IEEE P802.11
Wireless LANs

Mesh Networks Alliance (MNA)

Proposal

IEEE 802.11s – MAC Sublayer Functional Description

IEEE 802.11s – Mesh WLAN Security

Date: 2005-06-15

Author(s):

Name	Company	Address	Phone	email
Guido R. Hiertz	ComNets, Chair of Communication Networks, RWTH Aachen University	Kopernikusstr. 16, 52074 Aachen, Federal Republic of Germany	+49-241-80-25-829	hiertz@ieee.org
Yunpeng Zang	ComNets, Chair of Communication Networks, RWTH Aachen University	Kopernikusstr. 16, 52074 Aachen, Federal Republic of Germany	+49-241-80-25-829	zangyp@ieee.org
Lothar Stibor	ComNets, Chair of Communication Networks, RWTH Aachen University	Kopernikusstr. 16, 52074 Aachen, Federal Republic of Germany	+49-241-80-25-829	lsr@comnets.rwth-aachen.de
Sebastian Max	ComNets, Chair of Communication Networks, RWTH Aachen University	Kopernikusstr. 16, 52074 Aachen, Federal Republic of Germany	+49-241-80-25-829	smx@comnets.rwth-aachen.de
Hans-Jürgen Reumerman	Philips Research Laboratories	Weißhausstr. 2, 52066 Aachen, Federal Republic of Germany	+49-241-6003-629	hans-j.reumerman@philips.com

David Sánchez	Philips Research Laboratories	Weißhausstr. 2, 52066 Aachen, Federal Republic of Germany	+49-241-6003-535	david.s.sanchez@philips.com
Jörg Habetha	Philips Research Laboratories	Weißhausstr. 2, 52066 Aachen, Federal Republic of Germany	+49-241-60-03-56-0	joerg.habetha@philips.com

Abstract

The Mesh Networks Alliance describes MAC layer enhancements to IEEE 802.11 to provide efficicient methods for Mesh WLAN. It offers a flexible design, which coexists with legacy 802.11 devices on a single channel. Furthermore, the Mesh Networks Alliance offers a security concept for distribution of secret keys.

Table of contents

Additional Supporting Material

Number	Name	Definition	Coverage (Yes/No)	Notes	References
AD1	Reference submissions	A list of IEEE 802 submissions related to the proposal, both documents and presentations.	Yes		• 11-05-0605-00-000s-mesh-networks-alliance-proposal.doc • 11-05-0600-00-000s-mesh-networks-alliance-proposal.ppt
AD2	Simulation and/or experimental methodology	Any proposal submission that includes simulation results must include a description of the simulation methodology used for mesh simulations. The simulation methodology documentation should provide enough information to, in principle, reproduce the simulation (e.g., including node positions, traffic and propagation model (including PHY assumptions), packet sizes, etc.).	Simulation results will be presented later		ComNets, RWTH Aachen University, WARP2 simulation environment

Coverage of Minimum Functional Requirements

Number	Category	Name	Coverage (Complete /Partial/ None)	Notes	References
FR1	TOPO_RT_FWD	Mesh Topology Discovery	Complete		
FR2	TOPO_RT_FWD	Mesh Routing Protocol	None		
FR3	TOPO_RT_FWD	Extensible Mesh Routing Architecture	None		
FR4	TOPO_RT_FWD	Mesh Broad-cast Data De-livery	Complete		
FR5	TOPO_RT_FWD	Mesh Unicast Data Delivery	Complete		
FR6	TOPO_RT_FWD	Support for Single and Multiple Ra-dios	Complete		
FR7	TOPO_RT_FWD	Mesh Network Size	Complete		
FR8	SECURITY	Mesh Security	Partial		
FR9	MEAS	Radio-Aware Routing Met-rics	None		
FR10	SERV_CMP	Backwards compatibility with legacy BSS and STA	Comlete		
FR11	SERV_CMP	Use of WDS 4-Addr Frame or Extension	Complete		
FR12	DISC_ASSOC	Discovery and Association with a WLAN Mesh	Complete		
FR13	MMAC	Amendment to MAC with no PHY changes required	Complete		
FR14	INTRWRK	Compatibility with higher-layer protocols	Complete		

MAC Sublayer Functional Description

This part of the document introduces and explains the mechanism of the MAC Sublayer.

MAC Architecture

The main target of the MAC layer in a Mesh Point is to provide access to the Distribution System (DS) with the aim of relaying data which originates from associated 802.11 stations or gateways (portals). Communication between different Mesh Points is either MAC internal management communication or the effect of a previous communication between a mobile 802.11 station and its Access Point.

The MAC protocol offers efficient support for single and multi radio Mesh networks. In a single radio Mesh network division between intra BSS traffic and intra DS traffic is done in time: Periods for the exchange of data between a Mesh Point and its associated mobile stations alternate with Periods intended for peer traffic between Mesh Points. Traffic in the first period is called AP traffic, whereas traffic in the second one is called mesh traffic. With multi radio Mesh Points one or more frequencies for AP traffic and one or more frequencies for Mesh traffic may be used.

To allow for an efficient usage of the radio resource, a solution for a single radio/single frequency Mesh network is much more complicated than a multi radio solution. The solution proposed here, is able to support single and multi frequency solutions. Without limiting the generality of our solution, a solution for single radio Mesh networks is presented here.

In the AP traffic period (ATP), the 802.11 DCF, 802.11e EDCA or 802.11e HCCA is used to access the wireless medium (WM) by Mesh Points and by stations. Thus, the ATP is compatible to non 802.11s stations. The mesh traffic period (MTP) uses the announcement of a CFP to silence any non Mesh Points (legacy 802.11 stations). Therefore, it can be structured differently to support the goals of the intra DS traffic, especially a good multihop performance. The mesh traffic period is explained in the chapter “Mesh Traffic Period”.

One MTP and one ATP together define the Superframe known from standard 802.11. A superframe has a fixed length of mSuperframeSize. The fraction of this superframe that is used for the MTP must be in between mMTPMinTime and mMTPMaxTime. The duration of the ATP is not restricted furthermore.

Silencing the 802.11 - Stations

According to standard 802.11, each CFP starts with the transmission of a beacon by the AP at Target Beacon Transmission Time (TBTT). Among other information, the beacon announces the duration of the Contention Free Period (CFP) in the Basic Service Set of the AP and the duration of the superframe. Thus the start time of the next CFP is defined too. All 802.11 respect the CFP as period during which no transmission may be initiated by any other station than the AP (Point Coordinator). Having learned from previous beacons all 802.11 stations will refrain from accessing the channel until they are either polled (if they are CFPollable) or the CFP ends. Furthermore, any station keeps in mind the start point of the next CFP, and will silence even if no beacon was received at the begin of the next superframe/CFP.

Since no station will access the wireless medium during the CFP without being polled by the PC, an Mesh Coordination Function (MCF), that is independent from legacy 802.11 contention, can be used during the CFP, see Figure 1. Every 2nd MTP starts with a beacon period (BP). During the BP every Mesh Point sends a beacon frame. In its beacon frame, it announces the start of a CFP to its associated stations including the start time of the next CFP. As all stations will respect the latter CFP, no special announcement is needed. Therefore only one BP (which can be considered as protocol overhead) is needed in two superframes. The missing BP is indicated by the term “Ghost Beacon Period” (GBP) in which the stations expect a beacon, but do not get one.

It is important to notice that during the ATP following the MTP with the GBP, each AP has to send a beacon to announce the beginning of the upcoming MTP.

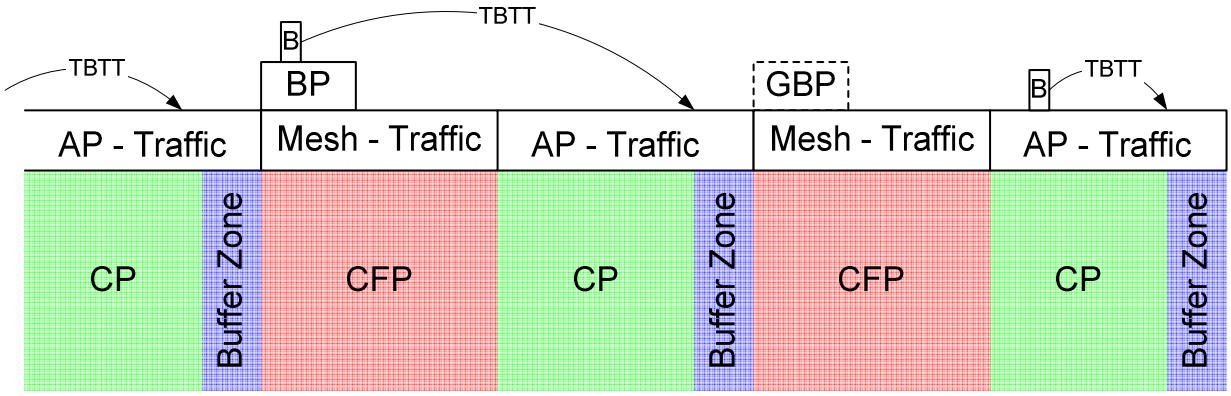


Figure 1: Alternation of AP – Traffic and Mesh - Traffic

Using the CFP as a means to allow a mesh specific protocol needs special care. In non 802.11s, a situation called a "foreshortened" CFP can happen: Stations may start a transmission before the CFP, even if the transmission takes longer to finish than the rest of the CP. Therefore, the 802.11 AP may sense a busy medium at TBTT which marks the start of the CFP, and refrains from sending the beacon until the transmission ends. This behaviour shortens the CFP by the delay; therefore, it gets "foreshortened".

A "foreshortened" MTP is not acceptable in the mesh network, since there might be stations that did not hear the "disobedient" mobile station because of their distance. These stations will start the MTP as scheduled. Hence, the starting point becomes unsynchronized. To guarantee an idle medium at the beginning of the MTP, the TBTT is announced to be a small moment before the real start. This buffer zone has exactly the duration of a maximum sized packet send at the basic PHY mode, so that the "disobedient" station will stop sending before the MTP. APs may send traffic in the buffer zone, using the 802.11e EDCA to avoid collisions with other APs. Therefore, Channel time is not wasted, and the APs will take care of stopping the transmission at the start of the MTP.

Mesh Traffic Period

In the MTP all Mesh Points use the mesh coordination function (MCF) to share the medium. Two subsequent equal length periods, the first starting with a BP, the other one with a GBP, are connected with each other by the BP in which the coordination of the remaining time is done. A proposal of their length is stated by each station in an IE in its beacon, any station will use the maximum of the proposed values. The proposal does not affect the current pair of MTPs, but the following one, as the silencing of the associated stations is done with the "old" value.

The MCF divides the two periods into several transmission opportunities (TxOPs, known from QoS supporting amendment 802.11e) of mTxOPLength and provides a protocol to acquire the ownership of one or several TxOPs. The negotiation of ownerships is performed by the including of information elements in the BP.

After a few BPs, the negotiation of a TxOP ownership is finished, which results in an agreement between the new owner of the TxOP and the intended receivers. The agreement ensures that the receivers are listening for a transmission from the owner during the TxOP.
All other stations in the neighborhood of the owner and the receivers will respect the agreement and therefore

- refrain from being sender if that could disturb the owner's transmissions
- refrain from being receiver if the sender could disturb the owner's transmission

An ownership of a TxOP guarantees therefore the best possible chance of a successful transmission during this time. The negotiation process, which is performed using the BPAP, is explained in the section "TxOP Negotiation".

The time flow during one mesh traffic period from the viewpoint of one station is drafted in Figure 2.

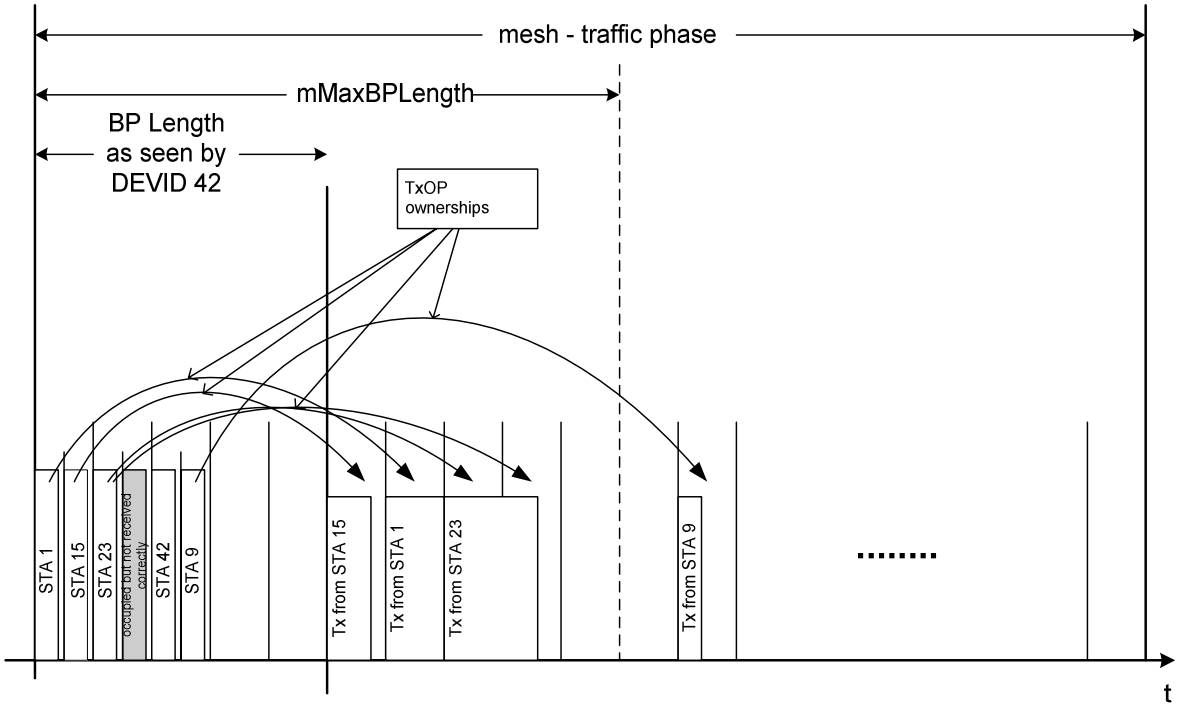


Figure 2: Structure of the mesh – traffic period, including the BP and TxOP ownerships

At the beginning of the traffic period, each Mesh Point sends a beacon, in which it states the ownership of one or more of the following TxOPs, which have already been negotiated. After the BP, the owners may transmit in the appropriate TxOPs.

Once a Mesh Point is the owner of a TxOP, it may use the given time for sending data to the previously announced receivers. This data falls into one of the following categories:

- Payload from the sender's BSS to another BSS
- Relayed payload from a different BSS to another BSS
- Positive or negative acknowledgement of previous data receptions
- Information Elements addressed to the receiver only

In one TxOP, the owner combines all data it plans to send during this TxOP into one large MPDU, which is called a "train" due to its structure: In the MPDU, several data packets are aligned in a row, divided by internal information like CRCs, and send by the owner as one long packet. This is known as frame aggregation from the proposal of TGnSync to Task Group 802.11n and further enhanced here. As there may be multiple receivers in a single TxOP, the long packet can be logically divided into a header, which is send at the basic PHY mode and describes the following structure, and several wagons of different size, which are addressed to the different receivers and may be send at different PHY modes. The construction of a train and other related topics including the acknowledgments are discussed in the section "Transmission Procedure".

To sum it up, the MTP falls into three building blocks: The beacon access protocol (section "Beacon Period Access Protocol"), the TxOP ownership negotiation (section "TxOP Ownerships") and finally the data transmission during the owned TxOP (section "Transmission Procedure").

Device IDs

The expected number of Mesh Points in a typical scenario, for example a campus environment, is typically less than or equal to 32. Therefore, a six octet field (like it is used in 802.11) for addressing traffic between Mesh Points is not needed. As long as it can be ensured that every Mesh Point in the mesh network has its own unique identifier, a shorter identifier may be used. The source and the destination of a data packet in the network are still addressed using the common address. However, any intermediate Mesh Point uses a mDevIdBits bit Device Id (DEVID) as the transmitter and the receiver address during the MTP.

Before selecting a random Device ID, a new Mesh Point listens to the current traffic and collects all IDs from the beacon period access protocol, so that conflicts with stations in the neighbourhood and also with stations in the neighborhood's neighbourhood are avoided.

Note: All other conflicts are not harmful, as the DEVID is only needed for forwarding traffic, and therefore the uniqueness in the neighbourhood of all neighbors suffices.

Beacon Period Access Protocol

Every 2nd MTP starts with a beacon period. It is used to silent non Mesh Points (non 802.11s stations) by starting a CFP. Further it is used to organize the traffic in the rest of the MTP and in the next MTP, which starts with a GBP.

The Mesh Coordination Function shares the wireless medium between the Mesh Points. It is organized as follows. During the BP the beacon period access protocol (BPAP) is used. The BP is segmented into small slots. The status of each slot is disseminated in the near neighborhood. This is done to lower the probability of a collision of two beacons from different Mesh Points in the same time slot. The dissemination is done over a three hop distance. The reason for this is explained using Figure 3:

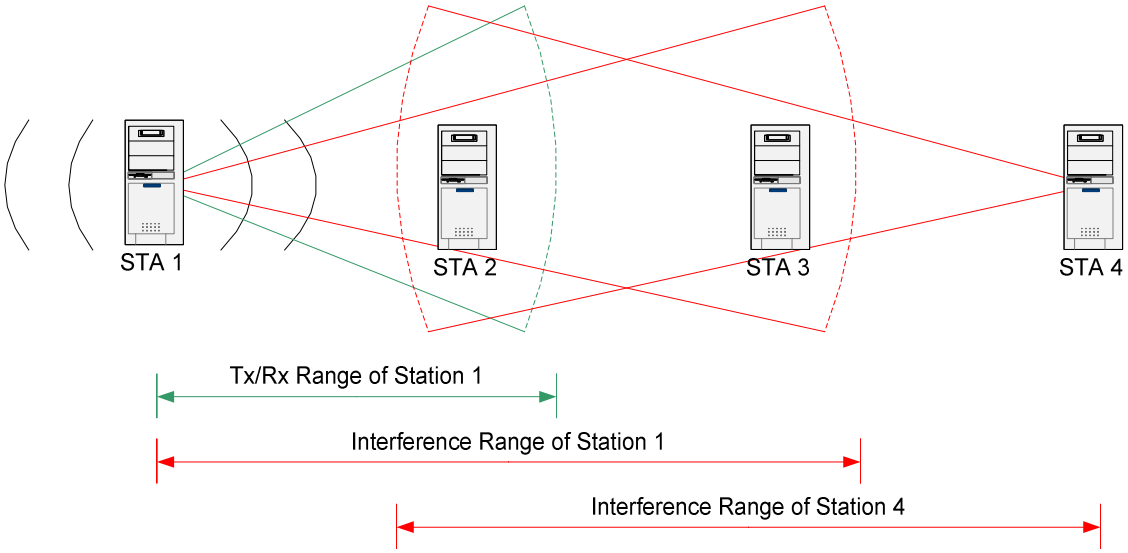


Figure 3: While Station 1 sends a beacon, the beacon period access protocol has to avoid interference by station 4

Here, the situation on the wireless medium is shown during a beacon slot which is occupied by Mesh Point "1". All stations (802.11s Mesh Points and non 802.11s stations) in the transmission range of a Mesh Point must correctly receive the beacon frame of Mesh Point. A beacon collision may occur at a receiving station if a Mesh Point (like station 4) would transmit a beacon in the same time interval. To prevent beacon collisions, the beacon period occupancy information element (BPOIE) in every beacon

informs neighboring Mesh Points about when a beacon will be send or received. The BPOIE has four possible entries per beacon slot, which have one of the following meanings:

- The beacon slot is occupied by the sending Mesh Point.
- The Mesh Point knows about a blocked Beacon Slot. It must listen to a neighbor which occupies this beacon slot.
- The Mesh Point will receive interference during this beacon slot and therefore cannot guarantee reception in this slot.
- From Mesh Points point of view the beacon slot is free.

In the scenario in Figure 3, Mesh Point "1" sets the beacon information to beacon slot type 1. Mesh Point "2" sets it to type 2, and so on. Mesh Point "2" propagates this information in its beacons. As station "4" receives the interference information about this slot from Mesh Point "3", it knows that it shall not send in this slot, because

- Mesh Point "3" might not be able to receive the beacon successfully, or
- the beacon may collide with another beacon.

This method of collision avoidance is called virtual clear channel assessment (V-CCA). In contrast to this, the stations can also use the traditional physical clear channel assessment (P-CCA), which is done by sensing the strength of occurring transmission in a beacon slot in one BP and marking the slot as used if a threshold of mBPNoiseThreshold is exceeded.

In the following paragraphs, the detailed implementation of the BPAP is explained, including the beacon structure, the process of joining and leaving the BP, the detection of collisions and the contraction of the BP.

Beacon Period Timing Structure

During the BP, time is slotted into intervals of mBPSlotLength length. Any transmission of a beacon has to start at the beginning of an interval. mBPSlotsPerTxOP subsequent intervals have the same size of a TxOP. The duration of the BP must be a multiple of a TxOP.

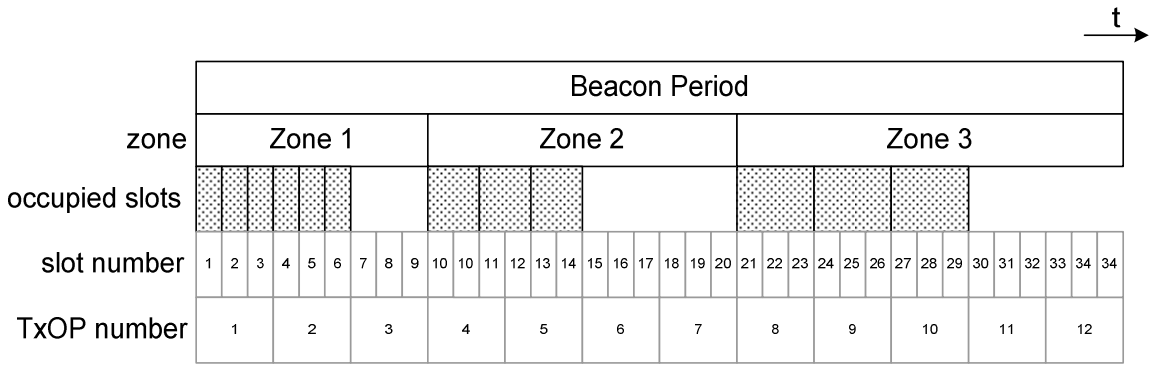


Figure 4: The detailed structure of a beacon period with three zones

As one beacon can occupy several subsequent beacon slots, beacons of the same size are ordered in their dedicated zone. In zone number "i", only beacons of the length "i" times mBPSlotLength are allowed. Zone "i" ends with the end of a TxOP, furthermore there have to be "i" * mFreeSlotsInZone at the end of each zone, which allow new Mesh Points to join the BP by sending a beacon in these free slots. The owner of the first beacon in the subsequent zone is responsible for freeing his slot if the number of free slots in the previous zone falls below this number. If the number of free slots in the last zone is below the minimum, the beacon period grows by the required number.

If a Mesh Point wants to send a beacon in a zone which does not exist, it sends a beacon in the next smaller zone, indicating the creation of the new zone in its BPOIE.

A possible beacon period is shown in Figure 4. In the configuration chosen here are three slots per TxOP and mFreeSlotsInZone equal to 2.

The maximum length of the beacon period is limited to mMaxBPLength TxOPs, but may be considerable smaller, and may even differ in separated areas of the mesh network.

Any Mesh Point that wants to transmit or receive data in the upcoming traffic period has to send at least one beacon in the beginning of an unoccupied beacon slot and listen to the neighbor's beacons.

It is possible for any Mesh Point to send more than one beacon in the BP as long as different information is transmitted in each beacon. It is recommended that the Mesh Point tries to send its information in one beacon of appropriate size in the proper zone, creating a new zone if needed. Each transmission has to end with a guard time of at least mTimeBetweenBeacons before the next beacon slot starts.

Note: Alternative Beacon Timing Structure

The BP Structure can be simplified by dropping the idea of different zones for different length beacons, but this inevitably complicates the BP Contraction.

As an alternative proposal for the BP, we consider an arbitrary alignment of the beacons during the BP. If a Mesh Point stops sending beacons, a gap of one or several continuous slots is created, which should be filled by existing beacons either by sliding (if the beacon is situated directly after the gap) or by jumping. To be efficient, large jumps shall be preferred over several consecutive small jumps. This can be done by a last-come-first-served strategy during the processing of the intentions to change to this beacon slot: The Mesh Point that sends the last beacon in the BP in which it announces the new ownership of the free slots will get the slots.

Beacon Contents

The beacon carries two important information: On the one hand, it transports information elements which are used to coordinate the beacon period access protocol and the traffic period. On the other hand, associated 802.11 stations must be capable of understanding the beacon structure to identify the start of a CFP.

To supply the latter functionality, the beacon structure must comply with the structure defined in [IEEE Wireless LAN Edition, 7.2.3 Management frames ff], which is repeated shortly in Figure 5.

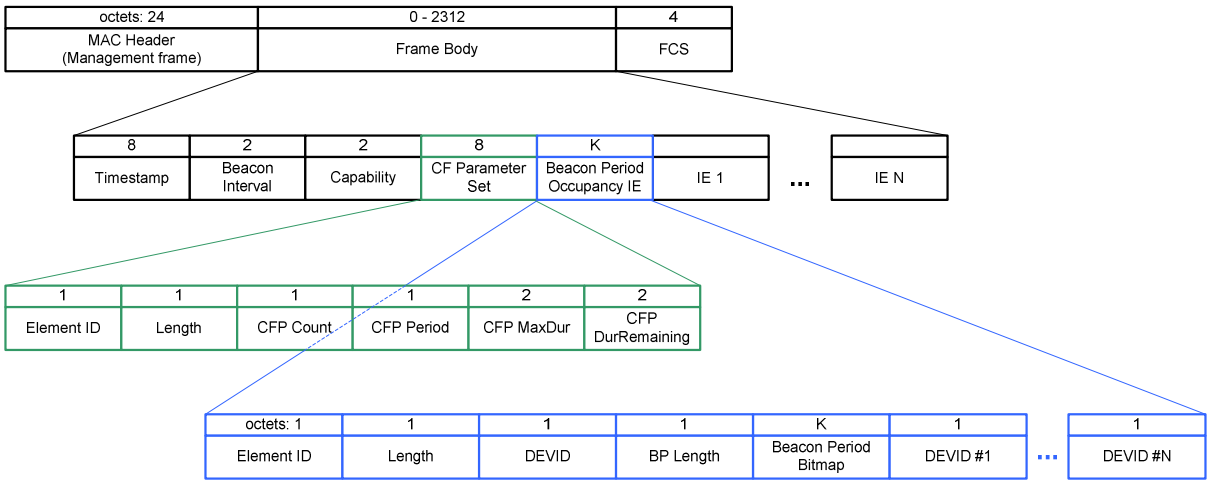


Figure 5: The standard 802.11 beacon with a CF Parameter set and a BPOIE

As every beacon send by a Mesh Point starts a CFP, it has to include a CF – Parameter set, which silences the associated stations for the current and the next MTP, which starts with a GBP.

The beacon period occupancy IE (BPOIE) is responsible for the beacon period access protocol and the dissemination of the BP slot status in the mesh network. The entries in the BPOIE are explained in the following paragraphs.

BP Length

The BPLength field is used to indicate a Mesh Point's view of the current length of the BP, which is the number of TxOPs that it will listen for beacons before starting to transmit or receive data in the MTP. As it is important to synchronize the BP Length in the neighborhood, it is calculated as the maximum of

- the last heard traffic in the last BP,
- the last occupied slot as reported from the received beacons in this BP,
- the last occupied slot as reported from the received beacons in the last BP

plus the appropriate number of free slots which can be calculated recognizing the number of zones (by the extension slots of each zone) in the last BP. The BP Length shall never grow larger than mMaxBPLength.

BP Bitmap

In any beacon send, a device announces its view of the occupancy of the BP, which is done by sending a BP Bitmap of the size 2 * mBeaconSlotsPerTxOP * BPLength bits. If the end of the BP Bitmap does not fall together with an end of an octet, the BP Bitmap is filled up with zeros which are not interpreted by any Mesh Point. The information inside the BP Bitmap shall be as fresh as possible, e.g. incorporating information of the BP Bitmaps of beacons that have been just received.

Each bit double inside the BP Bitmap corresponds to exactly one beacon slot. The bits inside the double express the occupancy of this slot as seen by the sending Mesh Point. The four possible combinations and their meaning are given in Table 1.

Table 1: The four possible beacon slot states, as indicated in the BP Bitmap

Element value (b1b0)	**Beacon slot interpretation**
00	**Free slot** The currently transmitting Mesh Point can receive beacons here.
01	**Occupied by sending Mesh Point** This slot is occupied by the currently transmitting Mesh Point and this Mesh Point has sent/is sending/will send a beacon in this slot.
10	**Occupied by neighboring Mesh Point** This slot is occupied by a neighboring Mesh Point, and the Mesh Point currently transmitting has successfully received a beacon in this slot or expects to receive one if it refers to a slot in the future.
11	**Occupied by neighbor's neighbor Mesh Point** This slot is occupied by a Mesh Point which is • a neighbor's neighbor but not a direct neighbor or • out of the receiving range but still creates noise. The Mesh Point expects that a beacon send to it will not be decoded successfully because of the existent interference.

The BP Bitmap is build up internally during the BP, incorporating new information while beacons are received. In each transmitted beacon the freshest BP Bitmap is send.

Owner Vector

In any beacon send which has a BP Bitmap with entries set to 10 or 11, an owner vector must be send after the BP Bitmap. The owner vector consists of mDEVIDBits bits for each entry set to 10 or 11 in the BP Bitmap, and indicates the DEVID of the appropriate Mesh Point. If the DEVID is unknown to the sending Mesh Point (which may happen only if the entry is set to 11), the DEVID is zero.

Beacon Transmission and Reception

After a Mesh Point is powered up, it scans for beacons in mScanBeacons subsequent BPs. If the device received no valid beacons after the scan, before it is to transmit or receive any frames, it creates a new BP by sending a beacon in the first beacon slot in the BP.

If the device received one or more valid beacons during the scan, it does not create a new BP. Instead it builds up an internal occupancy map (IOM) which is updated with every beacon received. The internal occupancy map is a bitmap consisting of mMaxBPLength bits. Each bit corresponds to a beacon slot in the BP. A bit is set to one if and only if the Mesh Point

- is the owner of this slot, which requires that it has send a beacon in this slot before, or
- has received a beacon in this slot, or
- has received a beacon with a 01, a 10 or a 11 in the corresponding entry in the BP Bitmap.

Otherwise, the bit is set to zero.

Using the occupancy map (and the information about the zones which can be computed from the received beacons), the Mesh Point sends a beacon in the first slot(s) marked zero in the zone that corresponds to the length of the beacon to be send. If the appropriate zone does not exist, the Mesh Point creates a new zone by sending a beacon in the last free beacon slot.

If a device detects a beacon collision as described in the next section, it shall randomly choose another slot which is marked zero in its IOM.

Beacon Collision Detection and Resolving

Let the Mesh Point with the DEVID “x” send a beacon in the beacon slot “j” in the BP “n”. The station shall consider the beacon to be transmitted successfully if and only if in all beacons received by neighboring Mesh Points in the following BP entry “j” in the BP Bitmap is set to “10” and the corresponding entry in the Owner Vector is “x”, or the entry “j” is set to “00”.

If the beacon cannot be considered successful, the Mesh Point is involved in a beacon collision and shall choose randomly another free slot using its IOM.

BP Leaving

If a Mesh Point wants to free one of its beacon slots because the amount of its beacon information has reduced, it shall free its last beacon slot in the BP. It shall furthermore announce its departure by sending a last beacon in the slot where this slot is marked as 00 in the BP Bitmap.

BP Contraction

If a Mesh Point is according to its IOM the last beacon holder of a zone and there are slots in the same zone which are marked as free, the Mesh Point shall shift its beacon to the free slots by the following procedure. If “j” is the number of the free beacon slot, it shall

1. transmit a beacon in the original slot with slot “j” set to “01” in the BP Bitmap
2. transmit a beacon in slot “j” in the next BP
3. transmit a departure beacon as described in “BP Leaving” in the original slot

Figure 6 shows an example of beacon shifting: First the slot “3” is sensed free by the Mesh Point with DEVID “8”, furthermore it knows that it is the Mesh Point sending the last beacon in the BP. Therefore it tries to occupy slot “3” by reserving the slot in Figure 6b. In the next BP, it is can send its beacon in slot “3” and announce its departure in slot “10”. Finally, in Figure 6d the shift is completed successfully.

It is possible that the extension zone and therefore the beginning of the next zone or the traffic period shifts after a shifting of one or more beacons.

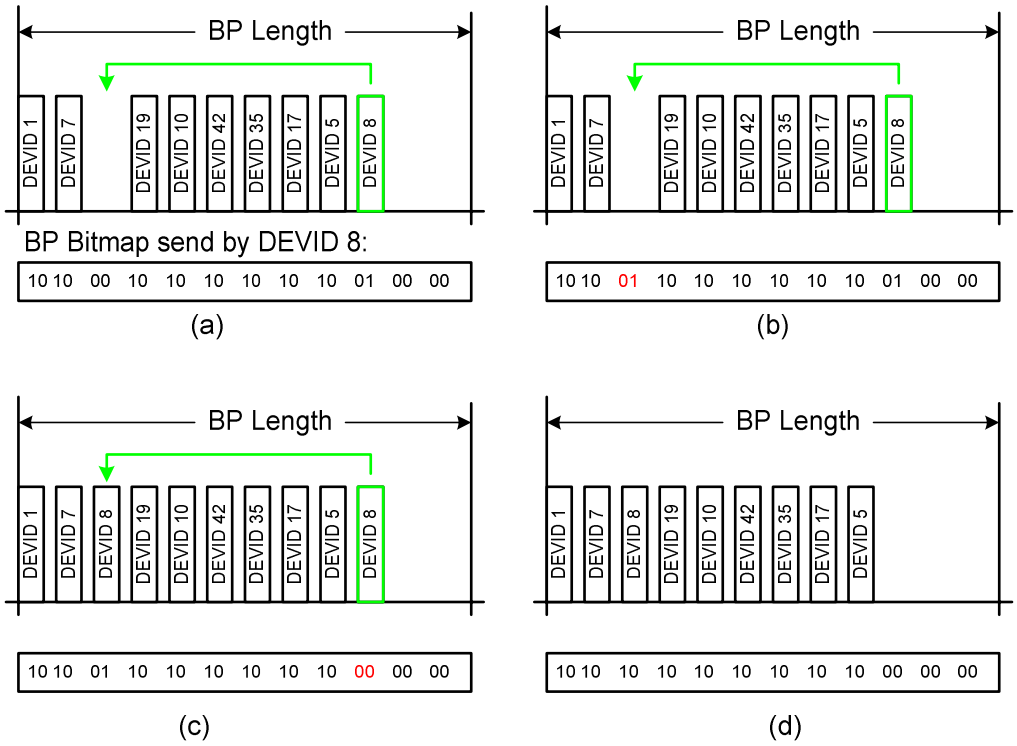


Figure 6: The four steps of a BP Contraction

TxOP Ownerships

Using the beacon period access protocol, any Mesh Point can send information elements (IE) to its neighbors, which can be used to negotiate the ownership of the upcoming TxOPs in the current and the next MTP. The previous negotiation of the TxOP is important because it makes the usage of the wireless medium predictable, giving Mesh Points the exact knowledge about which neighbor is transmitting and which is receiving at which point in time.

This knowledge enables several advantages in comparison to a random access protocol. One of them is the low probability of collisions: When the negotiation is finished, the owner of the TxOP can be sure that the channel will not be used by any Mesh Point which could interfere with the transmission.
Another important aspect of the improved knowledge is the easy ability to plan simultaneous transmission between pairs of Mesh Points that would not be feasible under other circumstances. More about simultaneous transmissions can be found in the chapter “Multihop Extensions”.

TxOP Negotiation

The occupation of a TxOPs is negotiated between the sender (which becomes the owner of the TxOPs if the negotiation is successful) and the receiver. To accelerate the process, it is possible to negotiate several TxOPs in the same time. Furthermore, a TxOP can have up to mMaxNoOfReceivers receiving Mesh Points. This allows a transmitter to maximize the usage of a slot. A TxOP ownership may therefore be multi-TxOP and multi-receiver, but it can have only one owner.

The negotiation of new occupations is done by including special TxOP ownership information elements (OIE) in the beacons of the participants. Additionally, an Availability IE might be included before or during the negotiation to improve the speed of finding TxOPs that are free for all participants. The structure of an OIE is drafted in Figure 7; the meaning of the different fields depends on the step of the negotiation.

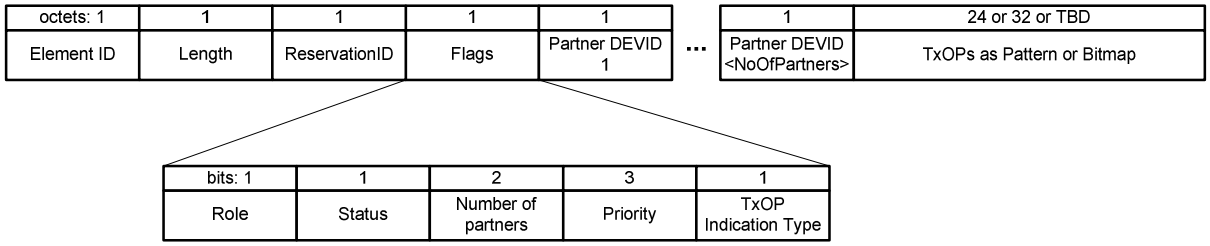


Figure 7: Structure of a TxOP Ownership IE

All active Mesh Points that listen to beacons have to process the OIEs to build up an internal traffic period occupancy map. In this map, a Mesh Point marks slots as occupied or free, and if it is occupied it additionally stores

- The owner of the slot, which is the Mesh Point that wants to transmit in the slot.
- The receivers of this slot which expect to receive data from the owner during the slot.

A slot is marked as occupied if

- A OIE is received in which it is marked as "occupied"
- Noise is sensed in this slot during the previous MTPs which is above mNoiseThreshold

The negotiation can roughly be seen as a two way handshake between the transmitter and the receiver(s). In the first step of the handshake, the transmitter proposes some TxOPs, in which it intends to send data. This is followed by the receiver's reply, which either finishes the negotiation by fixing the announced TxOPs, or by declining the proposal and thus restarting the negotiation.
By indicating the status of the negotiation in the status bit of the OIE, all neighboring Mesh Points know if the negotiation has finished and they have to respect the ownership, or if it is only proposed and therefore not obligatory. In the latter case the TxOPs can be reserved by themselves the ownership of TxOPs is done in a first come, first served way. This also means that if one TxOP has been reserved by two Mesh Points in the same BP, the earlier beacon wins the TxOP.
Because of the two way handshake, the ownership negotiation has also a similar function as the 802.11 RTS/CTS procedure as it signals an occupation of the channel. However, it is more efficient because of the possibility of occupying several TxOPs in one handshake.

In detail, if a Mesh Point wants to own slots in the MTP, it starts the negotiation process by choosing a suitable pattern of free slots (as marked in the internal map), probably including previous heard Availability IEs of the receiver(s) in the computation, and includes a OIE in its next beacon indicating the chosen TxOPs, the DEVID(s) of the intended receiver(s), its role in this reservation ("transmitter") and the status of the ownership ("announced"). The ReservationID shall be set to a randomly chosen value that is currently not used for this set of receivers.
Any active device scans all beacons of the BP for the occurrence of its DEVID in an OIE where the role is set to "transmitter". If such an OIE is received the device checks if the ReservationID is already in use, a new ReservationID indicates a new negotiation. The intended receiver evaluates whether it can acknowledge the announced ownership, which is the case in the following situations:

- The medium is free during the announced TxOPs according to the locally stored information, or
- The new reservation has a higher priority than the reservation(s) occupying the intended slots, or
- A parallel transmission as explained in "Multihop Extensions" is possible with high probability.

A higher priority reservation is allowed to take over some, but not all slots of an existent lower priority reservation.

A receiver acknowledges an OIE by including an OIE in its own beacon with the following parameters:

- The indicated TxOPs and the ReservationID are the same as in the transmitter's OIE
- The Partner-ID is the transmitter's DEVID
- The role is set to "receiver"
- The status of the ownership is set to "occupied"

In case of a multiple receiver transmission, which is indicated by several receivers in the transmitter's OEI, the receiver should include an Availability IE in the OIE to shorten the negotiation process in case the other receivers cannot accept the proposed slots. The Availability IE shall be included until a RIE send by the transmitter with the status "reserved" is received.
A receiver may change a proposed ownership by answering with an ownership status of "announced". If possible it should also propose an alternative reservation by setting the reserved slots in the REI and by including an Availability IE, which can be used by the transmitter to compute a successful reservation.

The transmitter has to keep sending its "announced" occupation until it has received an answer from all intended receivers or for mTryReservations beacon periods, depending on what occurs first. In the second case, the transmitter must cancel the reservation.

After the transmitter has collected acknowledging OIEs from all intended receivers the negotiation has finished successfully and the transmitter becomes the owner of the TxOPs, and all other Mesh Points in the neighborhood which have overheard the OIEs have to respect this ownership. The intended receiver(s) have to listen during the reserved slots for data transmissions.

If an intended receiver of the RIE in the initiating beacon finds out that the proposed slots are occupied and no other slots can be reserved, or if the device is not willing to accept the reservation for any other reasons, it shall send a RIE in its next beacon with

- The DEVID set to the transceiver's DEVID
- The ReservationID set to the ReservationID of the initial OIE
- The role set to "receiver"
- The status of the ownership set to "announced"
- The reservation information set to zero

Such a RIE shall be interpreted as a declining of a reservation and the initiator shall not re-initiate the reservation negotiation with this receiver.

Maintaining the ownerships

After a successful negotiation the participating Mesh Points keep including an OIE in their beacon that indicates the occupied TxOPs and has the status set to "occupied". All other devices that receive these beacons honor this negotiated ownership.

In case that the owner or one of the receivers wants to change the occupation, they can restart the negotiation process by sending an OIE with the new information and the old ReservationID, but with the status set to "announced". If a receiver initialized the restart of the negotiation, it should include an Availability IE in its beacon.

If a transmitter or a receiver wants to cancel an existing reservation, they send a cancelation OIE which consist of the same ReservationID and the partner's DEVID, the status "occupied" but the reservation information filled with zeros. All neighboring Mesh Points may delete this reservation from their internal occupancy map after receiving this special OIE.

Transmission Procedure

If a Mesh Point is the owner of one or several subsequent TxOPs during the MTP, which are not used as beacon period, it can transmit data during this time. The start time may be arbitrarily chosen, as long as the transmission ends before the beginning of the next reserved or unreserved TxOP. It is recommended either to start the transmission at the beginning of the first owned TxOP or to align it so that it ends simultaneously with the last owned TxOP, which could be helpful for simultaneous transmissions in the same TxOP, as it may shorten the duration of the interference.

The owner of a TxOP can use two different techniques to optimize the usage of the channel time:

- Frame aggregation

The owner may aggregate several MSDUs, fragments of MSDUs, control frames (like ACKs) and information elements into one single entity, dividing them by CRCs and giving their structure in a frame aggregation header. Frame aggregation as presented here is an enhanced version of the procedure defined by TGnSync for Task Group 802.11n.

- Multiple receiver MPDU

  The owner may send data to several different receivers during one transmission. It may also change the PHY mode during the transmission. The sequence and the duration of the different PHY modes are indicated in a header which is send in the basic PHY mode. Therefore, every receiver can compute the start time of its reception.

Therefore, the transmitter may send one multi receiver, multi mode frame during the subsequent TxOPs. This frame is called a "packet train", as it consists of a header and one or more wagons. Furthermore, each wagon is composed of a wagon header and one or more payloads, separated by CRCs. This structure is presented in Figure 8.

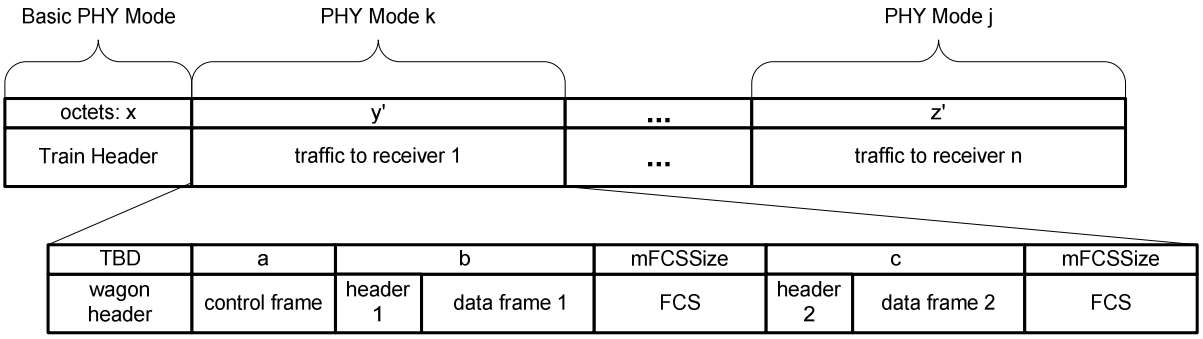


Figure 8: The general structure of a packet train, consisting of a header and several wagons

The intended receivers (as given by the reservation negotiation) listen to the train header and determine if one of the upcoming wagons is addressed to their DEVID. If so, it can compute its start time using the information given in the header.

The content of the train header is defined in section "Train Header", the construction of the wagons including the wagon header in section "Wagon Format".

Train Header

The structure of the train header is shown in Figure 9:

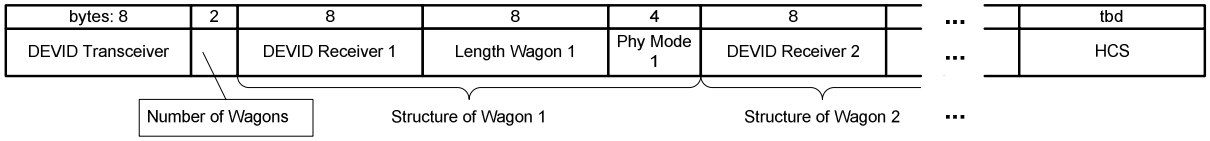


Figure 9: The structure of the train header

After the transceiver's DEVID, the number of wagons in the immediately following train is announced (up to mMaxNoOfReceivers), followed by a description of each wagon in the train, which consists of the receiver's DEVID, the length of each wagon in OFDM Symbols and the chosen PHY mode. The train header ends with a header check sequence.

In many scenarios it is possible that the receiver cannot decode every wagon successfully, especially if it is encoded in a fast PHY mode. Without loss of generality, an OFDM PHY layer is assumed in the following explanations.

An MP can always understand the symbol boundaries, and therefore stay synchronized to the transmitter. As the length is given in multiples of (OFDM) Symbols, it can compute the start point of its wagon and single it out in the appropriate moment

The maximum duration of a wagon is restricted by the length indicator of the train header, whose maximum value is 2^8 – 1, resulting in a wagon length of 765 octets (if BPSK½ is used).

Wagon Format

Wagon Header

The wagon header announces the payload of the wagon, which are either MSDUs, fragments of MSDUs or information elements that are intended to the receiver only. The header states the number of elements and the length in OFDM Symbols for each payload element.

Data Frame Format

Data frames transport the payload from the associated mobile stations through the mesh network, either to another mobile station or to a Mesh Point acting as a gateway or portal to another network. Likewise payload is transported from the gateway or portal to mobile stations. Therefore, the data frame format has to be adapted to the requirements and the standard of the legacy 802.11 format.

Consequently many of the data frame's field resemble the 802.11 fields: The frame control bits, the final destination/first source address, the sequence control and the frame check sequence. Because of this similar structure, the fields of a MPDU from an associated station, addressed to the mesh network, can be copied directly into the data frame.
This also implies that the sequence numbers and a previous fragmentation are not changed by any Mesh Point, which furthermore reduces the complexity, as a Mesh Point does not have to buffer fragments of a MPDU for a defragmentation before the relaying.

The structure of a data frame can be found in Figure 10.

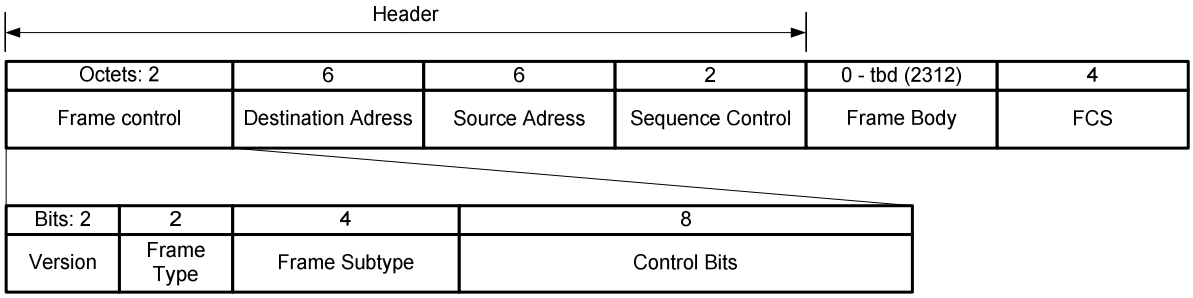


Figure 10: The structure of a data frame

Acknowledgements

The ACK frame is used by a receiver to report the successful or failed reception of a MSDU, or a segment of a MSDU respectively, which was send by a transmitter before. Because of the ownerships of TxOPs, the receiver is not allowed to send an ACK frame immediately after the reception of the data frame. In a multi reception TxOP this would be impossible. Furthermore, immediate acknowledgments would imply a change of the transceiver/receiver roles which is unpredictable for the neighboring Mesh Points.

Therefore, acknowledgements are handled in the same way as any data frames: A TxOP, negotiated between the receiver and the transmitter, has be occupied; the ACK frame can be send together with other frames using a packet train, preferably with frames targeted to the transmitter.

Consequently, the receiver might receive several data frames before it is able to acknowledge the first frame, especially if a suitable TxOP ownership by the receiver does not exist and has to be created first. Once a TxOP is owned, it can be used to send two different type of acknowledging frames:

- A cumulative ACK
  Sending a cumulative ACK, the receiver acknowledges all MSDUs (or fragments of MSDUs) that have been send to him up to, but not including the sequence/fragment number indicated in the

cumulative ÁCK. The transmitter may delete all MSDUs up to the indicated one from its sending queue.

- A bitmap ack
  The bitmap ACK is an explicit enumeration of the success or failure status of the last received packets. The sequence control field specifies the next sequence/fragment number of the next packet which is expected at the receiver, excluding packets that have already been send but were received with faults.
  The attached bitmap indicates the status of the MSDUs that have been received, it starts with the last successful MSDU (as indicated by the sequence control field – 1), for each sequence number two octets in the bitmap represent the status of up to 16 fragments of the corresponding MSDU. The last two octets in the bitmap stand for the MSDU with the lowest sequence number (in a modulo sense) that was not received correctly.

The transmitter may delete all MSDU fragments that are indicated as successful in the bitmap from its sending queue, as well as the MSDUs that have a lower sequence number than the corresponding number of the last two octets in the bitmap.
The combination of both ACK types inside one wagon directed to the transmitter is of course possible, but the bitmap ACK must anticipate the cumulative ACK; the content of the first one has precedence over the latter one.

In both ACK frame types the buffer size field indicates the amount of free space in the receiving buffer reserved for this particular transmitter, counted in bytes. This size indicator is used as a flow control mechanism to prevent the transmitter from overstraining the receiver. The transmitter may send only the given amount of bytes before it has to wait for the next ACK. Retransmission of the last frame by the transmitter or the receiver can be used to update this indicator.
Additionally, congestion control like schemes can be used by the transmitter to estimate the optimal number of packets he can send before waiting for the next ACK.

Note: In the case of a multi – hop route, the buffer size indicator might be useful to avoid bottlenecks.
A Mesh Point in an overload condition may signal its problem by lowering the free buffer size below the actual capacity, and therefore slowing down the neighboring transmitters.
A forwarding Mesh Point with enough capacity may use the free buffer size as told by the next hop to calculate its indicated free buffer size for the previous hop.
In this way, the information about a congestion would travel from the congested node back to the source.

Multihop Extensions

In contrast to the EDCA which is used in the AP traffic perdiod, the presented MCF allows an efficient multihop communication in the mesh network. The use of negotiated ownerships of equal length TxOPs result in a predictable medium access, as all neighboring Mesh Points are able to learn which Mesh Point plays which part during a TxOP.

This enhanced knowledge allows the MCF to allow a greater spatial reuse, which directly is followed by a capacity increase of the mesh network.

A simple example for the possibilities of spatial reuse can be found in Figure 11.

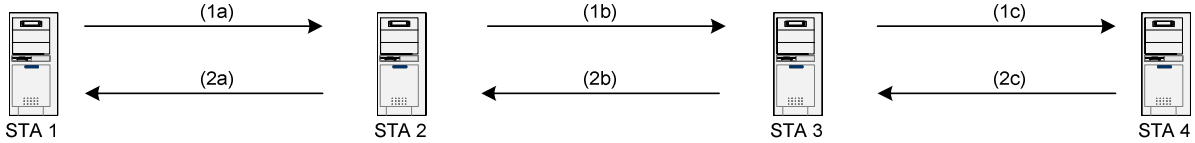


Figure 11: A simple scenario where spatial reuse is possible

Mesh Points “1” to “4” have their own BSS and probably several associated mobile stations. The mobile stations in the BSS of Mesh Point “1” generate traffic which is addressed to Mesh Point “4” (which is for example a gateway or portal to the internet), and Mesh Point “4” replies to the traffic.
As Mesh Point “1” and “4” are mutually out of reception range, they cannot communicate directly with each other. They must use two three hop routes via Mesh Point “2” and “3”, which is depicted as (1a-c) and (2a-c).
If Mesh Point “3” is able to guess that simultaneous usage of link (1a) and (2c) is possible because the interference created by Mesh Point “1” at Mesh Point “3” during the transmission is low, it may negotiate with Mesh Point “4” the number of used TxOP to be the same as they are used for the link (1a). The latter information is directly available to Mesh Point “3” via the negotiation procedure between Mesh Point “1” and Mesh Point “2”.
Similarly, links (1c) and (2a) can be used simultaneously, which results in a traffic/time diagram as given in Figure 12.

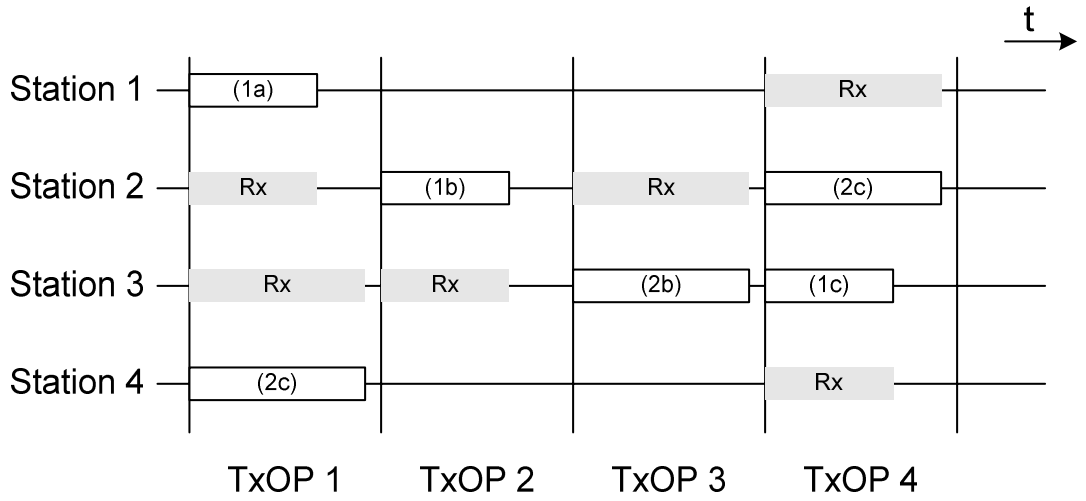


Figure 12: An optimal alignment of the transmissions during time for the scenario in Figure 11

The described scenario is an example for an optimal behavior of the Mesh Points which can be seen from an external observer, but it is not obvious how the Mesh Points can reach this behavior. The possible internal mechanisms of the Mesh Points are explained in the next section.

Learning Mesh Points

Before Mesh Points can take advantage of simultaneous transmission, they must learn a model of the current environment, called the world model. This world model shall be as simple as possible, abstracting from reality as much as possible. Also, it shall be as detailed as needed to give good estimations of the options of a specified transmission. The world model is updated continuously by the sensors of a Mesh Point, which are the receiving entity of the physical layer together with the information about the TxOP ownerships, received beacons, information elements and heard transmissions.

From time to time, a request for a new TxOP ownership or a change of an existent one arises in the Mesh Point, for example because a new traffic stream is started by an associated Mesh Point or a TxOP ownership negotiation request is received by a neighboring Mesh Point. This request is processed using the world model to find free TxOPs that suit the current status regarding the intended role (transmitter or receiver) and the priority of the traffic.
With this information, the TxOP negotiation process selects a suitable set of TxOPs and starts the negotiation process (or answers the request respectively), probably preferring TxOPs that lead to a simultaneous transmission.

The abstracted structure of a station which is able to adapt to the current interference can be seen in Figure 13.

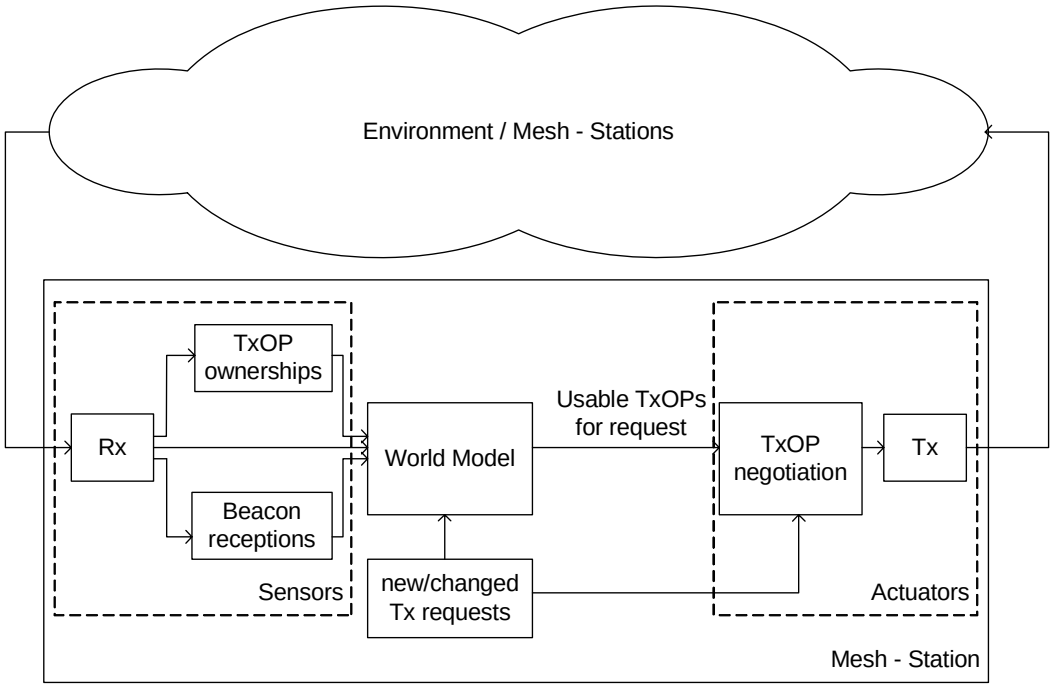
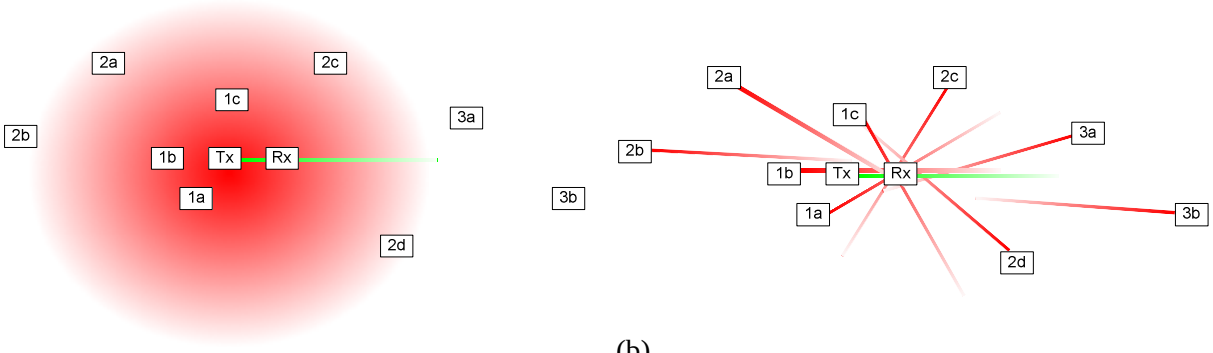


Figure 13: The general structure of an interference – aware Mesh Point

Measuring the Learning Performance

As the scope of this chapter is limited to the ability of simultaneous transmissions, this will be the only quality measure; other criteria that involve the optimal selection of TxOPs under fairness conditions or QoS requirements like throughput and delay are not discussed. Therefore, the algorithm which chooses and negotiates the TxOPs is handled as a black box which gets a set of TxOPs that could be suitable for a specified transmission to/from a Mesh Point, optionally combined with a rating of each TxOP. As a result, the performance of the learning algorithm can be measured by the number of "good" TxOPs it proposes to this black box, compared to the number of "bad" TxOPs.

To define the terms "good" and "bad" TxOP more precise, the Figure 14 is helpful.



(a) (b)

Figure 14: The measures of the signal strength if (a) Tx is transmitting or (b) Rx is receiving

Both subfigures show an example environment with 11 Mesh Points, two of them are marked as the transmitting and the receiving Mesh Point respectively. In the left figure, the transmission power of the transmitting Mesh Point is drawn in red color. Its strength is proportional to the distance to the Mesh Point. The right figure shows the transmission power of all stations in the environment as it is seen from the Rx Mesh Point. In both cases, a green line indicates the traffic from the Tx to the Rx Mesh Point.

The decision if a TxOP is "good" must be made regarding the desired role of the Mesh Point: If a Mesh Point wants to transmit, a TxOP is "good" if it does not disturb a simultaneous transmission by its interference. With the power that is indicated in Figure 14a, the transmitting Mesh Point would certainly infer with any transmission that is received at the Mesh Points "1a-1c". The impact on a reception in Mesh Points "2a-2d" would be much lower; a transmission from Mesh Point "2b" to "2a" should be no problem; whereas Mesh Points "3a-3b" would not sense anything from the transmission. Additionally, the effect of the transmission depends not only on the distance to the other Mesh Point, but also on the position of the simultaneous transmission's sender: It is less interfering if the distance from the sender to the transmitter is very small.
The second case, indicated in Figure 14b, would be if the role of the Mesh Point wants to receive. A TxOP is now called "good" if in the same time a simultaneous transmission creates only low interference at the receiver. This is for example the case if Mesh Points "2a-2b" or "3a-3b" are sending.

In the drafted environment some simplifications are made, as the shape of the signal strength may be more complicated than a circle around the sending Mesh Point. Furthermore, the shape may not be constant during time. Moving obstacles or different channel conditions can change the effects of a transmission.

The World Model

The task of the world model inside the learning Mesh Point is to represent the environment in the simplest way that allows a good prediction if a given TxOP is "good" or not. The detailed implementation of the world model, which also includes how the outputs of the sensors are used to update its state, is of course independent of the protocol specifications, and can be optimized to fulfill different aims; for example a trade off between the needed complexity, the used computational effort and the accuracy of the predictions must be made.

The world model is limited by the potential and the accuracy of the given sensors. An optimal model in the case discussed here would know the position of all Mesh Points in the network, as well as the link characteristics between them and the placement of any obstacles. This situation is of course out of reach, as some of the knowledge can only be obtained by much overhead traffic (for the mutual link characteristics) or is unachievable at all (like the obstacles).

The following world model is therefore only a proposal that relies on the described Mesh MAC protocol and some of the information that can be obtained as a side product of it.

It is derived from the fact that in wireless networks the success probability of a transmission is mainly determined by the ratio of the useful signal strength at the receiver versus the strength of the interfering signals. The two possible reasons for interference are the background noise and simultaneous transmissions. Therefore, this ratio, the Carrier over Interference (CoI), is measured as

$$CoI = \frac{C}{N + \sum I} \ .$$

C is the carrier's signal strength, N the current noise and the sum stands for the interference which is produced by other transmissions. Usually $\sum I >> N$, if a simultaneous transmission is existent; therefore, the noise can be neglected in the non trivial cases.

It is important to notice that two different CoI ratios have to be taken into account before a new, simultaneous transmission is started:

1. The receiver CoI

   This CoI reflects the success probability that the receiver of a simultaneous transmission is able to decode the signal in spite of the primary transmission.

2. The interference CoI

   By introducing a new simultaneous transmission, the transmitter creates a new source of interference for the primary transmission. Therefore, both Mesh Points of the new link have to avoid that this new interference is severe at the original receiver.

In this proposal, the current status of the world is represented by the signal strength graph, which is a complete graph G = (V, E) together with a weight function w: E -> N that connects an integer to every edge of the graph. Any Mesh Point that is recognized by a sensor (like the Rx entity or the beacon protocol) is represented as a node in the graph. The weight of an edge between two nodes (X, Y) is an estimation of the signal strength that is measured at node Y if node X is sending data. As the links between nodes are by assumption bidirectional, w (X, Y) = w (Y, X) and the graph can be undirected.

A simple example is given in Figure 15: The complete graph is given for the five Mesh Points Tx, Rx, 1, 2 and 3, and the signal strength is abstracted as an weight of the connecting edge.

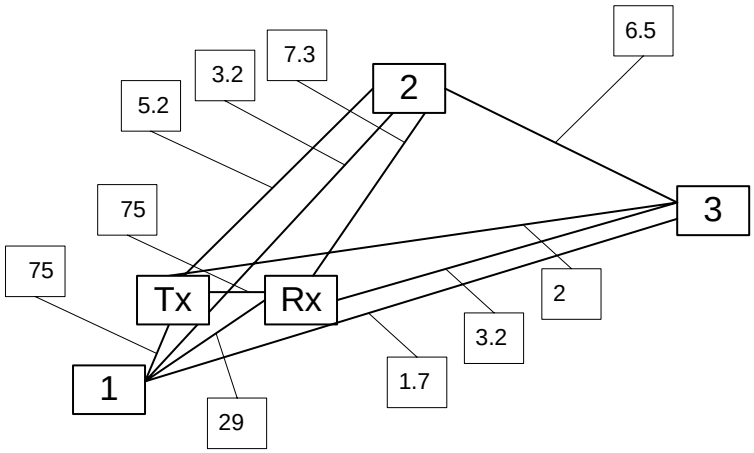


Figure 15: The signal strength graph for a scenario with stations Tx, Rx and 1 to 3.

Having well trained this world model in every Mesh Point, it approximates the current state of the environment. Then, Mesh Points possessing this graph can compute an estimation of the interference CoI during a simultaneous transmission from Tx to Rx. Furthermore, the model can support the computation of the receiver CoI at Rx.

The interference CoI is estimated by dividing the weight of the link that represents the simultaneous transmission by the interference that is produced by Tx (given by w (Tx, [receiver of the simultaneous transmission]). The higher the quotient of those two weights, the lower is the chance that Tx interferes with the transmission.
Similarly the receiver computes the value of CoI as the quotient of w (Tx, Rx) and the interference of the simultaneous transmission, which is represented by w (Rx, Sender of the simultaneous transmission). A high indicator would here also express a high chance of a successful reception.
Of course the method can be extended to multiple simultaneous transmissions or to multiple receiver transmissions.

An algorithm can compute the CoI for every possible simultaneous transmission and then rate all TxOPs given the information about the current ownerships using the ownership protocol as a sensor. Using this

graph, the outcome is a list of "good" TxOPs, which are likely to provide high success of reception and a low interference ratio to other transmissions in parallel. Furthermore, a threshold may be given which determines whether the computed CoI ratios high enough. Alternatively, the decision can be made based upon a (learnable) soft threshold function like the sigmoid function ($\frac{1}{1+e^{-x}} + Offset$).

The computed indicators for the transmission Tx to Rx in the given example graph can be seen in Table 2, all impossible pairs of transmissions (like Tx -> Rx and Rx -> 2 in the same time) are omitted.

Table 2: Interference CoI and Receiver CoI if a simultaneous transmission from Tx to Rx would happen

Transmissions in TxOP	Receiver CoI [dB]	Interference CoI [dB]
None	0	maximum
1 -> 2	4	-2
2 -> 1	10	-14
1 -> 3	4	-1
3 -> 1	13	-16
2 -> 3	10	5
3 -> 2	13	1

This table clearly shows that the transmission Tx -> Rx cannot be scheduled simultaneously to most of the other possible transmissions, perhaps only parallel to the transmission 2->3. A different case can be seen if the graph of the introduction example (Figure 11) is examined, which is given in Figure 16.

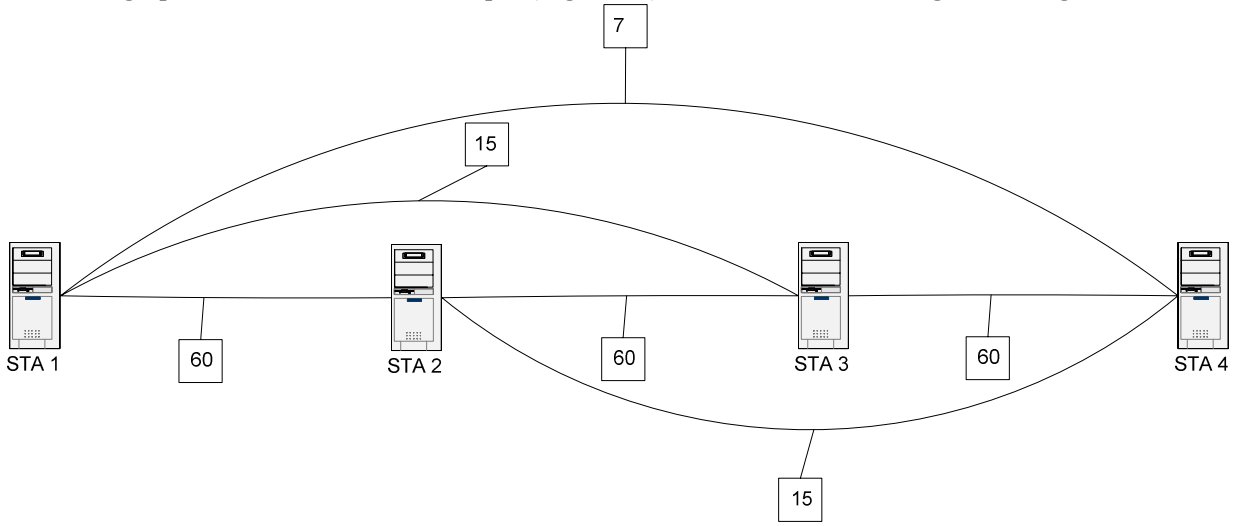


Figure 16: The signal strength graph for the scenario given in Figure 11

If the transmission from Mesh Point 4 to Mesh Point 3 is scheduled in a TxOP, the interference indicator for 1 -> 2 is 10*Log(60 / 15) = 6dB, and the reception indicator for 1 -> 2 is also 6dB, which may be rated as a "possible" TxOP if a slow PHY mode is used.

Before the possible methods of learning the graph and the weights are presented, it has to be noticed that the abstraction which is done in the world model incorporates easily all kinds of transmission technologies like directed antennas or MIMO devices: If they improve the receiver CoI ratio and/or lower the interference CoI, their performance is directly incorporated into the model.
Similar, the effects of obstacles like walls indirectly influence the graph and are therefore also incorporated.

The continuous learning of the graph can be divided into two separate tasks: First, the graph's structure (V, E) has to be learned, which is the identifaction of the network's participants. Second, the weights in

the graph are learned. Those two tasks are carried out continuously and with an adaptable speed, allowing the model to become a good approximation of the environment and reacting towards changes. The learning is made difficult by the insufficient and unreliable output of the three used sensors, as they are not made to fulfill the given task. A filtering of the sensor's output is therefore one of the most important subtasks of the learning process.

A last demand to the learning process is that it should recognize situations where its knowledge is insufficient to result good estimations for the two CoI values. In detail, it should be prevented that the interference CoI is overestimated and thus an existing transmission is disturbed.

Learning the Network's Participants

Recognizing other Mesh Points in the network can be done easily using the beacon period access protocol and by receiving other Mesh Point's traffic headers. From the beacon protocol, a Mesh Point can identify the beacon's sender, the sender's neighbors and the neighbor's neighbors, because each of them is announced in the owner vector of the BPOIE.

In the traffic during the MTP, each traffic train has an initial header which gives the structure of the following wagons, including the recipient of each wagon. Using this information, a Mesh Point can detect other Mesh Points by listening to the headers even if in the TxOP it is not a receiver.

Each occurrence of a Mesh Points's DEVID (either in the BP or during the MTP) can be seen as a "ping" indicating the Mesh Point being "alive". It is recommended that the Mesh Points are included to the graph the first time a "ping" was heard from them, they should be deleted from the graph with a probability that increases with the time no "ping" has been heard.

Learning the Signal Strength

For every new Mesh Point that is recognized, the weights to the other Mesh Points have to be estimated, which is done is several ways. Each sensor gives some hints how the weight should be set. The sensor's outputs are noisy and have to be filtered or weighted before they can be taken into account.

If the current graph consists of N Mesh Points, (N+1) * N/2 weights have to be estimated. Of those links, (N – 1) are directly connected to the learning Mesh Point. Therefore, they can be learned faster and with more confidence. It is noteworthy that in the interference and in the receiver CoI, three out of four needed weights are direct links of either the transmitter or the receiver; only one weight in the interference CoI is in a one hop distance of one of them, as this weight describes the signal strength of the primary transmission measured at the primary receiver. To avoid overestimating the interference CoI, the lower bound of this weight is crucial.

Learning (N – 1) direct links can be done by using the timing information in the beacon access period protocol together with some side information by the PHY layer. Using the BP, a Mesh Point knows the point in time when a neighboring Mesh Point is transmitting its beacon. Furthermore, because of the strict rules in the BP, it knows that no other near Mesh Point is transmitting during this time.
For each beacon slot, the PHY layer can measure the integrated signal strength, and then report this strength to the MAC layer, which combines this information with the BP access protocol to determine an estimation of the signal strength of a particular neighbor.

The weight on the link can now be computed using this estimation. The easiest solution would simply take the most current estimation, neglecting older values. Another, more intelligent solution would be a low pass filtering of the estimates to obtain a running exponential weighted average. If the newest measurement, obtained in the beacon period number t, is denoted as e_t, the running estimation $\hat{e}_t$ is computed as

$$\hat{e}_t = \alpha \cdot e_t + (1-\alpha) \cdot \hat{e}_{t-1}$$

with α as a parameter weighting the importance of new measurements versus the old knowledge. This solution would of course solve the problem of short noisy measurements, although it increases the computational complexity.
Finally, a third possibility is the usage of a one dimensional Kalman filter to obtain an incremental estimation using the measurements. A Kalman filter assumes an additive white Gaussian noise with an unknown variance as an error on the PHY measurements; it can compute the current expected "real" signal strength together with the variance that it assumes together with this estimation. An advantage of the Kalman filter is that it weights the influence of new measures proportional to the current degree of believe of the estimation. Therefore, it can be seen as an enhancement of the exponential weighted average: In the latter case, all measurements are weighted with the same α ; In contrast, the Kalman filter is able to adapt this coefficient to the current variance.
The increased computational complexity in comparison to the exponential weighted average is an obvious downside of the Kalman filter.

Using one of the described mechanisms, the learning Mesh Point is able to learn the weight of all direct links whereas all other links remain unknown. As it was explained above, an estimation of the lower bound of the weight of the other links suffices for a good interference CoI computation; therefore, two different methods with different complexity can be used.

The first method is explained by the use of Figure 17. In this very simple scenario, Mesh Point "2" wants to initialize a transmission which is simultaneous to the transmission (1) from Mesh Point "3" to Mesh Point "4". Therefore, it has to compute the interference CoI, which needs a lower bound of the signal strength that is detected at Mesh Point "4" if Mesh Point "3" is transmitting.

Figure 17: Mesh Point "2"wants to learn the signal strength of route (1)

Here, the medium access protocol during the MTP can be used as a simple sensor to get information about this signal strength. In the train header (consider section "Train Header"), for each receiver the used PHY mode is indicated. As the train header is send in the basic PHY mode, chances are high that Mesh Point "2" can understand this header and therefore it knows the used PHY mode. As fragile PHY modes can only be used successfully if the signal strength at the receiver is above a minimum threshold, Mesh Point "2" can conclude the minimum signal strength, which suffices for the CoI. Table 3 shows the minimum signal strength in dBm for the different 802.11 PHY modes.

Table 3: The minimum signal strength for the successful reception, depending on the PHY - mode

PHY mode	Minimum C (dBm)
BPSK ½	-82
BPSK ¾	-81
QPSK ½	-79
QPSK ¾	-77
16QAM ½	-74
16QAM ¾	-70
64QAM 2/3	-66
64QAM ¾	-65

The other possible method results in more overhead because it uses special IEs to disseminate the information about the received signal strengths over the network. This signal strength IE consists only of three

fields: The Mesh Point where the signal is received, the transmitting Mesh Point and finally an 8b value expressing a lower bound on the signal strength.
The lower bound can be obtained by the estimation of direct links at it was discussed earlier, especially if a Kalman filter was used: Together with the variance, a confidence interval can be computed for the estimation, and the lower limit of this interval can be disseminated.

The frequency of sending of SSIEs should be very low; additionally, it is possible to adapt it to the behavior of the link, e.g. information about a steady, only slightly changing link is disseminated fewer than information about a fluctuating link. Furthermore, information about a link should not be send at all if the current knowledge is not very profound.

A the data in a received SSIE can be handled with more trust than data from the sensors about direct links, as it was already filtered and only the lower limit was sent. Therefore, a low pass filtering of the data with a high alpha should be sufficient. A station may decide whether to resent a received SSIE or to drop it. The probability of dropping the SSIE should be anti-proportional to the maximum direct link strength to the mentioned stations in the SSIE, as the information becomes irrelevant for Mesh Points that are even farer away.

Deterministic Pairwise Key Pre-Distribution Scheme for IEEE 802.11s Security

Security proposal introduction

IEEE 802.11s will define a new standard for low-cost, easily deployable, high performance WLAN mesh networks. Among the list of 802.11s usage model requirements, the most restrictive include:

- Low susceptibility to vandalism,
- Network self-configuration and self-management,
- Power conservation.

In many WLAN mesh scenarios (e.g. see Figure 18) mesh points will be mobile and take different roles, including mesh AP. In such scenarios, the network topology changes dynamically as users roam. Timely self-configuration of the network is paramount for the success of some target applications (such as in fire rescue).

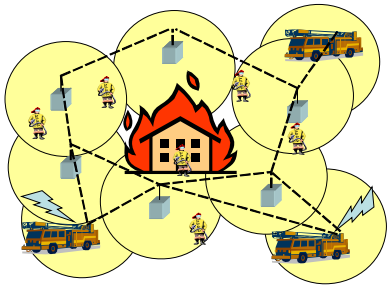


Figure 18 Public Safety Scenario

In this context, security provisioning plays an equal relevant role for the success of target applications, so that only authorized users (by the administration) can communicate in the network. A security solution that perfectly meets the afore mentioned requirements is paramount for the success 802.11s and final development of 802.11s into products.

In this document we describe the Deterministic Pairwise Key Pre-Distribution Scheme (DPKPS) for 802.11s. The details in this document are based on proved assumptions. A related paper is to appear at the conference IEEE Securecomm05 [1].

Supported Security Services

Key pre-distribution consists in pre-loading some keying material into network nodes, before they are actually deployed in the network. Once the network is formed, nodes use their respective keying material to establish cryptographic keys, which are subsequently used to protect network links and, in some cases, even to authenticate network nodes.

The DPKPS (in this document and in [1]) is a key pre-distribution system with advanced properties, including:

- Support for any-to-any *direct* pairwise (unique symmetric) key establishment,
- Support for paramount services, including node authentication and revocation, and communication confidentiality and integrity protection,
- Support for secure multicast group formation,
- Supports security in big-scale (resource-constrained) MeshWLANs (e.g. sensor networks)
- Energy, storage and bandwidth efficiency,
- Robustness and resiliency against mesh point captures.

Since *any* pair of nodes can establish a key to protect their communication, the DPKPS provides security independently of the network topology and membership. Since established keys are *pairwise*, a unique different key is used for each different pair of nodes. Consequently, node authentication, revocation as well as identity-based access control are also enabled.

Since the DPKPS uses symmetric key cryptography, the DPKPS provides a power conserving security solution. Additionally, since nodes can *directly* protect communications without security server support, the DPKPS provides a reliable and timely security solution. These properties make the DPKPS to cover a wide span of WLAN usage scenarios and to perfectly cover WLAN mesh ad-hoc-like deployments.

Use Model

Before going into the details of the DPKPS, let us introduce how to use it for protecting network communications.

Security Set-Up Phase

Before the mesh points are deployed in the mesh WLAN, keying material is pre-loaded in each mesh point using a ***combinatorial distribution*** method (see details of the method in Section 4).

Secure (Dynamic) Network Formation

Once deployed in a mesh WLAN, ***any pair*** of mesh points (which establish a mesh link) can derive a ***pairwise*** key from their pre-distributed keying material.

Secure Communication

Mesh points use the derived pairwise keys for node authentication and/or data encryption/integrity.

Description of the DPKPS

In the DPKPS, the ***combinatorial distribution*** during the security set-up phase is a novel key pre-distribution method, which enables paramount security services with very advanced performance properties.

In this section we describe DPKPS security set-up and key establishment phases. First of all, we will briefly introduce the basis of the DPKPS, including Blundo polynomials [2] and theory of block designs [2]. Then, we will describe the DPKPS.

Blundo Polynomials

Blundo et al. 2 proposed a polynomial-based KPS to derive group keys. For groups of two users, Blundo's KPS can be used to establish pairwise keys in MSNs:

Set-up. A set-up server randomly generates a symmetric bivariate λ-degree polynomial $f(x,y)=\sum_{i,j=0}^{\lambda} a_{ij}x^i y^j$ over a finite field F_q (q is a prime number large enough to accommodate a cryptographic key). By the property of symmetry $f(x,y)=f(y,x)$.

Key Pre-distribution. The setup server computes and distributes a polynomial share of $f(x,y)$ to for each sensor u, i.e. $f(u,y)$. Each sensor u has a unique identifier.

Key Establishment. After the deployment phase, for two arbitrary nodes u and v, node u can compute the common key $K_{uv}=f(u,v)$ by evaluating $f(u,y)$ at point v, and node v can compute the same key $K_{uv}=f(v,u)=f(u,v)$ by evaluating $f(v,y)$ at point u.

Theory of Block Designs

A *Balanced Incomplete Block Design* (BIBD) is an arrangement of v distinct objects into w blocks such that each block contains exactly k distinct objects, each object occurs in exactly r different blocks, and every pair of distinct objects occurs together in exactly t blocks. The design can be expressed as (v,k,t), or equivalently (v,w,r,k,t), where: $t(v-1)=r(k-1)$ and $wk=vr$.

In a symmetric BIBD (SPIBD) $w=v$ and, thus, $k=r$. A SPIBD has four interesting properties: every block contains $k=r$ elements, every element occurs in $k=r$ blocks, every pair of elements occurs in t blocks and every pair of blocks intersects in t elements.

An FPP is an SPIBD with parameters $\left(n^2+n+1, n+1, 1\right)$ 2**Fehler! Verweisquelle konnte nicht gefunden werden.**. An FPP exists for any prime power *n*, where n≥2. FPP of order *n* has four properties: (i) every block contains exactly *n*+1 points, (ii) every point occurs on exactly *n*+1 blocks, (iii) there are exactly n^2+n+1 points, and (iv) there are exactly n^2+n+1 blocks.

DPKPS Security Set-Up

The DPKPS pre-distributes $n+1$ distinct polynomial shares $F_{b_{i,j}}(p_{u_j}, y)$ to each mesh point *u*, $j = 1...n+1$. The indices $b_{i,j}$ of $F_{b_{i,j}}(p_{u_j}, y)$, for $j = 1...n+1$, are associated to the element $b_{i,j}$ of a block B_i of an FPP[1]-$\left(n^2+n+1, n+1, 1\right)$.

DPKPS Key Establishment

The DPKPS pre-distribution guarantees that any two mesh points *u*,*v* carry distinct polynomial shares $F_k(p_u, y)$, $F_k(p_v, y)$ of (at least) one common polynomial $F_k(x, y)$ and, thus, can establish a pairwise key K_{uv}.

Advanced Properties

1. The DPKPS improves the computational efficiency in the generation of pairwise keys with Blundo polynomials and augments the scalability of Blundo polynomials as well as its resiliency in front of attackers capturing mesh points randomly. It is especially suited for networks of very low-resource mesh points.

[1] The FPP can be constructed from a set of *n mutually orthogonal Latin squares* (MOLS) to further improve the bandwidth usage of the key establishment phase, when relatively high values of *n* are used. The details of this construction are not relevant to understand the DPKPS. For more details we refer the reader to [1].

References

1. D. S. Sánchez, H. Baldus. A Deterministic Pairwise Key Pre-Distribution Scheme for Mobile Sensor Networks. To appear at IEEE Securecomm. September 2005.
2. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, Perfectly Secure Key Distribution for Dynamic Conferences. In Advances in Cryptology - CRYPTO '92, Springer-Verlag, Berlin, 1993, pp. 471-486.
3. W.D. Wallis. Combinatorial Design. Marcel Dekker Inc., 1988.
4. http://mna.comnets.rwth-aachen.de