

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/265296204>

A survey on IEEE 802.11 ah: An Enabling Networking Technology for Smart Cities

Article in *Computer Communications* · March 2015

DOI: 10.1016/j.comcom.2014.08.008

CITATIONS

97

READS

1,071

4 authors:



[Evgeny Khorov](#)

Institute for Information Transmission Proble...

65 PUBLICATIONS 301 CITATIONS

[SEE PROFILE](#)



[A. Lyakhov](#)

Russian Academy of Sciences

135 PUBLICATIONS 677 CITATIONS

[SEE PROFILE](#)



[Alexander Krotov](#)

The Institute for Information Transmission Pr...

4 PUBLICATIONS 111 CITATIONS

[SEE PROFILE](#)



[Andrey Guschin](#)

The Institute for Information Transmission Pr...

2 PUBLICATIONS 98 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



LoRaWAN [View project](#)



Improving efficiency of dense wireless networks [View project](#)

All content following this page was uploaded by [Evgeny Khorov](#) on 19 October 2017.

The user has requested enhancement of the downloaded file.

A survey on IEEE 802.11ah: an Enabling Networking Technology for Smart Cities *

Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, Andrey Guschin
IITP RAS
{khorov, lyakhov, krotov, guschin}@iitp.ru

Abstract

Smart technologies play a key role in sustainable economic growth. They transform houses, offices, factories, and even cities into automatic, self-controlled systems acting often without human intervention and thus sparing people routine connected with information collecting and processing. The paper gives an overview of a novel Wi-Fi technology, currently under development, which aims to organize communication between various devices used in such applications as smart grids, smart meters, smart houses, smart healthcare systems, smart industry, etc.

1 Introduction

At the end of the last century computers replaced people in many areas facilitating routine actions. Connected together, computers broke the boundaries limiting information dissemination.

5 In early 2000s, social networks and mobile gadgets connected people all over the world. Having replaced face-to-face communications, they gave us the Internet of people. Although the amount of data transmitted over the

*This is the draft of paper *Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, Andrey Guschin, A survey on IEEE 802.11ah: an Enabling Networking Technology for Smart Cities. Computer Communications, Volume 58, March 2015, pp. 53–69, 2015. ISSN 0140-3664. Available online: <http://authors.elsevier.com/a/1QbtUVwcQFhij>, <http://dx.doi.org/10.1016/j.comcom.2014.08.008>*

Internet is continuously growing, the number of active users in such a network is limited to the number of people on the Earth.

10 Both phenomena, computers and Internet, have unpredictably changed our life, making people check mail before washing up in the morning. No doubt that the desire to automate whatever possible will definitely revolutionize economics, politics, and social life. New applications and services of scalable smart systems – grids, factories, and cities – require myriads of
15 smart things (sensors, robots, controllers, etc.) connected together. Analysts forecast that the total number of devices in such a network, called Internet of Things (IoT), will reach 50 billion by 2020 [1]. Apparently, the best way to connect such a huge number of devices is by wireless.

While futurologists predict our life in 2020, networking engineers inquire
20 whether state-of-the-art wireless technologies are able to provide connectivity for such a huge number of devices, most of which are battery supplied. Although a number of solutions based on RFID, ZigBee, Bluetooth, or other WPAN technologies already support low power device communication, their capabilities are limited by the number of devices, throughput, transmission
25 range, etc. On the other hand, such technologies as WiMAX and LTE are also not suitable because of high energy consumption.

3GPP, IEEE and other international organizations adopt their technologies to the emerging market of the IoT. For example, IEEE 802.11 aka Wi-Fi, used everywhere nowadays, is not suitable for the IoT, since this wireless tech-
30 nology was originally designed to offer high throughput to a limited number of stations located indoor at a short distance between each other. To meet IoT requirements, IEEE 802 LAN/MAN Standards Committee (LMSC) has formed IEEE 802.11ah Task Group (TGah) to extend the applicability area of .11 networks by designing an energy efficient protocol allowing thousands
35 of indoor and outdoor devices to work at the same area.

This paper addresses the activities of TGah, its challenges and the key mechanisms of the upcoming IEEE 802.11ah (.11ah) standard amendment. Although the work is expected to be finished by 2016 [2], draft standard IEEE 802.11ah-D1.0 [3] adopted in October 2013 provides us with the entire
40 view of the novel solutions developed in the Task Group. Because of the refinement process of the draft standard, all the solutions will hardly stay unchanged, however, it is very unlikely that they will be excluded from the final version, the more so, that in May 2014 TGah estimates that 90% of the draft is stable [4].

45 Thus, the early acquaintance with .11ah is useful for both industry and academical sides. Dozen of papers studying .11ah confirm this idea [5–12]. Written at the beginning of the standard development process, they provide only a brief overview of some solutions discussed in TGah at that time,

leaving many interesting issues without consideration. Having waited for
50 the work on version D1.0 to be finished¹ and seeing obvious difficulties to
explain MAC and PHY protocols described in the 394-page draft standard,
its motivation and necessity for smart scalable system in a single paper, we
try to do it, focusing on the MAC layer aspects.

The rest of the paper is organized as follows. Section 2 describes the set
55 of use cases considered by TGah, their relevance to scalable smart systems
(such as smart cities) and problems to be solved in .11ah. Section 3 provides
a brief overview of the PHY layer needed to understand MAC solutions.
In Section 4, we describe MAC solutions developed in the Task Group to
address all problems related to challenges of smart city implementation. For
60 each solution, we provide an explanation² why it was included into draft
standard and what benefits it brings. Finally, Section 5 concludes the paper.

2 Use Cases

In 2010, having studied the sub 1 GHz (S1G) license-exempt bands (ex-
cept for TV white spaces), LMSC determined this spectrum to be promising
65 for outdoor communication of .11 devices.

Because of the scarcity of the available spectrum, S1G does not allow us-
ing wide bands, especially >20 MHz wide bands introduced in .11n and .11ac.
Nevertheless, the novel modulation and coding schemes (MCS), designed in
the .11ac amendment and brought to .11ah, can provide hundreds Mbps³ if
70 channel conditions are good enough. At the same time, S1G frequencies have
better propagation characteristics in outdoor scenarios than traditional for
Wi-Fi 2.4 and 5 GHz bands, which increases transmission range up to 1 km
at the default transmission power of 200 mW.

2.1 Smart Sensors and Meters

75 Efficient MCSs and favorable propagation characteristics joined with rel-
atively narrow bands allow to create a technology for sensor networks, which

¹Thanks to the review process we refined the paper, having included modifications
made by the time of paper submission, i.e. those which appeared in D2.0 [13] published
in June, 2014. Fortunately, they are not dramatic.

²In this paper, we cannot provide thorough performance evaluation of .11ah, which is
definitely a huge work. Our speculation is based on the results obtained in few existing
scientific papers or numerous internal documents of TGah. The interested reader may find
some extra figures in cited literature.

³According to the draft standard [3], the maximal data rate at the PHY layer equals
346 Mbps.

Draft. For internal usage only

excels ZigBee, Bluetooth, NFC, etc. in throughput and coverage, remaining very energy efficient. Most of the adopted use cases [14] consider sensing applications, including

- 80 • smart meters (gas, water and power consumption),
- smart grids,
- environmental and agricultural monitoring (temperature, humidity, wind speed, water level, pollution, animal condition, forest fire detection, etc.),
- 85 • automation of industrial process (petroleum refinement, iron and steel, pharmacy),
- indoor healthcare/fitness system (blood pressure, heart rate, weight),
- elderly care system (fall detection, pill bottle monitor).

In these applications, an access point (AP) covers hundreds or even thousands of devices — sensors or actors — that periodically transmit short packets. Huge number of stations contending for the channel results in collisions, long transmission range leads to high interframe spaces, and short packets increase overhead caused by headers. Although the required aggregate throughput in the considered use cases does not exceed 1 Mbps, all these
95 issues manifold degrade network performance and the standard developers need to pay much attention to them. One more issue is the energy consumption, since sensors are often battery powered.

2.2 Backhaul Aggregation

Widely used in industry, IEEE 802.15.4g wireless devices⁴ can operate on
100 a battery for a long time, however the transmission range and available data rates are very low. The second group of use cases adopted by TGah covers the backhaul connection between IEEE 802.15.4g devices and remote servers [15]. IEEE 802.15.4g routers gather data from leaf devices and forward information to the servers by .11ah links, see Fig. 1.

105 Since IEEE 802.15.4g rates are insufficient for video streaming, IEEE 802.11ah can also be used in these scenarios to transmit images or surveillance videos obtained from autonomous cameras, the more so that .11 channel access is more efficient than the one of IEEE 802.15.4g [11].

⁴Since IEEE 802.15.4g also works in S1G band, TGah addresses coexistence with these devices. However, this issue is left beyond the scope of the paper.

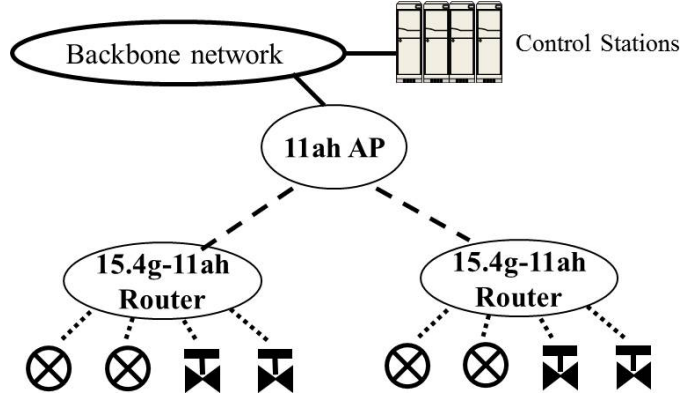


Figure 1: Backhaul aggregation usecase [14]

Scenario	Location	Environment	Data rate	Mobility	STA/AP capacity
Sensors and meters	indoor outdoor	urban suburban rural	100 kbps	stationary	AP: 1 STA: 6000
Backhaul aggregation	outdoor	industrial rural	< 1 Mbps	stationary low velocity	AP: 10 STA: 500
Extended Range and cellular offloading	outdoor	urban sub-urban	< 20 Mbps	pedestrian	AP: 1 STA: 50

Table 1: Requirements for different use cases [14].

2.3 Extended range hotspot and cellular offloading

Both high throughput and long transmission ranges make S1G attractive for extending hotspot range and for traffic offloading in mobile networks, which is a significant issue for operators and vendors because of mobile traffic explosion [16]. Although .11n and .11ac data rates are comparable to or even higher than the rates of the modern mobile networks, e.g. LTE, they can hardly be used for offloading in outdoor scenarios because of short transmission range. In contrast, extending the transmission range, IEEE 802.11ah will provide real additional value, especially in countries with wide available S1G channel, e.g., USA [6]. According to the document defining functional requirements for .11ah [17], the novel amendment shall provide at least one mode of operation capable of achieving a maximum aggregate multi-station data rate of 20 Mbps at the PHY layer.

Table 1 summarizes requirements for the adopted use cases.

Draft. For internal usage only

2.4 Not adopted use cases

Several use cases discussed in TGah have not been adopted at straw
125 polls [18]. The list of them includes

- media streaming for home entertainment,
- electronic menu in restaurants and coupon distribution in malls,
- indoor and outdoor location (in mall, parking, etc.),
- AP power saving.

130 Such a decision does not forbid to use either IEEE 802.11-2012 or IEEE 802.11ah in these scenarios, but bounds the vast range of requirements to be considered by TGah.

While the Extended Range Hotspot and Cellular Offloading meet well the continuous natural intention of the .11 Working Group to increase data
135 rates and transmission ranges, the sensor-related use cases are absolutely new for .11 networks. Since legacy .11 is not designed for a huge number of power limited stations transmitting short packets, typical for emerging smart systems, TGah has significantly revised the MAC layer in addition to the PHY one.

140 3 PHY Layer Overview

3.1 Channelization

The IEEE 802.11ah PHY layer is inherited from .11ac and adopted to available S1G bandwidth. The channels used in .11ah are 10 times narrower than those in .11ac: 1, 2, 4, 8 and 16 MHz. Only 1 and 2 MHz channels are
145 mandatory.

Having studied the S1G regulation in various countries, TGah has been faced to the problem that the bands available for S1G ISM (industrial, scientific and medical) communication are different depending on the country. The current version of the draft standard already specifies which channels
150 shall be used in the United States, Europe, Japan, China, South Korea and Singapore. Figure 2 illustrates channelization opportunities for the US, where frequencies from 902 to 928 MHz are available for ISM communication.

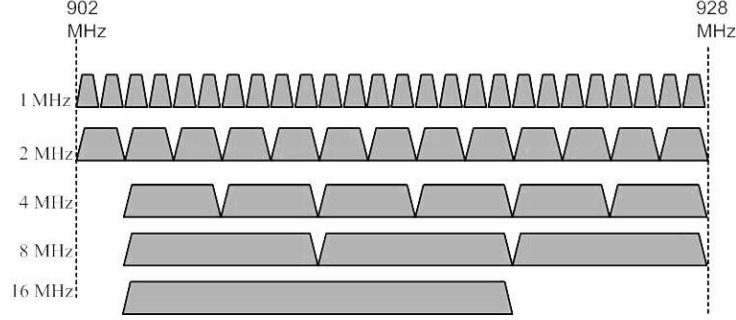


Figure 2: US Channelization [19].

3.2 PHY properties

Similar to .11ac, .11ah uses Orthogonal Frequency Division Multiplexing (OFDM), Multiple Input Multiple Output (MIMO) and Downlink Multi-User MIMO (DL MU-MIMO).

For the channels ≥ 2 MHz, the PHY layer is just 10 times down-clocking of the .11ac's PHY, i.e., the duration of OFDM symbols in .11ah is 10 times longer than in .11ac, while the numbers of sub-carriers in .11ah channels are the same as those in the corresponding .11ac channels. E.g., both 2 MHz channel in .11ah and 20 MHz channel in .11ac have 64 sub-carriers including pilot and guard, and only 52 of them transmit data.

For the 1 MHz channel the total number of sub-carriers is twice lower, but only 24 (which is less than $52/2$) transmit data because the number of guard sub-carriers cannot be reduced.

.11ah inherits 10 MCSs (referred to as MCS0, ..., MCS9) with different reliability properties and transmission rates from the .11ac standard. Since MCS9 is not available in 20 MHz .11ac channel, it is not valid in 2 MHz .11ah channel, too. To extend transmission range of 1 MHz channel, the standard defines a novel MCS10, which is nothing but a modification of MCS0 with 2x repetition, increasing transmission reliability.

Authors of [5] model .11ah channel and prove that in outdoor scenarios with 200mW transmission power and 1 MHz channel, the transmission range indeed exceeds 1km if MCS 10 is used, while MCS 0 provides 850 m, and MCS 10 gives about 200 m. With the default Wi-Fi frequencies of 2.4 GHz and 5 GHz, the transmission range is 3...9 times lower.

The regular data rates for various bandwidths and MCSs are listed in Table 2. They can be improved by reducing the duration of OFDM symbol and using several spatial streams.

The duration of a normal OFDM symbol is $40 \mu s$, 20% of which is the

Draft. For internal usage only

MCS	1 MHz	2 MHz	4 MHz	8 MHz	16 MHz
MCS0	0.3	0.65	1.35	2.925	5.85
MCS1	0.6	1.30	2.70	5.850	11.70
MCS2	0.9	1.95	4.05	8.775	17.55
MCS3	1.2	2.60	5.40	11.700	23.40
MCS4	1.8	3.90	8.10	17.550	35.10
MCS5	2.4	5.20	10.80	23.400	46.80
MCS6	2.7	5.85	12.15	26.325	52.65
MCS7	3.0	6.50	13.50	29.250	58.50
MCS8	3.6	7.80	16.20	35.100	70.20
MCS9	4.0	—	18.00	39.000	78.00
MCS10	0.15	—	—	—	—

Table 2: Data rates for various MCSs in Mbps, single spatial stream and normal OFDM symbol.

guard interval (GI) containing redundant data and preventing inter-symbol interference. IEEE 802.11ah allows twice shorter guard interval which $\frac{10}{9}$ times increases data rates.

IEEE 802.11ah stations can use up to 4 spatial streams. N spatial streams
185 N times increase the data rates.

TGah moves some MAC functionality from MAC headers to PHY headers, e.g. acknowledgment indication. Being related to the MAC layer rather than to the PHY layer, these changes are described in Section 4.

4 MAC Enhancements

190 As mentioned in Section 2, the most difficult task for TGah is to support a tremendous number of power limited stations transmitting short packets. Being well designed, IEEE 802.11 MAC has the only formal limitation preventing its usage with a huge number of stations. It is connected with frame formats and described in detail in Section 4.1. However, breaking this limita-
195 tion is not enough to make .11ah suitable for emerging niches, and TGah puts much effort into the MAC layer to improve power efficiency and reduce overhead caused by 1) short packets transmission and 2) long time characteristics of .11ah PHY. Both issues lead to high percentage of channel resources occupied by frame headers, interframe spaces, control and management frames,
200 or wasted by channel access procedure. This section presents a long list of solutions designed by TGah. Many of them are interconnected, complicating their description. Although the classification may be disputed, we divide

Draft. For internal usage only

Characteristics	Value
Backoff slot	52 μs
SIFS	160 μs
CCATime	< 40 μs
AirPropagationTime	6 μs
PHY-RX-START-Delay	1MHz: 600 μs , 2MHz/4MHz/8MHz/16MHz: 280 μs
PPDUMaxTime	27.84 ms (511 bytes at 1 MHz using MCS10 and 1 spatial stream)
PSDUMaxLength	797160 octets (511 symbols (limited by PPDUMaxTime) at 16 MHz using MCS9 and 4 spatial streams)

Table 3: Time characteristics of .11ah.

MAC solutions into several groups.

Section 4.1 describes how TGah overcomes formal .11 limitations on the number of devices. Section 4.2 overviews new short frame formats needed to reduce overhead and to improve power efficiency. Section 4.3 introduces novel channel access methods aiming to reduce channel busy time, collisions and power consumption, when thousands of stations aim to access the channel. Section 4.4 presents new power management mechanisms supporting huge number of battery powered stations. Aiming to further improve power efficiency (by using higher MCS) and coverage, IEEE 802.11ah extends infrastructure BSS with two-hop relaying, described in Section 4.5.

4.1 Breaking Formal Limitation of IEEE 802.11

Developed for moderate network size, the baseline IEEE 802.11 standard [20] does not limit the number of stations in the network explicitly. The only limits presented in the standard are connected with the length of some fields in management frames.

The Association IDentifier (AID) — a unique value assigned to a station by the AP during association handshake — is 14 bits long, but values other than 1-2007 (0 and 2008-16383) are reserved. In particular, AID=0 is reserved for group addressed traffic. So, an AP cannot have more than 2007 associated stations.

The same limit is given by the Traffic Indication Map (TIM) bitmap used by power-management mechanisms and indicating the set of stations for which the AP has buffered frames (for details, see Section 4.4.1). The

Draft. For internal usage only

TIM length is bounded by 2008 bits.

Thus, the latest approved version of the standard [20] does not support more than 2007 associated stations⁵, while the first use case described in Section 2 requires support for up to 6000 stations. For this reason, TGah
230 extends the range of AID values for S1G stations from 1-2007 to 0-8191. Also the draft standard increases the maximal length of the TIM bitmap for S1G stations from 2008 bits to 8192 bits [21].

Having resolved the issue at the tip of the iceberg, TGah focuses on how to operate with such a large number of stations transmitting short pieces of
235 information.

4.2 Frame shortening

Although .11ah PHY provides high data rates, the aggregate throughput may be very low because of the huge overhead inherent to short packet transmission typical for sensor networks. In .11ah networks, the situation
240 is worsened by very long time characteristics of the PHY layer presented in Table 3. Apart from reducing throughput, the overhead degrades power efficiency. Aggregation, Block Ack and some other .11 solutions are often inapplicable to sensor networks: used in uplink (from sensor stations to the AP), they lead to a high latency, not acceptable in many use cases. That is
245 why TGah has made many efforts to reduce overhead, paying much attention to:

- frame headers (see Section 4.2.1),
- control frames, e.g., ACK, just signalling an event and so containing a small piece of information but taking much time to transmit (see
250 Section 4.2.2), and
- periodically transmitted beacons containing redundant information (see Section 4.2.3).

Fortunately, free of legacy devices S1G band opens the door for revolutionary changes in the frame formats.

255 4.2.1 Short Headers

In legacy .11 infrastructure networks, the length of the MAC header containing 3 addresses is 30 bytes, see Fig. 3. Frame Check Sequence (FCS) gives

⁵This does not claim that any network with 2007 stations works well, but 2008 stations cannot be associated to a single AP at all.

Draft. For internal usage only

another 4 bytes. Thus, for a 100-byte payload (messages), MAC header overhead exceeds 30%. For smaller messages, the overhead is ever higher.

260 To reduce it, the draft standard defines a new backward incompatible format of shortened headers for data, management and novel control frames (e.g., TACK and STACK described in Section 4.4.5). To distinguish legacy frames and frames with short headers, both used in .11ah, the standard changes protocol version bits in the Frame Control (FC) field of the short
265 header from 00 to 01, which is the first-ever change of the Wi-Fi protocol version.

Figure 3 illustrates the differences between the legacy header and the short one.

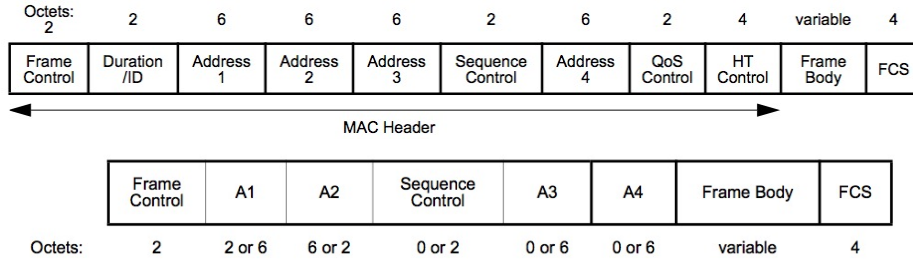


Figure 3: Legacy MAC header (top) [22] and short MAC header (bottom) [3].

A significant change is that the short header contains no Duration/ID
270 field required for NAV, a legacy virtual carrier sense mechanism, which made TGah develop a novel channel access mechanism called RID (see Section 4.3.1). Also, Quality of Service (QoS) and High Throughput (HT) fields are excluded from the header.

Similarly to the legacy frames, the short ones may contain up to four
275 Address fields. However in contrast to IEEE 802.11-2012 [20], only two addresses (not three) are mandatory: the receiver and the transmitter ones. Indeed, *two* addresses are enough if a frame is sent from the AP to a station, or in opposite direction. However, *three* addresses are required if a frame is sent between stations via the AP and the stations belong to the
280 same infrastructure Basic Service Set (BSS), a network with the only AP. *Four* addresses (receiver, transmitter, source and destination addresses) are needed to transmit frames over a multihop network.

Nevertheless, .11ah allows to use only two address fields, reducing overhead. By default, if the destination and/or source addresses are not present
285 in the frame, they equal the receiver and/or transmitter ones, correspondingly. To modify the default behavior, recently developed Header Compres-

Draft. For internal usage only

sion (HC) handshake can be used. By this handshake, the transmitter tells the intended receiver the values of the Destination and/or Source addresses. HC is very useful in scenarios with intense flows of sensor or offloading data.

290 A 6-byte address field is more than enough to identify 8000 stations. To minimize overhead, TGah replaces non-AP address with a 2-byte Short Identifier (SID) field. SID is composed of a 13-bit AID and flags. Two flags indicate presence of the third and the fourth addresses and the third flag is used by the aggregation mechanism⁶.

295 The AP address – which is also the BSS identifier (BSSID) – is never replaced with SID for two reasons: (1) APs have no AID, and (2) full address is needed to distinguish frames transmitted in various overlapping BSSs (OBSS).

300 Described in this Section approach allows to significantly (more than twice) reduce header-induced overhead, which is very useful for sensor networks transmitting short messages.

4.2.2 NDP MAC frames

In addition to data frames, TGah shortens control frames such as ACK, CTS, etc. These frames do not transmit any useful information (except for the Duration field), just indicating frame reception, channel access, or other event. However they cause overhead, especially high in case of short transmissions. For example, if a 100-byte packet is transmitted at the lowest data rate in 2 MHz channel, ACK duration is 0.3 of the data frame duration (480 us vs. 1600 us in the 2 MHz channel, at 600 kbps [23]).

310 To reduce overhead, TGah develops a novel frame format called Null Data Packet (NDP) MAC frames (do not confuse with frames with short headers!).

NDP frames were included in .11ac as short frames used for channel calibration needed for beamforming. Channel calibration can be carried out by analyzing the received sounding symbols in the PHY header, so NDP frames do not need and do not have any payload from the MAC layer [24].

315 TGah extends the concept of NDP, allowing to include some useful information in the SIG field of the PHY header. For example, the PHY header of NDP ACK contains

- ACK ID containing some bits from the received frame to reduce probability of false positive acknowledgement,

⁶IEEE 802.11ah redefines A-MSDU frame format (so-called Dynamic A-MSDU). A-MSDU frames aggregate several subframes, each of which has the header with its own destination and sender addresses. TGah makes these addresses optional. If they equal the corresponding addresses in the header of the whole frame, they can be omitted.

Draft. For internal usage only

- Duration field which either has the legacy interpretation or is used by power saving mechanisms,
- More Data field indicating whether the NDP ACK transmitter has data to transmit to the NDP ACK receiver, etc.

325 The format of NDP frames and field meaning differs from 1 MHz and ≥ 2 MHz PHY. For example, the duration field resolution is 40 us for 1 MHz frames and 1 us for ≥ 2 MHz frames. Apart from NDP ACK, IEEE 802.11ah describes NDP CTS, NDP PS-Poll, NDP BlockAck, NDP Probe Request (the only NDP MAC management frame), etc.

330 Since the length of NDP MAC frame is just 6 symbols (240 us) and 14 symbols (560 us) for ≥ 2 MHz and 1 MHz channels respectively, NDP MAC frames significantly reduce overhead and shall be used instead of corresponding legacy frames in S1G bands by default.

4.2.3 Short Beacons

335 Another source of excessive overhead is beacon. In infrastructure BSS, beacons are periodically sent by the AP. Beacon content depends on the mode in which the AP is operating, and typically in .11g/n networks, its length may exceed 100 bytes [25]. To be received by edge stations, beacons should be sent at the lowest rate, which is less than 1 Mbps in case of .11ah.
340 At such low rates, even dozens of bytes sent several times per second occupy significant percentage of channel time.

To reduce medium occupancy and power consumption for both the AP transmitting the beacon and sensor stations receiving it, TGah uses 2 types of beacons: full and short. Short beacons are sent more frequently than the full ones and do not contain unessential or non-urgent information, which
345 can be obtained from normal beacons or with probe request. Thus, unlike full beacons, short beacons do not contain

- destination address, since beacons are always broadcast,
- BSSID, since it is the same as the sender address,
- 350 • Sequence control, since it is useless [26].

Some fields and information elements are shortened, e.g.:

- Timestamp (from 8 to 4 bytes), since it is enough to maintain synchronization [25].

Draft. For internal usage only

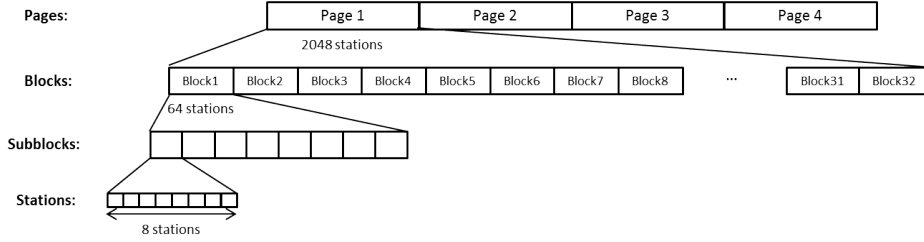


Figure 4: AID hierarchy.

- SSID information element is replaced by the optional 4-byte Com-
pressed SSID field containing the CRC32 of 32-byte SSID. Knowing
SSID, a station can determine whether the received short beacon be-
longs to the same BSS or not.

Almost unchangeable information elements can be excluded from short beacons. To notify stations about updates, short beacons contain a one-byte Change Sequence Field incremented with every critical update. Having received a short beacon with a new value in this field, a station waits for a full beacon to get updated information. The moment when the next full beacon is transmitted can be learnt from an optional Next TBTT field. So the station may sleep till this moment, saving energy.

Since offloading is an important use case of .11ah technology, pre-association discovery of Internet gateways is an important feature. That is why short beacons contain an optional 1-byte long Access Network Options field designed in .11u amendment⁷ [27] and indicating whether the access network is public, whether it is free, and whether it has connection to the Internet. Having received a short beacon, stations can determine whether the access network is suitable or not without waiting for a full beacon.

Apart from beacons, TGah compresses other management frames, e.g., Probe Response frame and Resource Allocation Frame used by novel RAW mechanism described in Section 4.3.2.

4.2.4 Grouping of Stations and Bitmap Compression

To simplify operation with a huge number of associated stations, IEEE 802.11ah groups them by AIDs according to a four-level structure shown in Fig. 4 [28]. At the top level, the stations are divided into 4 pages of 32 blocks each. A block includes 8 subblocks of 8 stations each. Thus, the first 2 bits of AID encode page number, the next 5 bits encode block, etc.

⁷In .11u, it is a part of the Interworking element.

Draft. For internal usage only

Grouping stations with similar characteristics into pages, blocks and sub-blocks allows many mechanisms developed by TGah and described in further Sections to reduce overhead while referring to stations. So AIDs are assigned with respect to device type, power management mode, location, station's traffic, etc. When a station changes these characteristics, the AID may be reassigned by means of Dynamic AID Assignment handshake between the AP and the station. After that, the station shall notify all its peers about the change of AID if it uses direct links with them.

Let us demonstrate how grouping stations allows to compress TIM bitmap. The length of uncompressed TIM bitmap may reach 8 kb, however most bits are typically zeros. Depending on the bitmap values, the AP may adaptively choose how to encode information. TIM may contain compressed information about the whole page, only a block, a range of AIDs, or individual AID. Fig. 5 shows how a block containing 4 non-zero bits (3, 8, 42, and 45) is compressed from 8 to 3 bytes. The first byte contains 8-bit map of non-zero subblocks (1 and 6). Next two bytes represent bitmaps of these subblocks.

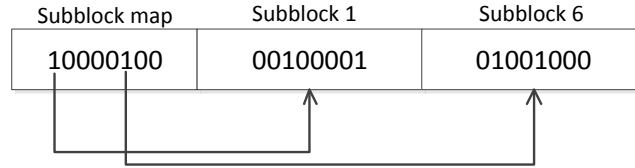


Figure 5: Block compression.

Apart from reducing overhead, grouping of stations with similar characteristics or located near each other and restricting channel access to a given group can reduce contention and avoid overlapping transmission from a large number of stations hidden from each other. Novel channel access methods to allow these features are described in Section 4.3.2 and Section 4.3.4.

4.3 Channel Access

The main task for the solutions described in this Section is decreasing overhead caused by channel access methods. This overhead includes backoff slots, interframe spaces, ACKs, collisions, and time intervals during which a station shall avoid transmission overlapping with other transmissions in the network, etc.

4.3.1 Virtual carrier sense

Since 1997, when the first release of the IEEE 802.11 standard [29] was published, the channel access methods⁸ have been using virtual carrier sense mechanism called NAV in addition to the physical carrier sense to avoid collisions during bidirectional frame exchange. For example, if a transmitter expects ACK after a data frame, NAV forbids all neighbour stations (except for the receiver) to access the channel during a time interval needed to transmit ACK. Neighbour stations learn about the length of this time interval from the Duration field of the data frame.

Exclusion of the Duration field from short frames (not from NDP MAC frames!) described in Section 4.2.1 disables NAV mechanism, so TGah develops another virtual CS mechanism, called Response Indication Deferral (RID).

The RID mechanism is similar to NAV. Both NAV and RID can be presented as timers counting down. When the value is 0, the channel is idle. The difference between RID and NAV is that RID is set just after reception of the PHY header, while NAV requires the whole frame to be successfully received (with correct checksum). Also, in contrast to NAV, which obtains accurate information about expected transmission duration, RID estimates the duration based on the type of response stored in the 2-bit Response Indication field of the PHY header of the recently received frame. The standard defines four types of response.

1. *Normal Response* sets RID to *SIFS* plus time needed to transmit either ACK (16-byte MPDU) or BlockAck (32-byte MPDU) depending on whether the received frame is normal or aggregated. This time depends on the channel width and data rate used for control frames according to the legacy rules.
2. *NDP Response* sets RID to *SIFS* plus the duration of an NDP MAC frame (which does not depend of data rate).
3. *No Response* (e.g., used for broadcast frames) resets RID to zero, indicating that the channel is idle.
4. *Long Response* sets RID to *SIFS* plus duration of the longest possible transmission, see Table 3. This mechanism is used in Bi Directional TXOP⁹ (BDT) described below and TXOP Sharing described in Section 4.5.3.

⁸Because of paper space limitation, we omit their description, assuming that the reader is aware of them, at least of DCF (Distributed Coordination Function).

⁹Originally, it was called Speed Frame Exchange.

Draft. For internal usage only

BDT is similar to Reverse Direction (RD) protocol which can also be used in .11ah. However unlike RD, it allows to implicitly acknowledge frame reception without sending ACK, which is very profitable for .11ah since .11ah PHY has much longer SIFS and PHY symbol duration than, say, .11g. So removing ACK (or NDP ACK) and corresponding SIFS from frame exchange sequence allows to save at least 400 us or 720 us for ≥ 2 MHz and 1 MHz channels, respectively.

Another difference from RD is that with BDT an AP and a non-AP station *exchange in turn* SIFS-separated data frames within one TXOP. Such an exchange is protected by RID: all frames except for the last one are transmitted with Response Indication field set to Long Response. Each frame acknowledges the reception of the last frame sent in the opposite direction. For error recovery, the next attempt is made when the medium is idle for PIFS.

Apart from reducing overhead, BDT eliminates contention and saves energy: BDT shortens and hastens frame exchange allowing stations to return to doze state earlier.

Another significant advantage of BDT is its simplicity and no need in any preliminary handshake: to start BDT, a so-called BDT initiator sends a frame with Response Indication field set to Long Response to BDT responder. If both BDT initiator and BDT responder have equal number of frames, they exchange them in turn. If the BDT responder has no frames, but immediate acknowledgement is required, it sends either NDP ACK or NDP BlockAck. For the case when the BDT responder has more frames than BDT initiator, BDT responder is allowed to send several frames in a row (BDT response burst). If acknowledgement is required, BDT initiator sends NDP ACK or NDP BlockAck after the burst.

Including information about response in the PHY header has some advantages and drawbacks compared to legacy DCF. In case of No Response, RID prevents wasting channel resource by a station which has started frame reception (i.e., has successfully received PHY preamble and PHY header) but has not succeeded (MAC FCS has been wrong). In contrast, in spite of enabling several improvements, RID may block stations in vain. Let us describe both cases in detail.

No Response In legacy .11 networks, ACK transmission is protected with NAV and EIFS. NAV can be set by a station only when it successfully receives the frame and FCS is correct. Otherwise, i.e. FCS is not valid, the station

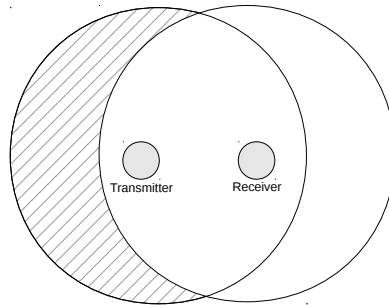


Figure 6: Hidden area example.

shall wait for EIFS instead of DIFS after channel becomes idle to allow ACK, if any, to be transmitted without collision. EIFS is larger than DIFS by SIFS plus the time needed to transmit an ACK at the lowest rate. It should be noted that in legacy networks, it is impossible to define whether
485 ACK is required or not for a frame with incorrect FCS. If many frames are transmitted without ACK, edge stations which cannot correctly receive frames wait extra time. While in legacy .11 networks this time is negligible, in .11ah it may last up to 720 us, which is definitely a notable overhead.

RID improves this situation in .11ah networks, making stations wait extra
490 time only when it is needed. Since ACK protection is guaranteed by RID, no EIFS is needed (for compatibility, EIFS equals DIFS in .11ah).

Long Response If a frame needs Long Response by the receiver, it means that the channel becomes busy for all stations in the transmitter neighborhood (except for the receiver) during a fixed (and long!) time interval. If the
495 receiver needs less time than reserved for the response, it shall release the channel afterwards. For that, the receiver uses Response Indication in the frame sent as the response. Having received it, stations shall update their RID timers according to the new value. In other words, in contrast to the NAV timer, which is never updated to lower value on frame reception, .11ah
500 allows the RID timer to be updated even if its current value is higher than the new one.

However, the stations from the gray area in Fig. 6 are hidden from the receiver: they get the first frame but do not get the second one, and so they do not update their RID timers. This decreases amount of available channel
505 resources for them, and increases packet service time and power consumption. Thus, use of Long Response may not be efficient in case of hidden stations. However, exact cases favourable for Long Response are still not studied.

Draft. For internal usage only

Finally, let us consider joint usage of RID and NAV. With a physical and
510 two virtual carrier sense mechanisms, a .11ah station considers the channel
as idle only if none of them indicates that the channel is busy. Since NAV
is more accurate than RID, its value shall have the larger weight. So RID is
reset to zero each time when a frame with the Duration field is received.

4.3.2 Restricted Access Window

515 To decrease collision probability in networks with thousands of stations
and thus to improve power efficiency, TGah has developed Restricted Access
Window (RAW) described in this Section. The key idea of RAW is to limit
the set of stations accessing the channel and to spread their access attempts
over a long period of time. In other words, RAW divides stations into groups
520 and splits the channel into slots. Then it assigns each slot to a group. Stations
can transmit only in their slots. Let us describe RAW in detail.

By broadcasting in beacons special RAW Parameter Set (RPS) infor-
mation elements, the AP allocates one or more restricted medium access
intervals, called RAW. During RAW, only a set of STAs determined by the
525 lowest and the highest AIDs, both from the same page (see Section 4.2.4),
can access the medium [30].

Each RAW consists of $N_{RAW} < 64$ equal time slots corresponding to
various stations. Due to the frame format, if $N_{RAW} < 8$, each slot may
reach 246.14 ms. Otherwise, the slot duration is limited to 31.1 ms. During
RAW, each station is forbidden to access the channel before its slot, which
is calculated as follows:

$$i_{slot} = (x + N_{offset}) \mod N_{RAW}, \quad (1)$$

where N_{RAW} is the number of slots, N_{offset} is a parameter to improve fairness
and equals two least significant bytes of the beacon FCS, and x is determined
as follows. If the RAW is restricted to stations with AID bits in the TIM
530 element set to 1, x is the position index of the station among others. Other-
wise, x is the station AID. Note that rule (1) means that a group of stations
may access the channel in a slot.

To access the channel in its RAW slot, a station uses EDCA. However,
backoff functions inside and outside RAW are different, since contention con-
535 ditions differ. At the beginning of the RAW, the first backoff function (values
of backoff counters, retry limits, contention window) is suspended and saved,
and the station initializes (but does not restore) new backoff function ac-
cording to an access category (AC) which is set as RAW AC. This backoff
function is used till the end of RAW, when the first backoff state is restored
540 and resumed [31].

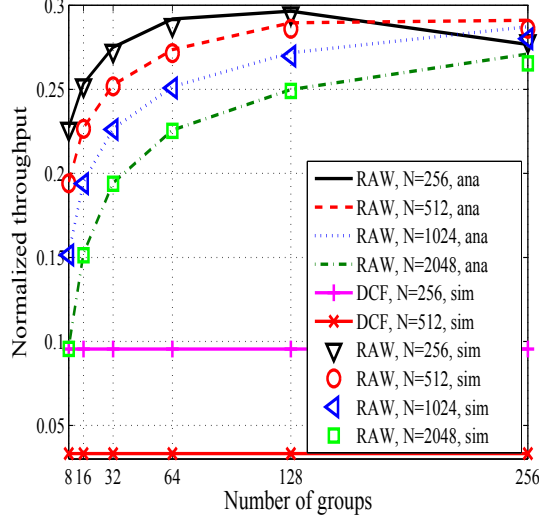


Figure 7: RAW vs DCF normalized throughput obtained with simulation (sim) and analytical model (ana) [32].

As shown in [32], dividing stations into groups and assigning an access slot to each group allow to significantly increase throughput. Fig. 7 compares throughput achieved with RAW and legacy DCF in a scenario with N stations and saturated traffic. While DCF provides almost zero throughput with $N = 256$ stations, RAW gives rather high throughput even in case of 2048 stations.

When number of groups equals N , the only station transmits in each slot. However, normalized throughput is less than 1 (which shall be in case of TDMA), since stations shall count down backoff in their RAW slots, which results in waste of channel resources. To reduce it an AC with low contention (e.g., AC_VO) shall be used as RAW AC.

The AP optionally allows stations to exceed their slots (Cross Slot Boundary) when transmitting or counting down backoff [31]. However, in this case, stations that wake up at the beginning of the next slot should wait until frame exchange ends or the channel is free for the Probe Delay interval before starting contention. If the AP does not allow to Cross Slot Boundary in RAW, stations may awake at the beginning of their slots and start contending for the channel immediately. Although restriction of Cross Slot Boundary provides fair resource allocation (the stations from the first slot do not contend in next slots), it may lead to the waste of channel resources when the slot is not ended yet but the remaining part is not enough for the whole frame

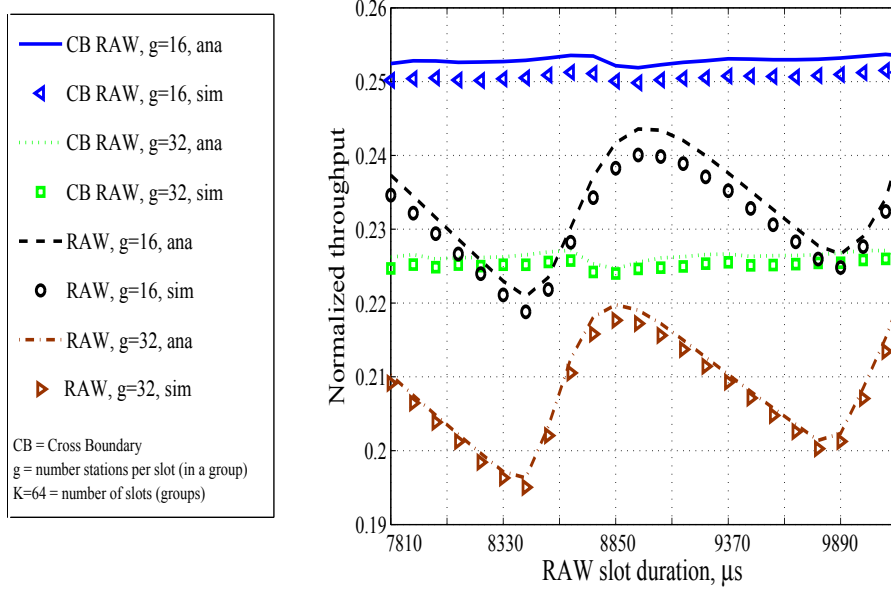


Figure 8: Dependence of throughput on RAW slot duration with/without Cross Slot Boundary (CB RAW/RAW) obtained with simulation (sim) and analytically (ana) [32].

transmission. It results in non-monotonic dependence of throughput on slot duration without Cross Slot Boundary, see Fig. 8 [32].

To reduce the overhead in case of periodic traffic, TGah develops a Periodic RAW (PRAW). PRAW is determined by the following parameters:

- period of PRAW (in units of short beacon intervals),
- offset from the end of the frame carrying information about RAW (in units of short beacon intervals)¹⁰,
- for how long PRAW is valid (the number of remaining PRAW occurrences).

When RAW is used for data transmission (Regular RAW), it reduces contention between stations and protects data frames from collisions. It also improves power efficiency, since station can sleep during alien slots [31]. Apart from Regular RAW, the draft standard describes other applications of this mechanism.

¹⁰Such an approach to describe a periodic set of reserved time intervals is close to that used by MCCA, deterministic channel access in Wi-Fi Mesh networks. It means that some scientific results (mathematical models [33], or algorithms [34]) can be applied to RAW.

Draft. For internal usage only

Sounding RAW protects signal frames, used by SST (see Section 4.4.8) or Sector sounding (see Section 4.3.4).

AP Power Management RAW can be used by AP to indicate time intervals during which AP is sleeping.

580 Non-TIM RAW protects transmission of so-called non-TIM stations, which do not wake up even to receive beacon and thus can operate for ages, see Section 4.4.5.

Triggering Frame RAW organizes polling. During the first RAW interval stations can transmit in their slots only one frame (if any) shorter than 1.7
585 ms, e.g., a PS-Poll frame. Based on the received frames, the AP determines the structure of next RAW intervals, during which stations can transmit or receive series of frames.

Although the efficiency of RAW in these cases as well as its applicability for M2M traffic may be apparent, the confirmative figures as well as algo-
590 rithms to group stations are still open issues.

4.3.3 Fast Association and Authentication

While RAW limit the number of associated stations contending for the channel, it cannot improve channel access at the stage of network initialization. When an AP is deployed, or after a power outage, large number of
595 stations are simultaneously trying to obtain a connection with the AP. This process consists of several frame handshakes. The first one is the authentication procedure.

If about 6000 stations try to authenticate at the same time, most authentication requests will not be received due to collisions. Even having received
600 a request, the AP cannot access the channel to respond. Even for 100 stations, the time required for all of them to finish the authentication procedure can exceed 5 min, see Fig. 9a.

The similar problem (fast initial link setup) is being solved by TGai (IEEE 802.11ai). However, firstly, TGai deals with dozens to a couple of hundreds
605 of stations while .11ah shall support up to 6000 stations. Secondly, the work in TGai is still ongoing. So, to address the issue, TGah has developed two authentication control mechanisms limiting contention: centralized and distributed ones.

Centralized authentication control works as follows. The AP includes in
610 each beacon Authentication Control Threshold selected according to some implementation dependent rule. The AP may change this value dynamically. When a station is initialized, it shall generate a random value from interval $[0, 1022]$. Having received a beacon, the station tries to associate with the AP only if its value is less than the received Authentication Control Thresh-

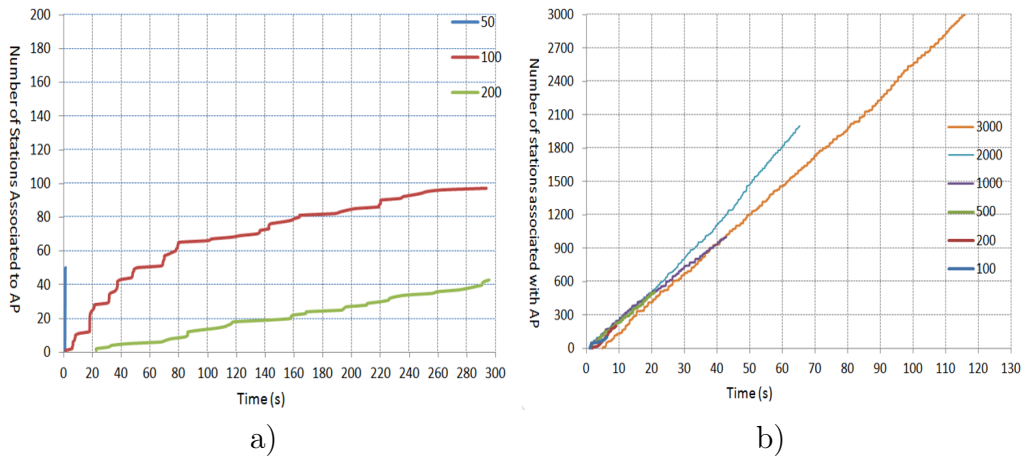


Figure 9: Authentication & association process for various number of stations: a) legacy, b) centralized authentication mechanism [35].

old. Otherwise, it shall postpone authentication till the next beacon. To avoid unfairness in the future, the station may regenerate its random value after authentication is finished. A method to adjust Authentication Control Threshold is proposed in [35]. With such a method, 100 stations connect successfully in just few seconds and 1 min is enough for 2000 stations to connect, see Fig. 9b.

When using centralized authentication mechanism, an AP can also defer authentication of actively scanning stations. When the AP receives a probe request from a station, it can include Authentication Control element with deferred channel access time in probe response instead of threshold. This way the AP can precisely control stations that actively scan for APs with probe requests, while still control other stations with Authentication Control Threshold.

Distributed authentication control is based on the truncated binary exponential backoff. Each beacon interval is divided into slots of equal duration T_{ac} . Prior to sending Authentication Request, each station selects two random values: l and m . l is uniformly distributed at $[0, L]$, where L is the number of whole slots in a beacon interval. m is uniformly distributed at $[0, TI]$, where TI is the transmission interval initialized to TI_{min} . After that, the station initiates normal EDCA access procedure in beacon interval m and slot l (numeration starts from 0) and transmits an authentication request. After each unsuccessful authentication attempt TI is increased as follows: $TI = \min\{2TI, TI_{max}\}$. By default, $T_{ac} = 10.24\text{ms}$, $TI_{min} = 8$, $TI_{max} = 256$.

To our best knowledge, the efficiency of centralized and distributed au-

Draft. For internal usage only

640 authentication control mechanisms have not been compared yet. Also an open issue is how to avoid collisions of authentication requests and traffic of already associated stations. So, these questions can be topics for future research.

4.3.4 Group Sectorization

645 Since the stations located at opposite edges of the network cannot hear transmissions of each other, and the number of stations is very high, hidden stations problem is very critical for .11ah networks. The Sectorization mechanism developed by TGah addresses this issue, limiting the number of stations accessing the channel, based on their positions.

The main idea of Group Sectorization is based on combined use of space- and time-division multiplexing. The AP divides the space into several spatial sectors. During association procedure, station obtains from the AP an ID of the sector which it belongs to. Then the AP divides the time into Sector Intervals. Each Sector Interval begins with a beamformed beacon, saying which sectors are allowed to access the channel during this Sector Interval. If a station does not belong to the sector, it is forbidden to access the channel.¹¹ 665 The AP can define some Sector Intervals as omni directional, i.e. any station can transmit frames during these intervals. Also sector intervals may overlap. In this case, more than one sector can be active.

As shown in Section 4.3.2, grouping stations manifold increases throughput with respect to pure DCF. In case of hidden stations, location-aware 660 grouping brings even more benefits avoiding starvation effect and allowing spatial reuse. Similar to RAW, in addition to improving throughput, Group Sectorization enhances power efficiency, since devices can sleep in non-active intervals.

The reasonable question is why RAW is not enough for grouping. The 665 answer is related to implementation complexity of RAW, which limits its usage in small and cheap sensor devices. In contrast, Group Sectorization is based on a rather naive location-aware method. Anyway, being optional, two methods addressing similar issues improve flexibility of .11ah.

4.3.5 Overlapping BSS

670 Since the transmission range of .11ah devices reaches 1 km, the situation when several BSSs operate at the same frequencies and area is very typical and should be taken into consideration by the standard developers. To improve co-existence of Overlapping BSS (OBSS) and to allow spatial reuse of

¹¹However, Group Sectorization is not mandatory, and stations which do not support it can transmit data during any Sector Intervals.

Draft. For internal usage only

wireless channel, TGah extends the idea of sectorization and beamforming
 675 described in Section 4.3.4.

In particular, TXOP-based Sectorization scheme allows stations of a BSS
 and stations of an OBSS to transmit their data simultaneously. Let us con-
 sider how TXOP-based Sectorization operates.

680 During the sectorized beam transmission, other “spatially orthogonal”
 OBSS STAs and APs cannot receive the signal, which gives an opportunity
 to start another transmission until the end of the current TXOP without
 any interference, see Fig. 10. The draft standard describes four ways to
 implement such an opportunity.

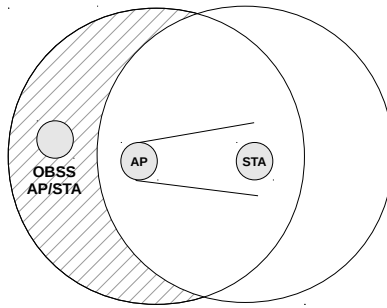


Figure 10: OBSS example

- 685 • Way 1. The AP starts transmission using omni-beam with the first
 frame that sets up NAV protection for the duration of the sectorized
 beam transmission. After receiving an ACK from the station involved
 in transmission, the AP sends the second frame with a long PHY
 header. While transmitting the PHY header, the AP switches from
 690 the omni-beam to the sectorized-beam transmission and stays in this
 mode till the end of TXOP. If an OBSS AP or an OBSS station receives
 omni-transmissions of the AP and neither the sectorized transmissions
 of the AP nor ACK sent in response, it can start its own transmission
 not exceeding the sectorized TXOP duration (see Fig. 11).

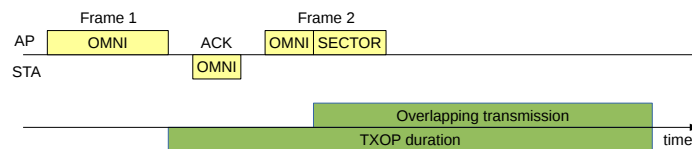


Figure 11: TXOP-based Sectorization. Way 1.

Draft. For internal usage only

- 695 • Way 2 is the same as Way 1, except for the usage of two frames with short PHY headers (transmitted omni and sectorized, correspondingly) instead of the frame with long PHY header.
- 700 • Way 3 is similar to Way 1 and Way 2. The difference is that the AP and the station first make a RTS/CTS handshake using omni-transmissions. Then the AP sends either a frame with long PHY header (as in Way 1) or two frames with the short PHY headers (as in Way 2).
- 705 • Way 4 is similar to Way 1 and Way 2. The difference is that the frame exchange sequence starts with a PS-Poll frame sent by a station. Then the AP omni-transmits a frame which is acknowledged. After that the AP transmits either a frame with long PHY header (as in Way 1), or a frame with short PHY header (as in Way 2), during which the OBSS AP and station can access the channel.

The gain of spatial reuse and the cost for that (i.e., increasing packet error rate) depend on chosen way. So, this issue should be carefully studied.

710 To facilitate the detection of spatial orthogonality by OBSS stations or OBSS APs, the AP may use the legacy CTS-to-self mechanism. In the NDP CTS frame sent prior to frame transmission, the AP can set Early Sector Indicator which notifies that the NDP CTS frame is followed by the sectorized beam frame exchange. It allows OBSS stations to cancel their NAV if they receive omni-transmissions of the AP and neither the sectorized transmissions
715 of the AP nor ACKs sent by the station.

Specific criteria how to choose sectors are out of scope of the standard. However, the draft specifies special procedure called Sector training operation. With this procedure, the AP transmits a sequence of NDP sounding frames. As a result, stations can respond to the AP with statistics about the received signal quality. With this information, the AP can reassign Sector
720 ID for the STAs.

4.4 Power Management

4.4.1 Brief Overview of the Power Management in IEEE 802.11

725 The key idea of numerous power management mechanisms used in IEEE 802.11 networks is based on alternating between two states: awake and doze. In the awake state, a station can receive and transmit frames. In the doze state, a station switches off radio module and can neither receive nor transmit. A station can work in two modes: in power save (PS) mode, it alternates between these states, while in active mode it is always awake.

730 In infrastructure networks, a station shall notify the AP before it changes the mode. If the station is in the PS mode, the AP buffers all frames (except for some kinds of management frames) destined for this station. To notify PS stations about buffered packets, the AP includes TIM in each beacon. TIM indicates the presence of packets destined for each station. Periodically,
745 beacons contain the Delivery Traffic Indication Map (DTIM) element, saying whether the AP has buffered groupcast packets. Groupcast packets are transmitted just after such a beacon.

A PS station periodically wakes up to receive a beacon. It does not need to listen to each TIM element, so it can sleep for Listen Interval which can
740 be much longer than Beacon Period. Although the standard does not require it, in practice, PS stations wake up just before DTIM beacon. It should be noted that having a frame to transmit, a station wakes up earlier than it is scheduled, however it shall wait for a frame reception to start accessing the channel (but not longer than Probe Delay which is implementation dependent
745 and may be comparable with beacon interval).

If no buffered packets are destined for the station, it returns to the doze state just after the beacon. Otherwise, the station sends a PS-Poll frame after groupcast transmission. As a response to PS-Poll, the AP sends buffered frames.

750 Strictly speaking, IEEE 802.11 Power Management has many features favorable for .11ah use cases [36], however their efficiency is not enough.

- The AP does not disassociate a station due to non-receipt of frames from it during BSS Max idle period, which can reach 18 hours. However, some use cases require that a sensor lives years without battery replacement, sending a packet once a month or even rarer.
755
- WNM-Sleep mode (an extension of PS mode) allows a station to signal to the AP that it will be sleeping for a specified number of DTIM intervals, but even receiving beacons consume energy, which decrease battery lifetime.
- 760 • Automatic Power Save Delivery (APSD) enables a station to retrieve traffic buffered at the AP by sending trigger frames at anytime without having to wait for a beacon frame. However trigger frames are not protected from collisions, which can lead to high power consumption caused by repetitive transmissions in case of a network with thousands
765 of stations.
- Power Save Multipoll (PSMP) allows the AP to assign an interval to each station waking in a particular beacon period. Every Listen Interval, each station wakes to receive its schedule, then depending on

770 the schedule, it may go to the doze state and wake up again before
its scheduled time. However the schedule advertisement overhead is
so high – 8 bytes per station – that it is definitely unacceptable for
networks with thousands stations working at the lowest MCS. Also it
is not acceptable for uplink scheduling in case of huge number of sta-
775 tion if only few of them have frames to transmit. Finally, PSMP may
schedule a transmission not far than 8 ms from the end of the frame
carrying this schedule, which is insufficient for .11ah with very long
time characteristics.

- Direct Multicast Service (DMS) enables a station to request the AP
780 to transmit group addressed frames destined for this station as indi-
vidually addressed frames, improving frame delivery for those stations,
which do not wake up at every DTIM beacon. However, the price for
reliability is high overhead caused by individual transmission.

Thus, power management enhancements already included in the IEEE
802.11 standard [20] by 2012 are insufficient for the use cases described in
785 Section 2, and Power Management is significantly improved in .11ah. Apart
from extension of possible doze state duration, the standard focuses on how
to efficiently organize channel access for large number of stations aiming to
transmit after a beacon, and how to reduce power consumption caused by
frame transmission/reception. In further subsections, we refer to these issues
790 in detail.

4.4.2 Insufficient duration of doze state duration

In .11 networks, the duration of the doze state is limited by Max idle
period, after which the AP de-associates doze station. The value of Max
idle period is chosen by the AP and transmitted to stations during their
795 association in a 16-bit field as a number of 1.024 ms time units. Thus, the
maximal value is $(2^{16} - 1) \cdot 1024/3600 = 18.64$ hours. However, some use
cases require doze state duration much longer than 18 hours. For example,
gas detectors only need to transfer alarm messages and may sleep months or
even longer [37, 38]. To avoid being de-associated, they would need to send
800 keep-alive messages, wasting energy. To reduce energy consumption, TGah
develops 2 solutions modifying Max idle period usage.

The first one is the use of two the most significant bits of the Max idle
period field as a scaling factor. Values 00, 01, 10, 11 represent scaling factors
1, 10, 1000, 10000 respectively. This way maximal value of Max idle period
805 is $10000/4 = 2500$ times greater.

Draft. For internal usage only

The second one allows the AP to set different Max idle period for various stations. Moreover, a station can request specific Max idle period in its association request.

In the same way, TGah has extended WNM-Sleep interval to improve
810 power efficiency in sensor scenarios.

4.4.3 Station classification

Different stations may support different types of services which may have different requirements on QoS, packet size, duty cycle etc. To address directly the requirements imposed by various devices which can work in .11ah
815 networks according to the approved use cases, TGah defines several types of stations.

First of all, TGah divides PS stations into two groups. While some stations (referred to as TIM stations) periodically wake up to receive beacons, others (non-TIM stations) require long doze states to work for years from
820 a single battery. TGah enhances power management framework addressing both types of stations, see Sections 4.4.4, 4.4.5.

Independently, TGah divides all stations into two groups.

Sensor stations Also referred to as Z-class stations in TGah internal documents, they transmit low traffic of short packets. Sensor stations are also
825 expected to have limited available power. The number of sensor stations associated to an AP may reach 6000.

A sensor station may have limited capabilities, e.g., it can implement a single AC which shall be AC_BE¹².

A sensor station powered by a small energy supply can be limited in
830 its ability to transmit or receive in some time intervals. For example, it can transmit only few frames, after that it needs to recovery for some time interval.

Such a station can specify their Max Awake Interval during association or later if needed. Other stations shall not schedule frame transmission to
835 the power limited station or cause it to transmit, if such a transmission exceeds Max Awake Interval following the most recent transition from Doze to Awake. The exact transition moment is unknown, however stations can estimate using information about beacons, or recent transmissions.

Similarly, an energy harvesting station (which derives energy from external sources, e.g. solar power, thermal energy, wind energy, salinity gradients,
840

¹²Note that in contrast to .11, in .11ah AC_BE has the highest priority since it is used for sensor traffic

Draft. For internal usage only

and kinetic energy) may indicate in NDP ACK that it needs some Recovery Interval, and switch to the Doze state.

Offloading stations Also referred to as H-class stations, they transmit intensive traffic, including video streams. This type includes laptops, wireless cameras, gadgets offloading data. It is unlikely that more than a hundred of such devices are associated to an AP.

Since these types of station require different configuration, TGah defines three modes [39] of BSS operation:

- Sensor Only BSS,
- Non-sensor only BSS, containing only non-sensor networks,
- Mixed mode, when the AP supports both sensors and non-sensors.

BSS of various types can be separated spatially or by assigning different channels, limiting the influence of non-sensor stations on the sensor ones.

4.4.4 TIM Slicing

In the current version of the .11 standard, beacons trigger PS station contention for the channel, which is the bottleneck of the whole power management framework.

For many reasons, polling used by Point/Hybrid Coordination Function (PCF/HCF) is not efficient with a large number of stations, most of which have no data to transmit. First of all, it leads to a huge overhead caused by polling requests. Then, it requires sensor stations to be active and to consume energy till they are polled. The lack of the energy efficient mechanism to eliminate contention has made TGah develop several mechanisms.

This Section presents the TIM Slicing mechanism which is used to eliminate contention of TIM stations. Another mechanism, for both TIM and non-TIM stations, is described in Section 4.4.5.

TIM Slicing allows to split information transmitted in TIM into several slices and to transmit TIM slices separately, see Fig. 12. Periodically, some DTIM beacons contain one or several Page Slice¹³ information elements (PSIE), *unique for each page*. which describe how TIM is split into slices.

PSIE contains information about Page Period, which is the interval between DTIM beacons containing consequent PSIEs. Also PSIE indicates

¹³Previously, it was called Segment Count.

Draft. For internal usage only

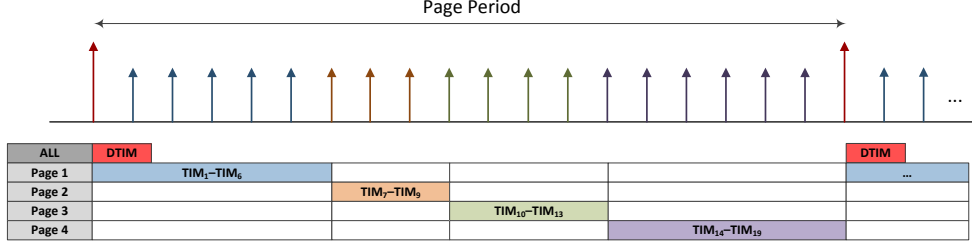


Figure 12: A TIM segmentation example.

number of TIM slices, their positions regarding current beacon, number of
875 blocks in each slice, etc. Apart from that, PSIE includes a Page Bitmap
which indicates the presence of buffered data for each of block in all the slices.
Thus, having received an PSIE, the station obtains information whether the
AP has buffered data destined for its block or not. If not, it can sleep until
the end of the page period. If the AP has frames destined for its block,
880 and the corresponding TIM slice is not included in the received beacon, the
station calculates the moment when this TIM slice is transmitted, and stay
doze until that moment.

Ideologically, TIM slicing is rather similar to PSMP, however it is designed
completely in a different way. Thus, TIM Slicing is more scalable, simpler
885 in implementation and generates much less overhead, which is critical for a
.11ah network operating at the lowest MCS.

4.4.5 Target Wake Time (TWT)

Stations which transmit data rarely can reduce power consumption by
refusing to receive beacons. To reduce contention, the AP schedules channel
890 access times for each PS station. A mechanism which implements such idea
is Target Wake Time (TWT).

TWT allows the AP to schedule a series of times for a station (called TWT
station) when the TWT station wakes up for some time interval (called TWT
Service Period or TWT SP) and exchanges frames. Due to this mechanism,
895 the TWT station can stay in the doze state always except for TWT SP
intervals. TWT stations are not required to wake up even for beacons [40],
eliminating energy consumption. Therefore, they can operate in non-TIM
mode.

To setup a TWT, either an AP or a station starts TWT negotiations.
900 During negotiations, they transmit to each other a special information el-

Draft. For internal usage only

ement which contains TWT parameters and can be interpreted as request, suggestion, demand, alternation, acception, dictation, or rejection. Unfortunately, the draft standard does not specify how to use all these levels of persistence. Either AP or the TWT station can teardown the TWT by
905 transmitting a TWT Teardown frame.

The most important TWT parameters are

- Target Wake Time indicating when the first TWT interval begins;
- Minimum Wake Duration indicating minimum value of TWT SP;
- Wake Interval, which is the period of TWT intervals (represented in
910 exponential form to cover vast range of values);
- Direction defining whether the AP or the station shall transmit the first frame during each TWT interval;
- Flow ID, which is used to distinguish up to 8 TWTs set up by a station for various flows, e.g. when they require different TWT parameters
915 values;
- channels on which the station is allowed to transmit during TWT SP (see Section 4.4.8);
- whether the TWT is implicit or explicit (see below).

At the beginning of each TWT interval, the TWT station schedules the
920 next TWT interval Wake Interval later than the current TWT interval. If TWT is always calculated in such a way, TWT is called implicit. Otherwise, it is called explicit TWT and it works as follows. The AP transmits to the station information about the next TWT interval, using one of the short control frames (see Section 4.2.1) referred to as TACK (TWT Acknowledgment), STACK (Short TWT Acknowledgment) or BAT (Block Acknowledgment TWT) frame. During TWT interval, the AP may transmit this
925 information more than one time, in this case the station uses the most recent information.

Stations transmit frames in TWT SP using legacy channel access methods. Since the standard does not forbid TWT stations to transmit outside
930 the TWT intervals, frames sent in TWT SP are not protected from collisions. To protect the frames from collisions with TIM stations, the AP may use NAV (as in Section 4.4.6) or RAW 4.3.2.

Protecting each TWT separately increases overhead. To reduce it, TGah
935 suggests to group them, i.e., to allocate them side by side in time. TWT

grouping mechanism allows the AP to create TWT groups and inform stations about them [41]. When a station requests a TWT, the AP assigns the TWT to an appropriate group. Neighboring TWTs in a group are equidistant from each other. Since the duration of TWT SP is not fixed, the distance
940 between TWTs is chosen by an implementation dependent algorithm, which can take into consideration expected duration of TXOP.

4.4.6 TWT Synchronization

Since TWT stations can operate in non-TIM mode, they need to adjust their TSF (timing synchronization function) timers without receiving beacons. For that, the AP can send the value of its TSF timer in the TACK,
945 STACK or BAT frames.

In spite of time synchronization by means of TACK, STACK or BAT frames, if a station stays in doze for long, the integrate error of the TSF timer may be very high. Apart from that, the channel may be physically or
950 virtually busy by transmission of other stations which can be hidden, which may lead to collision and waste of energy. To synchronize channel state, TWT stations follow the base rule of .11 power saving: when they wakes up, they shall listen to the medium for Probe Delay before transmitting a frame. However, this listening worsens both power efficiency and latency. To
955 improve channel access in such a situation and reduce synchronization time for TWT and RAW stations, IEEE 802.11ah provides Sync frame mechanism.

If the AP supports this mechanism, a station can request the AP to transmit a so-called Sync frame (which is an NDP CTS frame) at the beginning of its RAW slot or TWT interval. The request can be done during association or later by sending Sync control frame. If Sync frame is no more need
960 a group are equidistant from each other. Since the duration of TWT Sen sends nc frames as requested if medium is not busy. Similarly the station can request the AP to stop Sync frame transmissions at any time using Sync control frames.

965 Besides the main purpose, this mechanism can be used to protect its slots or TWT intervals with NAV.

When a station receives NDP CTS frame, it should transmit its data frame after SIFS. If the transmission is not started in ACKTimeout, the AP may release medium for other stations by transmitting CF-End or NDP
970 CF-End.

The authors of the described mechanisms [42] claim that under some conditions the gain of battery lifetime may reach 70% if a station wakes up once a minute and ProbeDelay is just 0.01 sec.

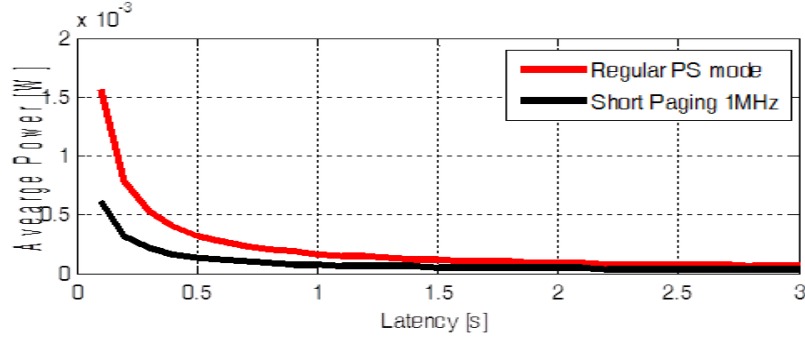


Figure 13: NDP Paging impact on battery lifetime [44].

4.4.7 NDP Paging

975 In industry scenarios, actuators shall react to commands with a very low latency [43]. It makes them check beacons for the information about buffered frames frequently. Even in case of short beacons, decoding wastes energy. To reduce power consumption, TGah proposes a mechanism, called NDP Paging, which works as follows.

980 When setting up a TWT, a station can request the AP to use NDP Paging frames. In this case, the AP sends NDP Paging frames at the beginning of TWT SP if it has buffered frames destined for the TWT station.

Having received the NDP Paging frame indicating the presence of buffered frames, the station sends a PS-Poll to the AP. If no NDP Paging frames are received, the station can switch to the doze state after a Minimal Awake Duration.

985 Apart from that, NDP Paging frames are also sent to inform the station about critical changes in beacon. Every NDP Paging frame contains Check Beacon counter, which is incremented after each critical update of beacon information. When a station detects that the value is incremented, it listens to the next beacon.

To maintain synchronization, NDP Paging frames are also sent periodically even if no events trigger them. The period is set up during the TWT negotiation.

995 Also NDP Paging frame contains the Action field which tells the station to wake up at a specific time moment, e.g. to receive beacon etc.

NDP Paging significantly reduces power consumption, see Fig. 13, as NDP frames are much shorter than the short beacons. It is possible to optimize NDP frames receiver to save even more power [43], since MAC layer is not used during reception of NDP frame. This receiver is not standardized yet.

1000

4.4.8 Subchannel selective transmission

IEEE 802.11ah network can operate in a 16 MHz channel providing high data rates. However, some stations may not need the maximal bandwidth provided by the BSS, since working in wider channels means higher energy
1005 consumption. Apart from that, stations with limited capabilities, e.g., sensor stations may support only mandatory 1 and 2 MHz channels. How can they operate in a 16 MHz BSS?

IEEE 802.11ah includes Subchannel Selective Transmission (SST) mechanism which provides an opportunity to use subchannels instead of the whole
1010 channel. The mechanism works as follows.

The AP announces SST operation within beacon interval by transmitting an SST information element in its beacons. In this element, the AP indicates which subchannels the station can use for uplink transmissions and which subchannels the AP intends to use for downlink transmissions during
1015 upcoming beacon interval. The beacon can be transmitted on a set of subchannels in parallel, in series or in a combination of the two.

Since the usage of subchannels may result in higher packet loss ratio, because the probability of deep fades is higher due to the lack of frequency diversity [45], SST allows a station to select the best subchannel.

For that, the AP periodically transmits sounding frame on subchannels
1020 in parallel, in series or in a combination of the two. Prior to sounding, the AP notifies associated station using SST elements, in which it includes information about subchannels on which it is going to transmit sounding frames. Based on the sounding signals, each station chooses the best subchannel.
1025 Transmission on this channel is an implicit report to the AP on the station's choice.

4.4.9 Flexible multicast

In .11 networks, it is possible to send multicast messages addressed to group MAC addresses. However, no mechanism is applicable to send multicast
1030 messages to a huge number of stations. If the group is large and AP has message for every station in the group, it should set to one many bits in the TIM bitmap. Even with TIM compression methods, if AIDs are not allocated sequentially, TIM size may be tremendous. Broadcasting multicast messages is often not applicable since stations that do not need the messages
1035 are wasting power [46, 47].

To solve this problem, IEEE 802.11ah includes a mechanism, which assigns so-called Multicast AIDs (MIDs) to multicast groups.

If a station belongs to a multicast group, it can request MID from the

Draft. For internal usage only

AP. In the request, the station includes its group MAC address and preferred
1040 listen period.

As various stations of the same group may have different power constraints and different preferred listen periods, the draft allows to have more than one MID for each group.

When the AP has buffered frames destined for a multicast group, it sets
1045 the corresponding bit in TIM and all the stations of the group remain Awake to receive downlink frames, while other stations do not waste power.

4.5 Relays

To improve efficiency of data transmission in the use cases described in Section 4.5, IEEE 802.11ah extends a hot-spot Wi-Fi network containing an
1050 AP and several non-AP stations with Relays. Relays forward frames between the stations associated with the Relay and the parent AP (called Root AP, as being the root node in the network topology), see Fig. 15. Thus Relays extend the distance between the Root AP and edge stations and improve reliability of data transmission in scenarios with obstructions. Another benefit of Relays
1055 is reducing energy consumed by stations in two ways. Since a station is closer to the Relay than to the Root AP, it can transmit frames (i) at lower power and (ii) at higher data rate making the transmission shorter. The latter reduces the time the station needs to stay Awake. For packets of 200 bytes, the gain may reach 30% if the distance between the AP and the station is
1060 close to 1 km and the Relay is located near the station, see Fig. 14.

Relays bring multi-hop concept into centralized network. The necessity to develop another multi-hop solution in addition to the existing mesh framework (inherited from IEEE 802.11s [49]) has a simple explanation: mesh networking protocols are too complicated to be used in battery-supplied small
1065 devices for which IEEE 802.11ah is being developed. The plain structure of mesh networks results in a heavy routing framework and distributed deterministic channel access aka MCCA – a remedy for the well-known hidden station effect – so awkward that it will doubtfully be implemented in the near future. In contrast, the Relay mechanism is much easier to implement.

1070 A Relay logically consists of two components: a Relay station and a Relay AP. A station associated with a Relay AP operates almost in the same way as being associated with a non-Relay AP.

Although it is not mentioned explicitly, the number of hops between stations and the Root AP is limited by 2. It simplifies the forwarding mechanism, ridding it from complicated path management, e.g., defined in IEEE
1075 802.11s. However, a mechanism in the forwarding framework described in Section 4.5.1 assumes paths longer than two-hop. Recently appeared in the

Draft. For internal usage only

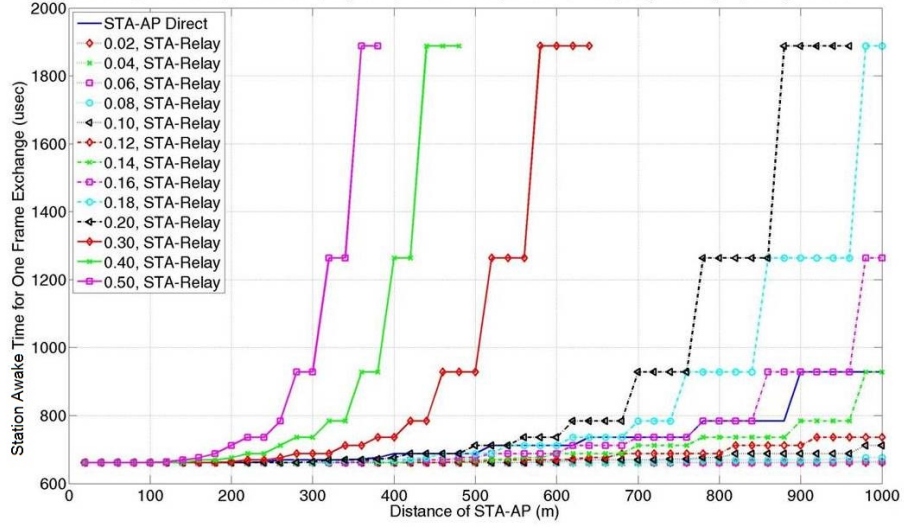


Figure 14: Relay impact on the station awake time. Each curve corresponds to a particular ratio of Relay-station distance to AP-station distance. [48]

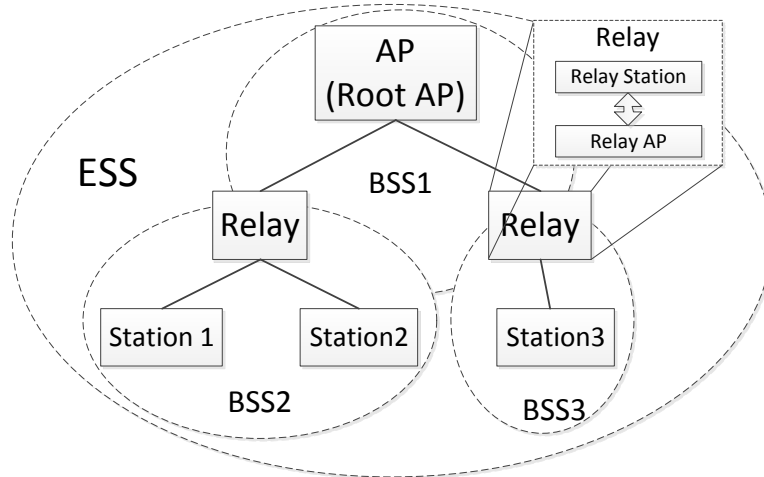


Figure 15: Network topology with Relays

Draft. For internal usage only

draft standard, this mechanism should be modified in the nearest future, so we pay the readers' attention to this discrepancy.

1080 4.5.1 Forwarding

To fill in AP's forwarding tables defining which Relay shall be used to deliver frames to a station, the AP may use a common method coming from bridging and called *backwards learning* [50]. In wireless networks, the method works as follows.

1085 After association with the Relay AP, the station starts resolution of the gateway's IP-address using ARP. Forwarding the ARP request, the Relay indirectly tells the Root AP that the station is reachable through this Relay. However, when moving between two relays in same subnetwork, the station needs not send ARP request, and may not send any frame to the Root AP
1090 for a long time. Apart from that, "smart networks" may use protocols other than ARP. All these issues prove necessity of a mechanism which guarantees the consistency of forwarding tables [51].

This mechanism works as follows. Every time a new station associates to or becomes disassociated from the Relay AP, the Relay station notifies the
1095 parent AP by sending special Reachable Address Update frame containing the list of reachable addresses. To decrease overhead, recent modifications allow to indicated only added or removed stations. However this mechanism is not defined clearly and we expect some improvements.

Also a Relay sends this frame to the parent AP when the Relay receives
1100 list of associated stations¹⁴.

Having obtained information about stations associated to Relays, the AP can forward frames destined for a station via an appropriate Relay.

Group addressed frames are firstly transmitted to the Root AP in a unicast manner. Then the Root AP groupcasts such frames to appropriate
1105 Relays, and they groupcast the frames to their associated stations.

4.5.2 Relay discovery procedure

Relay discovery procedure is organized as follows. A non-AP station performs active scanning for potential Relays using Probe Request frame with Relay Discovery element that contains information about link budget and desirable QoS requirements. A Relay that receives Probe request frame checks
1110 that link budget and QoS requirements are met and only after that responds

¹⁴This may happen only if the path from a station to the Root AP is longer than two-hop.

Draft. For internal usage only

with Probe Response frame. Information about link budget between the Relay and the Root AP may be optionally included in a Probe Response frame or Beacon frame. If non-AP station receives multiple Probe Responses, it
1115 selects a designated Relay among candidates.

4.5.3 TXOP Sharing

Relaying increases overhead, since frames are transmitted over two hops, resulting in two separate channel accesses instead of one, see Fig. 16. An additional channel access increases contention and leads to a higher collision probability. To reduce the number of contention-based channel accesses [52],
1120 IEEE 802.11ah extends BDT to allow two-hop TXOP sharing, which means that transmissions over the first and the second hops occur consequently in the same TXOP, being separated by SIFS. The recent proposal [53] has added RTS/CTS support to TXOP Sharing.

1125 TXOP sharing is only possible if both the Relay station and the Relay AP operates in the same primary channels for the duration of the TXOP.

To allow TXOP sharing, a station or the Root AP transmits a short frame (see Section 4.2.1) with the Relayed Frame bit of FC set to one; otherwise this bit is zero. If TXOP sharing is allowed, the Relay may perform either
1130 Explicit or Implicit ACK procedure.

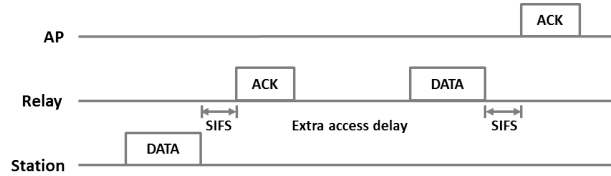


Figure 16: Usage of relays without TXOP sharing [48].

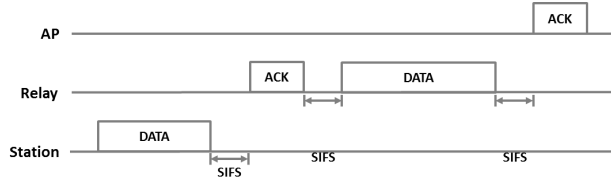


Figure 17: Usage of relays with TXOP sharing and explicit ACK [48].

Draft. For internal usage only

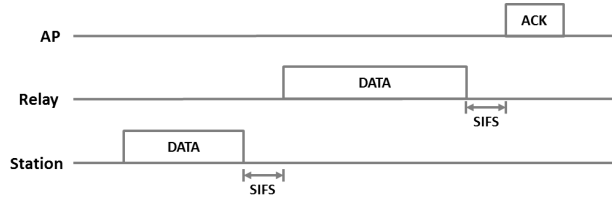


Figure 18: Usage of relays with TXOP sharing and implicit ACK [54].

Explicit ACK procedure Intended to use the explicit ACK procedure [48], the Relay acknowledges the frame received from the station by the NDP ACK frame, indicating long response. SIFS after NDP ACK transmission, the Relay forwards the frame to the AP, see Fig. 17.

1135 Meanwhile after receipt of acknowledgement, the source defers the next transmission for the time needed the relay to transmit a frame and to receive an ACK. For the next transmission, stations shall use a new TXOP.

Implicit ACK procedure To further improve MAC efficiency, [54] proposed an implicit ACK procedure.

1140 The main idea of Implicit ACK is that the Relay directly forwards frames SIFS after receipt without sending back an acknowledgment, see Fig. 18.

After transmitting a frame to the Relay, the source station waits for an ACK timeout. If during this timeout the source starts receiving a frame with corresponding Partial AID (PAID) value in the PHY header, the source
1145 assumes that the transmission was successful.

PAID is a hash of the receiver's AID. PAID mechanism has been developed in .11ac and enhanced in .11ah. Due to PAID subfield of the frame PHY header, a station can determine that the frame is destined for another station by decoding only its PHY header. In .11ah only ≥ 2 MHz PHY
1150 headers includes PAID, so implicit acknowledgement cannot be used with 1 MHz PHY.

For the downlink implicit ACK, the Root AP shall know PAID of stations associated with Relays. For this purpose, Relays may indicate an associated stations' AID by sending a special frame when a station becomes associated
1155 or its AID is changed.

For the uplink implicit ACK, the stations associated with the Relay shall know BSSID (which is used to calculate PAID) of the Root AP. For this purpose, a Relay AP may indicate the Root AP's BSSID by using Root AP BSSID field in the Relay element in Beacon frame or Probe Response frame.

1160 Since in .11ah networks, NDP ACK duration is comparable with short

Draft. For internal usage only

frame duration (e.g. the duration of a 100-byte frame transmitted with MCS8 in 2 MHz channel is 360 us, while NDP ACK + SIFS lasts 400 us), Implicit ACK allows to significantly decrease overhead and packet transmission time.

4.5.4 Flow control

1165 Different channel conditions at the first and the second hops may cause frames to be continuously buffered at the Relay, and subsequently leading to the Relay queue overflow [55].

To avoid it, [48] and [55] propose a framework to request one or several stations to stop sending frames to the Relay until a later time¹⁵. The 1170 framework defines two new Relay Action frames. The first one, Relay Flow Suspend, is sent unicast or broadcast to stop sending frames to the Relay for the time interval indicated in it (Suspend Duration field). The second one, Relay Flow Resume, is optional. It resumes sending frames even if the interval is not expired.

1175 Apart from the Relay Flow Suspend frame, the Relay may also use BAT, TACK, STACK, and NDP ACK frames to stop transmitting data to itself by setting up Flow Control bit in these frames.

Originally developed for Relays, the Flow Control mechanism appeared to be so simple and so useful, that the area or its applicability has been 1180 tended. With this mechanism any two stations can control the flow between them.

5 Conclusion

In the paper, we provide a deep overview of the key mechanisms included in the draft standard of the IEEE 802.11ah technology, focusing on the mech- 1185 anisms motivation and related open issues.

In three years, TGah has created or modified dozens of mechanisms, which radically change the core functionality and open emerging market of smart systems for the Wi-Fi vendors. In the paper, we have explained why these mechanisms enable various scenarios useful in Smart cities, including gather- 1190 ing information from numerous sensors and cameras, controlling autonomous devices, providing wireless Internet access over wide area.

Most of the described mechanisms are just frameworks: as usual, the standard leaves decision making algorithms out of the scope, saying what to do

¹⁵Originally designed for Relays, this mechanism has been extended to any transmission in .11ah network

Draft. For internal usage only

1195 but not when or how. Apart from improving flexibility needed to meet heterogeneous requirements imposed by numerous use cases, it allows numerous researchers and engineers to study and develop high efficient solutions.

We have focused on the open issues and provide description of the mechanisms enough to model and investigate them. Thus, we believe that our paper will attract researchers to .11ah and so will contribute to .11ah investigation and to development of low-cost reliable equipment for applications
1200 which will soon change our life.

References

References

- 1205 [1] D. Evans, “The Internet of Things – how the next evolution of the Internet is changing everything,” *Cisco Internet Business Solutions Group (IBSG)*, April 2011. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- 1210 [2] (2014) Official IEEE 802.11 working group project timelines. [Online]. Available: http://www.ieee802.org/11/Reports/802.11_Timelines.htm#tgah
- 1215 [3] *IEEE P802.11ah/D1.0 Draft Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Sub 1 GHz License Exempt Operation*, October 2013.
- [4] Y. Seok, *TGah PAR Extension*, May 2014. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/14/11-14-0590-01-00ah-tgah-par-extension.docx>
- 1220 [5] W. Sun, M. Choi, and S. Choi, “IEEE 802.11 ah: A long range 802.11 WLAN at Sub 1 GHz,” *Journal of ICT Standardization*, vol. 1, pp. 83–107, 2013.
- 1225 [6] S. Aust, R. Prasad, and I. G. M. M. Niemegeers, “IEEE 802.11ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi,” in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 6885–6889.

Draft. For internal usage only

- [7] A. Hazmi, J. Rinne, and M. Valkama, "Feasibility study of IEEE 802.11 ah radio technology for IoT and M2M use cases," in *Globecom Workshops (GC Wkshps), 2012 IEEE*. IEEE, 2012, pp. 1687–1692.
- 1230 [8] T. Adame, A. Bel, B. Bellalta, J. Barcelo, J. Gonzalez, and M. Oliver, "Capacity analysis of IEEE 802.11 ah WLANs for M2M communications," in *Multiple Access Communications*. Springer, 2013, pp. 139–155.
- 1235 [9] R. P. Liu, G. J. Sutton, and I. B. Collings, "Power save with offset listen interval for IEEE 802.11 ah smart grid communications," in *Communications (ICC), 2013 IEEE International Conference on*. IEEE, 2013, pp. 4488–4492.
- 1240 [10] Y. Zhou, H. Wang, S. Zheng, and Z. Z. Lei, "Advances in IEEE 802.11 ah standardization for machine-type communications in sub-1GHz WLAN," in *Communications Workshops (ICC), 2013 IEEE International Conference on*. IEEE, 2013, pp. 1269–1273.
- 1245 [11] B. B. Olyaei, J. Pirskanen, O. Raeesi, A. Hazmi, and M. Valkama, "Performance comparison between slotted IEEE 802.15.4 and IEEE 802.11 ah in IoT based applications," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013, pp. 332–337.
- 1250 [12] O. Raeesi, J. Pirskanen, A. Hazmi, and M. Valkama, "Performance evaluation of IEEE 802.11ah and its reduced access window mechanism," in *Communications Workshops (ICC), 2014 IEEE International Conference on*. IEEE, 2014.
- 1255 [13] *IEEE P802.11ah/D2.0 Draft Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Sub 1 GHz License Exempt Operation*, June 2014.
- 1260 [14] R. de Vegt, *Potential Compromise for 802.11ah Use Case Document*, March 2011. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-0457-00-00ah-potential-compromise-of-802-11ah-use-case-document.pptx>

Draft. For internal usage only

- 1265 [15] M. Iwaoka, *IEEE 802.11ah Use Case – Industrial Process Automation*, February 2011. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-0260-01-00ah-tgah-use-case-industrial-process-automation.ppt>
- 1270 [16] S. Kim, *TGah Use Case - Outdoor Wi-Fi for cellular traffic offloading*, February 2011. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-0244-01-00ah-tgah-use-case-outdoor-wi-fi-for-cellular-traffic-offloading.ppt>
- 1275 [17] M. Cheong, *TGah Functional Requirements and Evaluation Methodology*, January 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-0905-05-00ah-tgah-functional-requirements-and-evaluation-methodology.doc>
- [18] D. Halasz, *Categories of Use Cases and Straw Polls*, March 2011. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-0301-02-00ah-categories-of-use-cases-and-straw-polls.pptx>
- 1280 [19] R. Banerjee, *US Channelization*, May 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-0613-00-00ah-us-channelization.pptx>
- 1285 [20] *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2012.
- 1290 [21] Z. Lei, *Extend AID and TIM in Support of 6000 STAs in 802.11ah*, November 2011. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-1550-01-00ah-extend-aid-and-tim-in-support-of-6000-stas-in-802-11ah.pptx>
- 1295 [22] *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*, December 2013.

Draft. For internal usage only

- [23] Y. Liu, *Short Ack*, March 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-0324-02-00ah-short-ack.pptx>
- [24] M. Gast, *802.11 ac: A Survival Guide*. "O'Reilly Media, Inc.", 2013.
- 1300 [25] S. Merlin, *Short Beacon*, November 2011. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/11/11-11-1503-02-00ah-short-beacon.pptx>
- [26] —, *Short Beacon*, May 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-0129-03-00ah-short-beacon.pptx>
- 1305 [27] *IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 9: Interworking with External Networks*, 2011.
- 1310 [28] M. Park, *TGah Efficient TIM Encoding*, May 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-0388-02-00ah-tgah-efficient-tim-encoding.pptx>
- 1315 [29] *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1997.
- [30] J. Kim, *RAW Assignment follow up*, May 2013. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0510-01-00ah-raw-assignment-follow-up.ppt>
- 1320 [31] Y. Seok, *Backoff Procedure in RAW*, January 2013. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0080-00-00ah-backoff-procedure-in-raw.ppt>
- [32] L. Zheng, L. Cai, J. Pan, and M. Ni, "Performance analysis of group-synchronized dcf for dense ieee 802.11 networks," *Proc. of IEEE GLOBECOM'13 (accepted)*, 2013.
- 1325 [33] E. Shvets, A. Lyakhov, A. Safonov, and E. Khorov, "Analytical model of IEEE 802.11s MCCA-based streaming in the presence of noise," *ACM SIGMETRICS Performance Evaluation Review*, vol. 39, no. 2, pp. 38–40, 2011.

Draft. For internal usage only

- 1330 [34] E. Khorov, A. Krasilov, A. Lyakhov, and D. Ostrovsky, "Dynamic resource allocation for MCCA-based streaming in Wi-Fi mesh networks," in *Wireless Access Flexibility*. Springer, 2013, pp. 93–111.
- [35] H. Wang, *Supporting Authentication/Association for Large Number of Stations*, September 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-0112-04-00ah-supporting-of-the-authentication-association-for-large-number-of-stations.pptx>
1335
- [36] L. Chu, *Enhanced power save for large BSS*, January 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-0102-02-00ah-enhanced-power-save-for-large-bss.ppt>
- 1340 [37] L. Wang, *Consideration on Max Idle Period Extension for 802.11ah Power Save*, May 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-0069-05-00ah-consideration-on-max-idle-period-extension-for-11ah-power-save.ppt>
- 1345 [38] —, *Max Idle Period Extension*, July 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-0845-00-00ah-max-idle-period-extension.pptx>
- [39] G. Calcev, *Sensor Only BSS*, September 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-1083-01-00ah-sensor-only-bss.pptx>
1350
- [40] M. Fischer, *Target Wake Times*, July 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-0823-00-00ah-targetwaketime.pptx>
- 1355 [41] C. Ghosh, *TWT Grouping and Assignment for Z-Class STAs*, January 2013. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0079-00-00ah-twt-grouping-and-assignment-for-z-class-stas.pptx>
- [42] M. P. (Intel), *AP Assisted Medium Synchronization*, September 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-0840-01-00ah-ap-assisted-medium-synchronization.pptx>
- 1360 [43] S. Merlin, *Very Low Energy Paging*, November 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-1324-00-00ah-very-low-energy-paging.pptx>

Draft. For internal usage only

- 1365 [44] —, *Very Low Energy Paging*, November 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-1324-00-00ah-very-low-energy-paging.pptx>
- [45] M. Fischer, *Frequency Selective Transmission*, November 2012. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/12/11-12-1338-00-00ah-frequency-selective-transmission.pptx>
- 1370 [46] B. Zhao, *Flexible Multicast*, January 2013. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/13/11-13-0104-00-00ah-flexible-multicast.pptx>
- [47] —, *Flexible Multicast follow-up*, March 2013. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/13/11-13-0328-00-00ah-flexible-multicast-follow-up.pptx>
- 1375 [48] E. Wong, *Two-Hop Relaying*, November 2012. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/12/11-12-1330-00-00ah-two-hop-relaying.pptx>
- 1380 [49] *IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 10: Mesh Networking*, 2011.
- [50] *IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges*, 2004.
- 1385 [51] A. Jafarian, *Reachable Address Message for Relay*, January 2013. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0076-00-00ah-reachable-address-message.pptx>
- 1390 [52] E. Wong, *TXOP Sharing Operation for Relay*, March 2013. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0288-00-00ah-txop-sharing-operation-for-relay.pptx>
- [53] A. Asterjadhi, *LB 200 Comment Resolution for TXOP Sharing*, May 2014. [Online]. Available: <https://mentor.ieee.org/802.11/dcn/14/11-14-0560-01-00ah-lb200-mac-resolution-clause-relay-txop-sharing.docx>
- 1395 [54] Y. H. Kwon, *Implicit ACK for Relay*, January 2013. [Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0075-00-00ah-implicit-ack-for-relay.pptx>

Draft. For internal usage only

- [55] E. Wong, *Relay Flow Control*, May 2013.
[Online]. Available: <http://mentor.ieee.org/802.11/dcn/13/11-13-0506-00-00ah-relay-flow-control.pptx>

1400