ_{rd} is greater than the τ_s plus the self offset δ_s. If $((\tau_r + \delta_{rd}) > (\tau_s + \delta_s))$ then

$$\delta_{s'} = \tau_{rd} + \delta_{rd} - \tau_s. \quad (3)$$

Synchronization plays a critical role in the beaconing functionality of MPs (for the complete beacon generation process refer to [10]) and provides a means for MPs to avoid beacon collisions. MPs collect beacon timing information from neighbors and set their TSF accordingly. Some MPs, however, choose to be unsynchronized if communicating with MPs that do not support the feature.

2) Related Work: Features such as multi-channel coordination and power saving mechanisms require synchronization. Furthermore, there are performance benefits such as improved fairness with synchronization. For example, [11] establishes that starvation effects encountered in multi-hop scenarios can be significantly alleviated with synchronized contention; albeit the improvements are significantly reduced if clocks drift away from perfect synchronization.

B. Enhanced Distributed Channel Access

As a background, the EDCA mechanism allows service differentiation in IEEE 802.11 networks by using up to four different channel access functions (CAFs) that each execute independent backoff counters. The difference in absolute values of timers and the maximum contention window allows the differentiation of traffic types.

1) Proposed 802.11s EDCA Optimizations: The Network Allocation Vector (NAV) is specified within control, data, and management frames of IEEE 802.11 to inform other potential transmitters when the medium will become free, thereby reducing collisions. In the 802.11s draft standard, there is an optional enhancement to the traditional NAV behavior in the form of a Full NAV to protect the medium until the end of the TXOP, a Packet by Packet (PbP) NAV to protect until the receipt of an ACK, and a NAV clearing mechanism to inform the medium there has been no signal transmitted for two SIFS plus CTS duration plus two slot times. The latter reclaims the medium for use in the case of an incomplete 4-way handshake.

2) Related Work: Scenarios for unnecessary NAVs are outlined in [12] and a proposed NAV clearing mechanism called Receiver Initiated NAV Clearing method is analyzed via simulation.

V. Security

The IEEE 802.11s draft standard uses Efficient Mesh Security Association (EMSA) to prevent unauthorized devices from sending and receiving traffic on the mesh, both to preserve resources and protect against malicious attacks. Like single hop wireless LANs, EMSA uses the 802.11i link level authentication model which which includes 802.1X authentication, key distribution, and encryption of management frames. However, the key difference in security for mesh networks as opposed to traditional WLANs is that Mesh APs must act in both Authenticator and Supplicant roles. In this section, we discuss EMSA with respect to role negotiation, authentication, and key management as well as discuss work related to mesh security.

A. Role Negotiation

An MP must function in two different roles in order to be an Authenticator for client nodes and downstream MPs and a Supplicant to upstream MPs. Further, a single MP may set up multiple security relationships since there may exist paths to multiple MPs. When a node attempts to join a mesh network, it must first discover what Authenticated Key Management (AKM) and ciphersuites are available. Then, the two nodes each must negotiate its role in the authentication process. If a node can reach an Authentication Server (AS) and the other cannot (typically the node joining the mesh), the AS-connected node becomes the Authenticator. If both can reach an AS, then the node with the higher MAC address becomes the Authenticator, and the remaining node becomes the Supplicant.

B. Authentication and Key Management

Once roles have been established, two nodes will perform the four-way handshake as specified in 802.11i resulting in a Pairwise Master Key (PMK). If this is the initial contact the AS will generate a fresh PMK for the exchange. In the 802.11s draft standard, PMKs can be cached by the Authenticator for faster reconnections once the link has already been established. After authentication occurs, authentication occurs, the broadcast and unicast payload is secured by the Group Temporal Key (GTK) and Pairwise Transient Key (PTK), respectively, which are updated periodically by the AS.

C. Related Work

Potential denial-of-service attacks and their implications have been explored for WLAN [13] and ad hoc networks [14], with no work focusing on features particular to mesh networks. In [15], the potential for wireless intruders is explored from a multi-layer approach through anomaly detection. Likewise, a class of research has explored securing wireless routing protocols, such as [16]. Finally, [17] secures multihop wireless

networks by a novel distribution of keys and a decentralized solution where each node in the network is given equivalent roles.

VI. Power Management

While MAPs are required to be continuously awake, MPs may optionally support a Power Save (PS) mechanism if they do not have a permanent connection to a power source. Fully charged devices might stay awake continuously to more efficiently forward traffic, but when at critical power levels, could enter a sleep state to conserve power. In this section, we discuss the PS operation for MP to MP and MP to MAP communication.

A. Mesh Point to Mesh Point Communication

While in the PS mode, MPs periodically wake and listen for DTIM beacons and remain awake for the time window specified within the Announcement Traffic Indication Message (ATIM). MPs not entering the PS mode may communication with PS MPs by buffering data and delivering in three ways: (i) send the traffic in the agreed upon schedule as part of the Automatic Power Save Delivery (APSD), (ii) send traffic during the ATIM window to request PS-enabled MP to stay awake past the ATIM window, or (iii) send a single Null-DATA packet during ATIM window to reactivate a suspended flow or change PS state.

B. Mesh Point to Mesh Access Point Communication

MAPs can support PS mode whether they are synchronizing or not via the IEEE 802.11 infrastructure power management operation. Further, if a synchronizing MP wishes to communicate with a non-synchronizing MAP, the MP is required to be awake for the BSS DTIM interval of each MAP that he wishes to communicate in addition to the required Mesh DTIM regular beacon frame intervals on which to coordinate with synchronizing MP neighbors. Lightweight-MPs may act as a STA and associate with an MAP as an alternate way to enter a PS state if there is an MAP in the vicinity.

C. Related Work

Power saving mechanisms in mobile ad hoc networks and sensor networks have been widely studied. Ad hoc networks provide untethered connectivity during mobility, thereby requiring extended operation from a battery. Power saving mechanisms for ad hoc networks are compared and the legacy power saving mechanism of IEEE 802.11 is fully defined in [18]. Likewise, because sensors are small and have limited battery capacity, they must also efficiently use power. In [19], sensor nodes are synchronized and have duty cycles consisting of wake and sleep epochs, with message passing to notify neighbors of changes to periodic sleep schedules.

VII. Congestion Control

Two-tier mesh networks aggregate traffic at the portal nodes, resulting in a tree-like traffic pattern. MPs contend for a share of portal bandwidth as they forward traffic from MPs of greater hop count from the portals. Under high load, if there is no congestion control mechanism the MPs on the outer edges of the network will obtain low throughput and are prone to starvation [20]. This disproportionate usage of bandwidth based upon distance from the MPP is called spatial bias. In this section, we describe the congestion control mechanism within the draft standard. We then present measurements from the TFA deployment in Houston and other related congestion control mechanisms for mesh networks.

A. 802.11s Congestion Control

The draft standard outlines an optional hop-by-hop congestion control mechanism. Each MP observes the level of congestion based upon the amount of incoming and outgoing traffic (local congestion monitoring). When the traffic increases to a point such that the MP is unable to forward and source data upstream as fast as the incoming rate, congestion occurs, and the MP must notify one-hop neighbors (local congestion control signaling). These neighbors respond by limiting the rate at which they are sending to the congested MP (local rate control).

1) Local Congestion Monitoring: Two example congestion detection monitoring schemes are proposed in the standard. In the first, each MP regulates incoming and outgoing data to minimize the transit queue size, defined here to be the difference between aggregate packets received and transmitted at the MAC. With sufficient queue size, a notification of congestion is issued to one-hop neighbors. Alternatively, MPs could use the queue size as a metric for detecting congestion. Using lower and upper thresholds, congestion can be controlled by signaling congestion with probability p given by:

$$p = \frac{q - t_l}{t_u - t_l} \tag{4}$$

where q is queue size and t_l and t_u are lower threshold and upper threshold respectively.

2) Congestion Control Signaling: With sufficient queue size, the "Congestion Control Request" notifies the previous hop of congestion experienced at the signaling node so that the previous hop can rate limit its transmission. A "Neighborhood Congestion Announcement" can be broadcast by the congested node in which case all immediate neighbors will limit their traffic based upon service differentiation criteria from a common EDCA parameter set by an expiration time. Nodes may send out a specific congestion control message to selected nodes to request reduction of their offered traffic by some amount. The receiving nodes can then use this to compute the target rate n according to the channel capacity C, average packet size P, average overhead per packet in time units T_{oh}, and time units t:

$$n = \frac{tC}{P + CT_{oh}}. \tag{5}$$

3) Local Rate Control: Upon receiving either congestion message, a node is responsible to rate limit its outgoing traffic. The node must meter its own traffic and shape it according to the data rate specified by the "Congestion Control Request" message. MAPs must also consider rate control of the BSS

traffic in addition to mesh traffic. STAs do not require explicit knowledge of the congestion control scheme since MAPs can send CTS messages to themselves to free the channel.

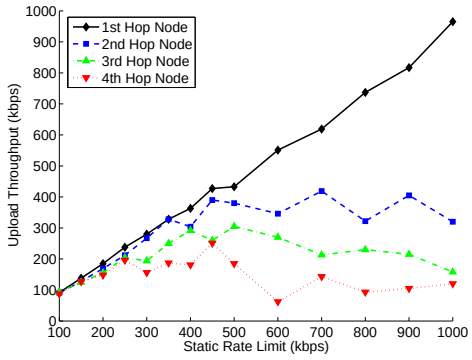

Fig. 4. The fully backlogged parking lot traffic matrix upstream with each flow equally rate limited at the source (Fig. 14 from [20]).

B. Related Work

In [20], measurements are presented from a 4-hop, 3-flow linear topology, with all traffic being long-lived upstream TCP flows. In Fig. 4, a uniform static rate limit is used to explore the fairness and spatial bias issue. The figure indicates that some spatial bias occurs even when rate limiting each node to the ideal fair rate of 450 kbps per node (computed as a 9 single hop subflow, 3-hop clique that mutually contends for a 4 Mbps capacity link). Further, as the static rate limit value is increased, the first hop MP achieves 1 Mbps (full rate) compared to 100 kbps at the last hop. Other experiments from the paper show that if no rate limiting is used, starvation occurs at the last node. Since traffic demand is highly variable within mesh access networks, a dynamic rate control scheme (i.e., congestion control algorithm) is clearly needed. The draft standard provides an optional mechanism for realizing mesh congestion control but leaves the algorithm itself unspecified.

VIII. Conclusion

In this paper, we illustrate how the developing IEEE 802.11s ESS Mesh Networking Standard draft addresses the technical challenges of the pervasive deployment of wireless mesh networks, the efficient allocation of mesh resources (routing and MAC layers), the protection of network resources (security and power savings), and the elimination of spatial bias (congestion control). We outline the current state of the standard with respect to examples from current deployments, simulations and analytical models to both motivate and discuss the efficacy of such a standard.

References

[1] R. Karrer, A. Sabharwal, and E. Knightly, "Enabling large-scale wireless broadband: the case for TAPs," in *Proceedings of HotNets-II*, Cambridge, MA, Nov. 2003.

[2] J. Camp, E. Knightly, and W. Reed, "Developing and deploying multihop wireless networks for low-income communities," in *Proceedings of Digital Communities*, Napoli, Italy, June 2005.

[3] IEEE, "Draft amendment: ESS mesh networking," IEEE P802.11s Draft 1.00, November 2006.

[4] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks and ISDN Systems*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[5] C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad hoc on demand distance vector (AODV) routing," IETF RFC 3561, July 2003.

[6] K. Viswanath and G. Tsudik, "Exploring mesh and tree-based multicast routing protocols for manets," *IEEE Transactions on Mobile Computing*, vol. 5, no. 1, pp. 28–42, Jan. 2006.

[7] S. R. Das, C. E. Perkins, and E. M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," in *IEEE INFOCOM*, Tel Aviv, Isreal, Mar. 2000.

[8] D. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of ACM MobiCom*, September 2003.

[9] R. Draves, J. Padhye, and B. Zill, "Comparisons of routing metrics for static multi-hop wireless networks," in *ACM SIGCOMM*, Portland, OR, Aug. 2004.

[10] IEEE, "Wireless LAN medium access control and physical layer specification," ANSI/IEEE Standard 802.11, 1999.

[11] J. Shi, T. Salonidis, and E. Knightly, "Modeling fairness and clock drifts under synchronized CSMA contention," Rice University ECE Department, Tech. Rep., Aug. 2006.

[12] L. Du and L. Chen, "Receiver initiated network allocation vector clearing method in WLANs," in *IEEE APCC*, Perth, Australia, Oct. 2005.

[13] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *USENIX Security Symposium*, Washington, DC, Aug. 2003.

[14] I. Aad, J. Hubaux, and E. Knightly, "Denial of service resilience in ad hoc networks," in *ACM MobiCom*, Philadelphia, PA, Sept. 2004.

[15] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *ACM MobiCom*, Boston, MA, Aug. 2000.

[16] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *ACM Wireless Networks*, vol. 11, no. 1–2, pp. 21–38, Jan. 2005.

[17] J.-P. Hubaux, L. Butty, and S. Capkun, "The quest for security in mobile ad hoc networks," in *ACM MobiHoc*, Long Beach, CA, Oct. 2001.

[18] Y.-C. Tseng, C.-S. Hsu, and T.-Y. Hsieh, "Power-saving protocols for IEEE 802.11-based multi-hop ad hoc networks," in *IEEE INFOCOM*, New York, NY, June 2002.

[19] Y. Wei, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE Transactions on Networking*, vol. 12, no. 3, June 2004.

[20] J. Camp, J. Robinson, C. Steger, and E. Knightly, "Measurement driven deployment of a two-tier mesh urban access network," in *ACM MobiSys*, Uppsala, Sweden, June 2006.