Principles of IEEE 802.11s

Guido R. Hiertz*, Sebastian Max*, Rui Zhao*, Dee Denteneer†, Lars Berlemann‡
*Chair of Communication Networks, Faculty 6, RWTH Aachen University, Aachen, Germany
†Philips, Eindhoven, The Netherlands
‡Swisscom, Bern, Switzerland

***Abstract*—In 2003, interests in the Institute of Electronics and Electrical Engineering (IEEE) 802.11 Working Group (WG) led to the formation of Task Group (TG) "s". 802.11s develops a Wireless Mesh Network (WMN) amendment. Unlike existing Mesh products, 802.11s forms a transparent 802 broadcast domain that supports any higher layer protocols. Therefore, 802.11s provides frame forwarding and path selection at layer-2. 802.11i describes a security concept for stations that associate with an Access Point (AP). However, in a Mesh Basic Service Set (BSS) devices need to mutually authenticate to provide integrity of the network. Thus, 802.11s adds additional elements to the concepts of 802.11i. While traditional Wireless Local Area Networks (WLANs) are AP centred an 802.11 Mesh is fully distributed. Hence, 802.11s considers extensions to the Medium Access Control (MAC) too.**

The authors have contributed to the standardization of 802.11s since 2003. As constant participants we give insight to draft 1.02 of TG "s" and provide an outlook to future evolution of 802.11's first Mesh standard.

***Index Terms*—IEEE 802.11s, IEEE 802.11, Wireless Mesh Network, Mesh BSS, WLAN**

I. Introduction

Wireless Local Area Networks (WLANs) have become ubiquitous. As soon as 802.11n becomes a finale amendment, data rates up to 600 Mb/s will be available. However, transmission range becomes a limiting factor as channels are limited to 20 MHz resp. 40 MHz and transmission power may not exceed 100 mW. In case of 802.11, dense deployment of Access Points (APs) is needed to meet customer's expectations of ubiquitous wireless connectivity at high speed. To interconnect, APs rely on a fixed backbone. While APs are cheap, the sufficient deployment of the wired infrastructure is expensive. To overcome the cost barrier, APs need to interconnect wirelessly [1], [2]. In 802.11, amendment "s" describes the necessary functions to form a Wireless Mesh Network (WMN). While in beginning the project was restricted to APs only, the latest change to its Project Authorization Request (PAR) makes 802.11s much more flexible. In the following, we provide an introduction to 802.11s and its latest trends.

A. Outline

This paper bases on [3] that is approved as revision 2007 of 802.11. Among others, it incorporates the amendments 802.11e (support for Quality of Service) and 802.11i (security enhancements). Section II introduces the 802.11 architecture and the amendments of 802.11s [4]. Section III describes Medium Access Control (MAC) in 802.11s. Due to limited space, the authors cannot present simulation results [5]. However, we explain in detail why the current scheme limits performance to a low degree. These findings are in accordance with simulation results presented at the 802.11 Working Group (WG) meeting in September 2006.

In section IV resp. V we explain synchronization and power saving concepts. In section VI we introduce the security concepts of 802.11i and the necessary changes for 802.11 Mesh. Link management and path selection are introduced in section VII and VIII. An outlook and conclusion is given in section IX.

II. 802.11 Architecture

In 802.11 [3], the most basic entity is a station. Any device that satisfies the requirement of an 802.11 conformant Medium Access Control (MAC) and Physical Layer (PHY) may be denoted as station. A station with extended capabilities that is the central device for other stations of a Wireless Local Area Network (WLAN) is named Access Point (AP). Wireless stations authenticate and associate with an AP to get access to the network. Thus, the AP and its associated stations form a star topology. In 802.11, this topology is called an infrastructure Basic Service Set (BSS). In addition, an Independent Basic Service Set (IBSS) is formed without an AP. 802.11 generically defines the BSS as a set of stations that have successfully joined. In the following we focus on the infrastructure BSS as it is the most often used type of deployment. In it, stations rely on the AP for communication. Each station has at least a link to the AP to be able to participate in the BSS.

In 802.11 the term link is defined from the MAC layer's point of view. A single physical path over the Wireless Medium (WM) describes the 802.11 link that enables two stations to exchange MAC Service Data Units (MSDUs). Despite the optional unacknowledged mode of 802.11e, in 802.11 every successfully received MSDU is acknowledged. As the Acknowledgment (ACK) is a short frame that is usually sent at a robust Modulation and Coding Scheme (MCS), its Packet Error Rate (PER) is much smaller than the acknowledged frame. Hence, in wireless communication successful transmission of a data frame from station A to station B does not guarantee the reverse [6]. However, although not explicitly stated 802.11 assumes all links to be bidirectional.

As the infrastructure BSS forms a wireless single-hop network where all participating stations send and receive frames via the AP, the AP operates as relay between them. With

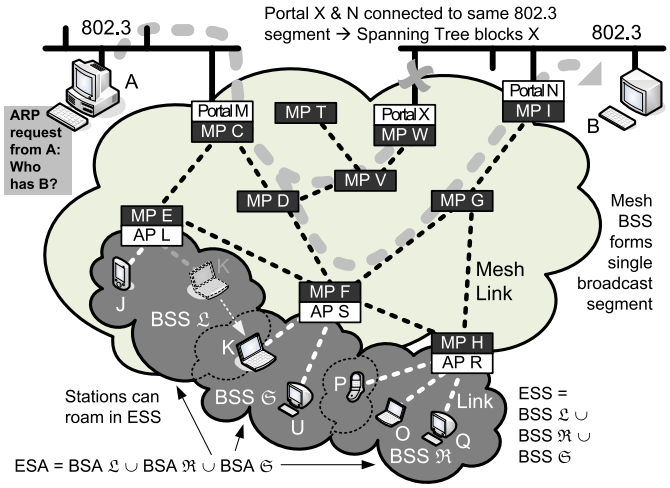

Figure 1. Here, A wants to communicate with B. It sends out an ARP request to resolve B's MAC address. Both 802.3 segments are transparently interconnected via a Mesh BSS. MPs C, I and W are co-located with a portal. They bridge the non-802.11 and the 802.11s segment. The spanning tree protocol seamlessly works over 802.11s to avoid looping. The Mesh BSS also connects APs L, R and S to form a single ESS. Thus, J, K, O, P, Q and U can roam inside the ESA.

the help of the Distribution Service (DS) multiple APs may interconnect their BSSs to form an Extended Service Set (ESS). 802.11 calls the total area covered by all interconnected BSSs the Extended Service Area (ESA). Within the ESA stations may roam from one AP to another. To form an ESS, APs use the Distribution System Service (DSS). The AP relies on the Distribution System Medium (DSM) to provide the DSS. At present, the DSM is a non-802.11 network. It may be either a logical entity that exist within in the AP or it is typically based on an 802.3 Local Area Network (LAN) segment. Even when in mutual communication range, APs do not use the WM to exchange frames.

Today's AP are usually collocated with a portal, since the latter provides the integration service that delivers MSDUs to non-802.11 networks. The portal allows the AP to access the 802.3 LAN that builds the DSM. Through the DS, the ESS appears as a single logical network to the Logical Link Control (LLC) layer. Thus, the DSS enables handover within the ESS and seamless frame forwarding between APs, portals and stations. To allow for addressing stations within a different BSS, 802.11 provides up to four address fields to the AP:

- The Source Address (SA) holds the MAC address of the station that generates a frame
- The ultimate and final receiver's address is denoted in the Destination Address (DA) field
- When an AP forwards a frame, Transmitter Address (TA) holds its own MAC address
- The AP uses the Receiver Address (RA) field to indicate the next intended receiver in the ESS.

A. Mesh BSS extensions to the 802.11 architecture

802.11s [4] defines the Mesh. The basic element in 802.11s is the MP. Unlike any other 802.11 entity, MPs may exchange frames over multiple wireless hops. Thus, MPs can communicate not only with other MPs inside but also outside mutual communication range. Similar to an AP or portal, the MP has relaying capability. On the one hand, the MP may operate like a station that solely acts as an application end-point (sink or source of data traffic). On the other hand, each MP may forward data frames for communication it is not involved in. However, the MP itself does not provide the AP services. While a portal bridges the 802.11 with non-802.11 networks, the MP relays frames within the 802.11 network.

In its current status [4] uses ambiguous terms and definitions. The 802.11 Working Group (WG) members' response to the first Letter Ballot of 802.11s clearly indicate the current mismatch. Thus, terms and definitions are subject to change. Therefore, in the following we use the terms that received largest support in 802.11 Task Group (TG)s. Following the 802.11 definition of a BSS, a set of MPs is referred to a Mesh BSS. 802.11 states that "Membership in a BSS does not imply that wireless communication with all other members of the BSS is possible." The same is valid for a Mesh BSS. However, with multi-hop connections members of the Mesh BSS may be able to communicate as long as a Mesh Path exists between them. More precisely, if MP A becomes an element of the set of MPs that is formed, when beginning with the set of MP B's peer MPs, for every element of the set each element's set of peer MPs is added until no new element can be added, MP A and MP can exchange MSDUs. Thus, the concatenated set of Mesh Links (MLs) defines a Mesh Path.

An MP may establish a ML with any candidate peer MP in its neighborhood. While the neighborhood includes any MP to which an 802.11 link exists, a candidate peer MP has additional credentials and properties in common. Accordingly, an MP to which an ML has been established is denoted as a peer MP. To set up an ML, two MPs perform the 802.11s peer link management protocol over the 802.11 link.

1) Mesh header field: Unlike Wireless Mesh Networks (WMNs) based on [7], 802.11s transparently supports any higher layer protocols. Furthermore, it seamless integrates in the Institute of Electronics and Electrical Engineering (IEEE) 802 set of standards. Thus, the Mesh BSS must support all kinds of unicast, multicast and broadcast traffic, see Fig. 1. Therefore, 802.11s introduces the Mesh header field. It includes four or sixteen octets. The first octet holds the Mesh Flags field. Its first bit indicates the presence the presence of Address Extension (AE). All other bits are reserved. The second octet defines the Mesh Time to Live (TTL). To avoid frames from endless looping, every MP that forwards a frame decrements the counter. As the 802.11 sequence control field is set per hop, octets three and four provide Mesh End-to-End (E2E) sequence numbering. When flooding frames, MPs use the Mesh E2E Sequence number field to avoid unnecessary retransmissions. Furthermore, the ultimate receiver of a frame uses the E2E sequence field to eliminate duplicates.

With the AE flag being set, an MP uses the six-address scheme. The additional address fields identify certain intermediate MPs on the Mesh Path. AE may be used when a root MP is present.

III. Medium Access Control in 802.11

All 802.11 Coordination Functions (CFs) base on Listen Before Talk (LBT) that is known as Carrier Sense Multiple Access (CSMA). In 802.11, the Clear Channel Assessment (CCA) combines the input of two Carrier Sense (CS) mechanisms:

- Physical Carrier Sense (P-CS) and
- Virtual Carrier Sense (V-CS).

A. Physical Carrier Sensing

With P-CS every station senses the Wireless Medium (WM) for energy. Energy exceeding one or more thresholds is interpreted as busy channel condition. Thus, the station will not try to initiate a frame exchange. The concrete threshold value depends on the 802.11 Physical Layer (PHY) layer.

B. Virtual Carrier Sensing

V-CS informs stations about ongoing or planned transmission. All stations that are not in power-save mode, constantly monitor the WM. Stations retrieve reservation information from any frame they could decode. 802.11 frames provide the reservation information in their Duration field. If present, stations set their Network Allocation Vector (NAV) to the according value. The NAV works as count-down timer. As long as the timer has a value different than zero, P-CS indicates a busy WM. The value of the NAV may be updated at any time. Thus, NAV duration may be prolonged or foreshortened.

1) The hidden station problem: In wireless communication, a device A that is close to a device B that receives data from device C is denoted as hidden if A's P-CS cannot detect C's transmission. Then, C is likely to cause interference at B thus interrupting the frame exchange. To mitigate 802.11's hidden station problem, an optional handshake exists. Based on a manually set threshold and depending on the actual frame size, the Request To Send/Clear To Send (RTS/CTS) handshake prepends a frame exchange. Both, Request To Send (RTS) and Clear To Send (CTS), are short control frames. Their transmission duration hardly depends on the Modulation and Coding Scheme (MCS). To maximize their robustness, usually they are transmitted using the lowest MCS. In their Duration field, RTS and CTS indicate the duration of the following frame exchange. Thus, all stations successfully decoding at least one of the handshake frames refrain from access to the WM.

C. Collision Avoidance

In contrast to wired networks, in wireless communication Collision Detection (CD) is not feasible. Thus, Collision Avoidance (CA) must be implemented. As part of CA, before starting a transmission each Station (STA) performs a backoff procedure. It has to keep sensing the WM for an additional random time after detecting the WM as being idle for a minimum duration called Arbitration Interframe Space (AIFS). The duration of AIFS depends on an MAC Service Data Unit (MSDU)'s priority. The additional random time is a multiple of aSlot. The duration of aSlot depends on the PHY layer. The amount of slots is determined by a random number drawn from the interval $(0, CW)$. The value Contention Window (CW) indicates the upper bound of this interval. Its initial minimum value is called CWmin and depends on an MSDU's priority too. The value of CW doubles after each unsuccessful transmission to diminish the probability of collision of a retransmission. Each successful transmission resets the the size of the CW to its initial size of CWmin. Whenever the WM remains idle for the duration of one aSlot, a STA decrements its slot counter by one. If the WM is determined busy before the counter reaches zero, the slot counter is frozen. The STA has to wait for the WM being idle for AIFS again, before resuming to decrement the slot counter. If the counter reaches zero the STA is allowed to initiate its transmission.

D. 802.11 – Coordination Functions

While the Distributed Coordination Function (DCF) supports no prioritization, Enhanced Distributed Channel Access (EDCA) forms a superset that enables for different medium access priorities. Furthermore, with EDCA stations may send multiple frames after contention. The amount of MSDUs is bound by the Transmission Opportunity (TXOP) limit. In conjunction with Block Acknowledgment (ACK) [8], EDCA operates more efficiently than DCF.

E. Medium Access Control in 802.11s

EDCA is the mandatory CF in 802.11s. A specific Mesh CF – Mesh Deterministic Access (MDA) – is described in section III-E2.

1) Problems with EDCA in Wireless Mesh Networks: To circumvent the hidden station problem, WLANs use the RTS/CTS handshake. However as factory default, all today's Wireless Fidelity (Wi-Fi) products' RTS/CTS threshold is set to its maximum value. Almost always, the setting is not user-changeable. Hence, RTS/CTS is never used. Measurement results in large wireless networks affirm its absence, see [9]. Studies show that usage of RTS/CTS has almost no impact on the network performance [10]. Accordingly, [11], [12] conclude that it only adds to the overhead.

As the sensitivity level of P-CS in 802.11 is low, the CS range is extremely large. On the one hand, P-CS prevents almost any occurrences of hidden stations, see Fig. 2. On the other hand, it prevents concurrent transmissions. As in

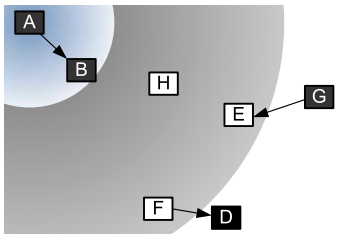

Figure 2. With 802.11, P-CS is large compared to the reception range. E, F and H refrain from channel access during A's transmission to B. G cannot detect A's transmission. Thus, it initiates a frame exchange with E. However, E does not respond as it detects a busy WM. Similar, F cannot initiate a frame exchange with D. Spatial frequency reuse is limited to low degree.

Wireless Mesh Networks (WMNs) the amount of elements in each station's set of neighbors' neighbors is larger than the amount of elements in the set of neighbors, by a single transmission many stations become exposed. These stations could reuse the WM for independent frame exchanges without causing interference. However, sensitive P-CS restricts the possibilities for spatial frequency reuse. Therefore, the exposed station problem becomes severe and EDCA achieves poor performance in Mesh BSS.

In a WMN, a station is very likely to be blocked due to CCA. Stations outside the blocked area sense an idle WM. If they have frames to be transmitted to a station inside the blocked area, they do not receive a reply. As EDCA has been developed for single hop Wireless Local Area Network (WLAN), stations interpret the absence of a response frame (ACK to data, CTS to RTS etc.) as a transmission failure. Thus, they double their Contention Window, increase a frame's retry counter and perform an additional backoff to resend the frame. As stations cannot detect their neighbors' availability, in a Mesh Basic Service Set (BSS) large idle gaps exist due to the unpredictable medium access. Thus, EDCA severely limits the performance. Fig. 3 shows a unidirectional example flow.

2) Extensions to the Medium Access Control in 802.11s: 802.11s defines an optional congestion control mechanism that works as a back-pressure scheme. It mitigates some problems of Enhanced Distributed Channel Access (EDCA) in Wireless Mesh Networks (WMNs). However, 802.11s also provides an optional Coordination Function (CF) that is aware of the difficult radio environment in WMN. It is called Mesh Deterministic Access (MDA) and it is based on the Wi-Mesh Alliance (WiMA) proposal. MDA capable Mesh Points (MPs) extend the 802.11 concept of medium reservation. While the 802.11 Virtual Carrier Sense (V-CS) provides instantaneous medium reservation after successful contention, MDA separates the negotiation process from medium reservation. Thus, MDA's reservation based medium access works similar to the Distributed Reservation Protocol (DRP) defined in [13]. With MDA a Mesh Basic Service Set (BSS) wide periodic superframe exists. Using MDA Opportunity (MDAOP) setup messages, an MDA capable MP negotiates with its neighbor MPs on the reservation of multiples of 32 µs time slots. As each MDA capable MP maintains and broadcasts in its beacon frames

1) a list of all MDAOPs during which it is a transmitter or receiver, and
2) a list of neighboring MDAOPs (interference report),

neighboring MPs are able to avoid to set-up overlapping MDA reservations. Once an MP obtains an MDAOP, it performs Clear Channel Assessment (CCA) and accesses the Wireless Medium (WM) with highest priority. Neighboring MPs refrain from channel access during that period. Fig. 4 shows a full MDA set-up and frame exchange sequence.

IV. Beacon Frames & Synchronization

In 802.11, at Target Beacon Transmission Time (TBTT) the Access Point (AP) transmits a beacon frame as soon as it senses an idle Wireless Medium (WM). In the beacon, the Beacon Interval field informs stations about the amount of Time Units (TUs) (1024 µs) between two TBTTs. Stations set their clock to the value of the Timestamp field that is a copy of the AP's Timing Synchronization Function (TSF) when the beacon was sent.

A. Synchronization in 802.11s

In 802.11s, synchronization is optional. At present, 802.11s extends the standard beacon frame by additional Information Elements (IEs) that provide routing messages for example. In 802.11, APs schedule beacons exactly at TBTT: $TBTT = TSF \pmod{dot11BeaonPeriod}$. To avoid beacon collisions,

1) Mesh Points (MPs) shall not synchronize their TSF and
2) may use Mesh Beacon Collision Avoidance (MBCA).

Due to the first measure, each MP announces a SelfTBTToffset value in its beacon. The value indicates an MP's shift to the global time. MPs use the announced SelfTBTToffset and the beacon timestamp, to calculate the common Mesh TSF. If it calculates a Mesh TSF in advance of its own time, the MP adapts its local Mesh TSF. The achievable accuracy is sufficiently high enough to enable Mesh Deterministic Access (MDA). With MBCA, MPs sometimes delay transmission of their beacon frame. Thus, they can determine if neighboring MPs have similar TBTT. Furthermore, each MP provides the beacon timing IE. It informs about TBTT of other MPs. An MP may use this information to find a time for its beacon that is less prone to interference.

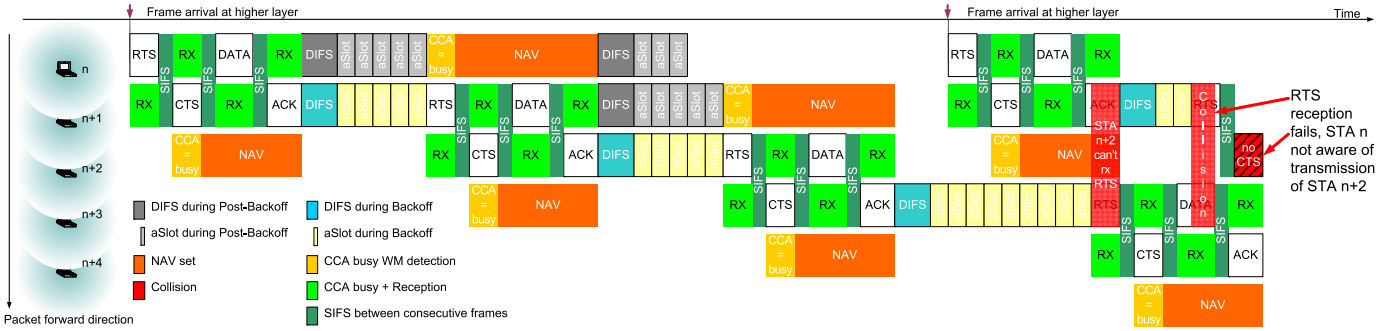

Figure 3. In this scenario, stations are placed equidistant. Each station can solely exchange frames with its immediate neighbor. P-CS is assumed to be less than twice the reception range. Although traffic flows from station n to station n+4 only, V-CS (RTS/CTS handshake) cannot prevent collisions.

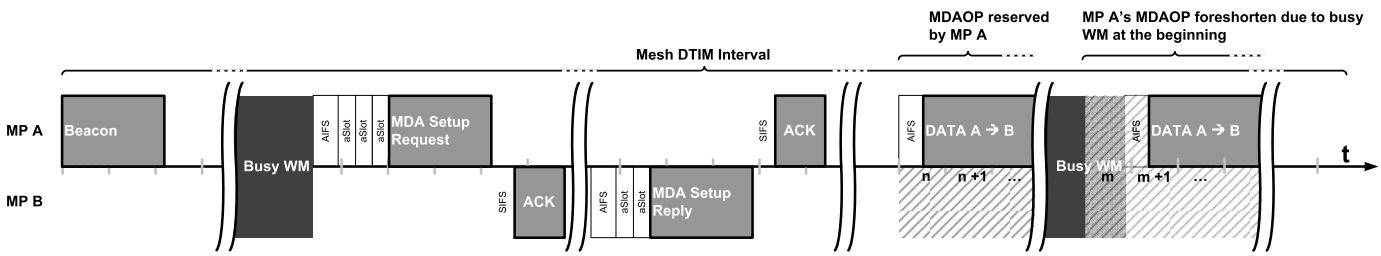

Figure 4. MP A negotiates on an MDA set-up with MP B. After establishing, MP A uses the periodic MDAOPs to send data to B. If the WM is busy at the beginning of an MDAOP, it is foreshorten. However, MP A does need to undergo the backoff procedure to access the WM during its MDAOP.

To avoid stations from trying to associate with MPs that are not collocated with an AP, the beacon frame must carry fake entries. At present, 802.11s discusses a Mesh specific beacon frame that prevents spoofed frames. Furthermore, the concept would simplify the beacon generation as it would separated from the AP functionality. Furthermore, it enables beacon periods different for MPs and APs.

V. Power Save support

In an infrastructure Basic Service Set (BSS), stations rely on the AP for power saving. A station informs the AP before switching from awake to doze state. As long as a station remains in doze state, the AP delivers multi- or broadcast traffic solely during the Delivery Traffic Indication Message (DTIM) period. The DTIM interval is a multiple of beacon periods. For unicast traffic that is buffered in the AP, stations periodically need to wake up to receive the Traffic Indication Map (TIM) that is present in all beacon frames. Having learned from a beacon frame that unicast traffic directed to the station is pending, a station sends out a Power Save (PS)-Poll frame to request the traffic's delivery from the AP.

A. 802.11s extensions for Power Saving

In a fully distributed network, power save support is difficult to achieve. 802.11s borrows from the 802.11 Independent Basic Service Set (IBSS) mode. The Mesh BSS has a common Mesh DTIM interval. However, the Mesh DTIM period is per Mesh Point (MP). During the Mesh DTIM period, the MP transmits broadcast traffic for its neighors. Power saving MPs must switch from doze to awake state for every Mesh DTIM of their peer MPs. In accordance with 802.11, an MP remains awake for at least an Announcement Traffic Indication Message (ATIM) period. During that duration, peer MP send buffered unicast frames or request the MP to remain in awake state for further frame delivery. Furthermore, MPs may use the TIM Information Element (IE) in their beacon frames to indicate buffered traffic to their peers.

VI. Security in 802.11

With respect to our focus on infrastructure Basic Service Sets (BSSs), 802.11 describes a hierarchical security concept. The Access Point (AP) operates as Authenticator that has connection to or implements an Authentication Server (AS). The station is denoted as supplicant that needs to provide credentials to gain access to the BSS.

A. 802.11s extensions to the Security Framework

802.11s secures Mesh Links (MLs) not Mesh Paths. Thus, it does not provide End-to-End (E2E) security. As a Wireless Mesh Network (WMN) is distributed in nature, 802.11s extends the 802.11 security concept by a key hierarchy. Either a manually chosen Preshared Key (PSK) or an Master Session Key (MSK) delivered by a central Authentication Server (AS) provides the source to derive the Mesh Distributor PMK (PMK-MKD) and Key Distribution Key (KDK). The latter one enables secure key distribution and management. The PMK-MKD provides keying material for mutual authentication of Mesh Points (MPs). Lifetime of all keys cannot exceed the validity of PSK or MSK and need to be periodically renewed.

For secure operation, each Mesh Basic Service Set (BSS) has one Mesh Key Distributor (MKD) and one or more Mesh Authenticators (MAs). An MP may implement none, solely the MA or both key holder functions. An MP that has discovered a candidate peer MP, performs an initial Mesh Security Association (MSA) authentication with an MA. Once the MP is part of the Mesh BSS, it has the necessary keys to authenticate with other candidate peer MPs.

VII. 802.11s – Link Management

Mesh Points (MPs) use passive or active scanning to discover the candidate peer MPs. With passive scanning, MPs listen for beacon frames. Active scanning includes transmission of probe request frames. Once an Mesh Link (ML) has been established, the peer MPs calculate its airtime cost c_a. It depends on

- Channel access overhead O_{ca} (depending on Modulation and Coding Scheme (MCS)),
- Protocol overhead O_p (depending on MCS),
- Number of bits B_t in a test frame (depending on MCS),
- MCS bit rate r and,
- Frame error rate e_f for the test frame.

The default airtime metric is calculated as $c_a = [O_{ca} + O_p + \frac{B_t}{r}] * \frac{1}{1-e_f}$. Vendors may define other metrics that depend on other or additional properties. As path selection protocols use the airtime metric to calculate the best path to a given destination, only a single airtime metric is used in a Mesh Basic Service Set (BSS).

VIII. 802.11s – Path selection

Finding of an optimal route in layer-2 is denoted as path selection. Although the 802.11s framework allows multiple

path selection protocols being implemented in an MP, only one is active in a Mesh BSS at any time. Any MPs must implement the Hybrid Wireless Mesh Protocol (HWMP). It relies on three different MAC Management protocol data units (MMPDUs):

- Path Request (PREQ),
- Path Error (PERR) and
- Path Reply (PREP).

Whenever an MP receives a path message that is to be forwarded, it adds the airtime cost c_a to the current path metric. Furthermore, the MP decrements the path message's Time to Live (TTL) field that is independent from the Mesh Medium Access Control (MAC) header TTL. HWMP operates in three different modes:

- The on demand driven path selection scheme operates similar to Ad-hoc On-demand Distance Vector (AODV) defined in the Internet Engineering Task Force (IETF) Mobile Ad-hoc Networks (MANET) working group.
- When building a tree, a specific MP in the Mesh Wireless Local Area Network (WLAN) becomes the root MP. It proactively sends
  - PREQ messages to maintain paths between all MPs and the root, or
  - Root Announcement (RANN) messages that enable MPs to build a path to the root on-demand.
- Null path selection indicates that the MP does not forward frames.

AODV and the tree-based modes may be used simultaneously. AODV is well described in [14], [15]. With HWMP's tree-based concepts, the root MP sends a broadcast PREQ message. If the PREQ contains

- a more recent sequence number, or
- a better metric to the root and the sequence number is similar to previously received PREQ messages

an MP updates its path table. Depending on the root MP's PREQ, an MP must or may reply with PREP frame. Once the root MP receives the PREP, a bidirectional Mesh path is established. To accelerate the process, intermediate MPs may inform the root MP. In contrast to PREQ, the RANN sent by the root MP solely updates each MP how to find the root. The Mesh path is still subject to be set-up on demand.

IX. Conclusions & Outlook

802.11s provides a mature framework for Wireless Mesh Networks (WMNs). The security and path selection mechanisms are robust and well developed. However, the standard Medium Access Control (MAC) in 802.11s cannot deal with the difficult radio environment and thus limits the performance to a low degree. The optional Mesh Deterministic Access (MDA) is a promising step forward towards a Mesh aware medium access scheme. Future designs need to consider spatial frequency reuse that provides further performance enhancement.

Our future work will present our simulation results and provides insight to the performance of 802.11s.

References

[1] G. R. Hiertz, S. Max, E. Weiß, L. Berlemann, D. Denteneer, and S. Mangold, "Mesh Technology enabling Ubiquitous Wireless Networks," in *Proceedings of the 2nd Annual International Wireless Internet Conference (WICON)*, Boston, USA, Aug. 2006, Invited Paper, p. 11. [Online]. Available: http://www.comnets.rwth-aachen.de

[2] G. R. Hiertz, S. Max, T. Junge, L. Berlemann, D. Denteneer, S. Mangold, and B. Walke, "Wireless Mesh Networks in the IEEE LMSC," in *Proceedings of the Global Mobile Congress 2006*, Beijing, China, Oct. 2006, p. 6. [Online]. Available: http://www.comnets.rwth-aachen.de

[3] *Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications*, IEEE Unapproved draft P802.11-REVma/D9.0, Rev. of IEEE Std 802.11-1999, Mar. 2007.

[4] *Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking*, IEEE Unapproved draft P802.11s/D1.02, Mar. 2007.

[5] G. R. Hiertz, T. Junge, S. Max, Y. Zang, L. Stibor, and D. Denteneer, "Mesh Deterministic Access (MDA) - Optional IEEE 802.11s MAC scheme - Simulation Results (IEEE 802.11 TGs submission)," Online, IEEE Computer Society, Melbourne, Victoria, Australia, p. 31, Sep 2006. [Online]. Available: http://www.comnets.rwth-aachen.de

[6] D. Kotz, C. Newport, and C. Elliott, "The mistaken axioms of wireless-network research," Darmouth College Computer Science, Tech. Rep. TR2003-467, Jul. 2003.

[7] "Mobile Ad-hoc Networks (MANET) Working Group," The Internet Engineering Task Force (IETF). [Online]. Available: http://www.ietf.org/html.charters/manet-charter.html

[8] G. R. Hiertz, L. Stibor, J. Habetha, E. Weiß, and S. Mangold, "Throughput and Delay Performance of IEEE 802.11e Wireless LAN with Block Acknowledgments," in *Proceedings of 11th European Wireless Conference 2005*, vol. 1, Nicosia, Cyprus, Apr. 2005, pp. 246–252.

[9] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "Understanding Congestion in IEEE 802.11b Wireless Networks," in *Proceedings of the IMC '05, 2005 Internet Measurement Conference*, ACM SIGCOMM. USENIX, Oct. 2005, pp. 279–292. [Online]. Available: http://www.usenix.org/events/imc05/tech/jardosh.html

[10] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, "Architecture and Evaluation of an Unplanned 802.11b Mesh Network," in *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, Association for Computing Machinery Special Interest Group on Mobility of Systems, Users, Data and Computing. New York, NY, USA: ACM Press, 2005, pp. 31–42.

[11] G. Anastasi, M. Conti, and M. Gregori, "IEEE 802.11 Ad Hoc Networks: Protocols, Performance and Open Issues," in *Mobile Ad Hoc Networking*, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds. Wiley, Aug. 2004, p. 480.

[12] G. Anastasi, E. Borgia, M. Conti, and E. Gregori, "Wi-Fi in Ad Hoc Mode: A Measurement Study," in *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*, 2004, pp. 145–154.

[13] *International Standard ISO/IEC 26907, Information technology–Telecommunications and information exchange between systems – High Rate Ultra Wideband PHY and MAC Standard*, International Organization for Standardization (ISO), International Engineering Consortium (IEC) International Standard ISO/IEC 26 907:2007(E), Rev. First edition, Mar. 2007. [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/c043900_ISO_IEC_26907_2007(E).zip

[14] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, Online, IETF Std. 3561, Jul. 2003, experimental. [Online]. Available: http://tools.ietf.org/html/rfc3561

[15] C. E. Perkins and E. M. Royer, "Ad-hoc on demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*. New Orleans, LA: IEEE, February 1999, pp. 90–100.