Wi-Fi HaLow for the Internet of Things: An Up-to-date Survey on IEEE 802.11ah Research

Le Tian[a], Serena Santi[b], Amina Seferagić[c], Julong Lan[a], Jeroen Famaey[b]

[a] *Information Engineering University - Zhengzhou, China*
[b] *University of Antwerp - imec, IDLab, Belgium*
[c] *Ghent University - imec, IDLab, Belgium*

Abstract

IEEE 802.11ah, marketed as Wi-Fi HaLow, is a new sub-1GHz Wi-Fi technology for the Internet of Things (IoT), aiming to address the major challenge of the IoT: providing connectivity among a large number of power-constrained stations deployed over a wide area. In order to achieve this goal, several novel features are introduced in IEEE 802.11ah in both the Physical Layer (PHY) and Media Access Control (MAC) layer. These features have been extensively studied from various perspectives in the past years. To provide readers with an insight into these novel features, this article provides an overview of the IEEE 802.11ah technology and conducts a comprehensive summary and analysis on the related research, revealing how to utilize these novel features to satisfy the demanding IoT performance criteria. Furthermore, the remaining issues that need to be addressed to fully realize the vision of large-scale and low power Wi-Fi networks for the IoT are discussed.

Keywords: Internet of Things, IEEE 802.11ah, Large Scale, Low Power

1. Introduction

The Internet of Things (IoT) introduces a novel dimension to the world of information and communication technology where connectivity is available anytime, anywhere for anything, which will bring significant changes to many aspects of our lives [1]. To make this into reality, it is essential to develop wireless communication technology that meets the demanding performance criteria of various IoT applications, such as long distance transmission range, large scale connectivity, low power consumption, bounded delay, and stable throughput [2].

1.1. Comparison to the Existing IoT Communication Technologies

Current low-power IoT communication technologies can be categorized into two groups: Wireless Personal Area Network (WPAN) [3, 4] and Low-Power Wide Area Network (LPWAN) [5] technologies. Table 1 provides a brief summary of these existing technologies from various aspects. As Table 1 indicates, WPAN technologies (e.g., Zig-Bee, Bluetooth Low Energy) provide medium data rate (i.e., up to a few hundred kilobits per second) at short range (i.e., tens of meters), while LPWAN technologies (e.g., LoRa, SigFox, NB-IoT, eMTC, Wi-SUN and IEEE 802.11ah) focus on long-range communications (i.e., up to tens of kilometers) and support low or medium data rate (i.e., from a few hundred bits per second to a few megabits per second). In terms of WPAN, Zig-Bee is developed based on IEEE 802.15.4 and supports a large number of devices and large coverage by the use of a mesh topology, while Bluetooth Low Energy consumes less energy. In terms of LPWAN, NB-IoT and eMTC are 5G technologies designed for IoT and operate in licensed frequency bands, while others work in ISM band. LoRa and e-MTC support high mobility, e-MTC supports critical service due to the high reliability and low latency, SigFox has the longest transmission range. Due to the short transmission range of WPAN and insufficient throughput of both WPAN and LPWAN, they are only applicable in a limited set of IoT scenarios. As such, a gap still exists for a low-power IoT communication technology that offers sufficient throughput (i.e., up to tens of megabits per second) over medium transmission ranges (i.e., a few kilometers). Therefore, the new Wi-Fi standard IEEE 802.11ah, marked as Wi-Fi HaLow, is introduced as a LPWAN technology to fill this gap, as it has the highest data rate, and medium transmission range between WPAN and most of the LPWAN technologies.

Traditional Wi-Fi technologies are designed for providing high throughput for small-scale networks with a few dozen stations and a coverage of tens of meters. They mainly employ the Distributed Coordination Function (DCF) mechanism based on Carrier-Sense Multiple Access with Collision avoidance (CSMA/CA) for channel access. To initiate packets transmission, a station first defers transmission until the channel is determined to be idle for a period of time equal to Distributed Inter Frame Spacing (DIFS) when the last packet detected on the channel was received correctly, or a period of time equal to Extended Inter frame Space (EIFS) when the last packet detected on the channel was not received correctly. After the DIFS or EIFS channel idle time, the station use Binary Exponential Backoff (BEB) mechanism to generate a random backoff period in

Table 1: A brief comparison of IEEE 802.11ah and the existing wireless technologies for the IoT.

Category	Technology	Frequency	Chanel width	Topology	Range	Date rate	Advantages	Disadvantages
WPAN	BLE	2.4 GHz (ISM)	2 MHz	star	30 m	1 - 2 Mbps	medium data rate	short distance
	Zigbee (IEEE 802.15.4)	2.4/Sub GHz (ISM)	5 MHZ	mesh	100 m	10 - 250 Kbps	large coverage	low data rate
LPWAN	LoRa	Sub GHz (ISM)	125/500 KHz	star	20 Km	300 - 500 Kbps	long distance, high mobility	low data rate
	SigFox	Sub GHz (ISM)	100 KHz	star	50 Km	100 bps	long distance	low data rate
	NB-IoT (5G)	Sub GHz (licensed)	180 KHz	cellular	15 Km	250 bps	long distance	low data rate
	eMTC (5G)	Sub GHz (licensed)	1.4 MHz	cellular	N.A.	1 Mbps	long distance, high mobility, low latency, high reliability	low data rate
	Wi-SUN (IEEE 802.15.4)	Sub GHz (ISM)	200 KHz - 1.2 MHz	mesh	1000 m	50 Kbps - 2.4 Mbps	medium date rate	medium distance
	IEEE 802.11ah	Sub GHz (ISM)	1 - 16 MHz	star	1000 m	150 Kbps - 78 Mbps	high date rate	medium distance

the range of $[0, CW-1]$ for an additional deferral time before transmitting. CW is the contention window that is set to its minimum value CW_{min} in the first transmission attempt and increases in integer powers of 2 at each retransmission, up to a pre-determined value CW_{max}. If the station senses that channel is busy at any time, it pauses the backoff procedure, and resumes after the channel becomes idle for the duration of a DIFS or EIFS. The packets transmission commence when the backoff time has expired, and the receiver send back an Acknowledgment (ACK) to confirm the reception. In addition, Enhanced Distributed Channel Access (EDCA), an extension of the DCF mechanism, is used to support service differentiation by classifying traffic into four Access Categories (ACs) with different priorities. Instead of using DIFS that has a constant value, EDCA uses Arbitration Inter Frame Spacing (AIFS) that has different values for each AC to set the deferral time before channel access.

Traditional Wi-Fi technologies have been proved a great success, becoming one of the mostly widely used wireless technologies around the world. In the past years, many variants of the above MAC layer design have been proposed for various network scenarios and objectives, such as, Time Division Multiple Access (TDMA)-based protocols for WiFi-based long distance networks [6, 7] and the coexistence of Wi-Fi and Ultra Wide Band (UWB) for indoor localization [8], Full-Duplex (FD)-MAC protocols for improving the symmetry between uplink and downlink throughput [9], and MAC protocols for networks with multi-beam antennas [10] and the coexistence of Wi-Fi and

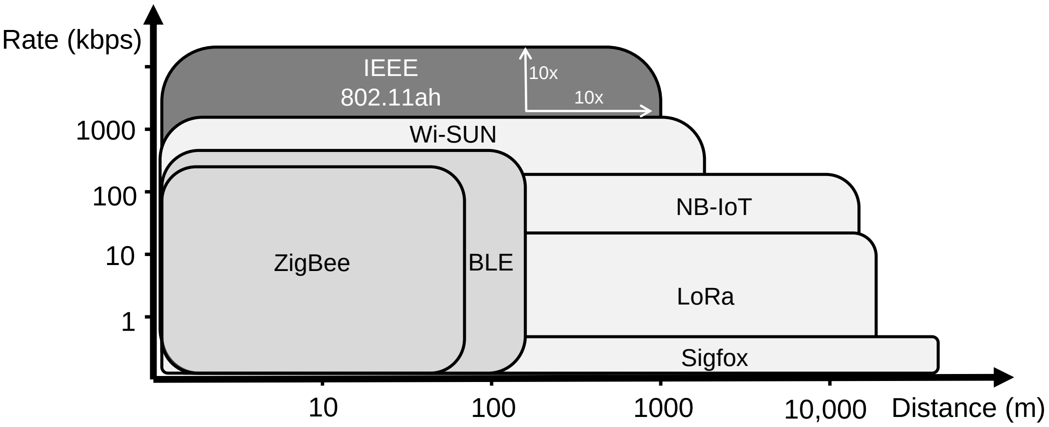


Figure 1: Position of IEEE 802.11ah compared to existing WPAN and LPWAN technologies, promising considerably extended range compared to WPAN and higher bitrate than LPWAN.

LTE [11]. However, with the emergence of the IoT, the requirements for wireless connectivity have dramatically changed. Therefore, The IEEE Task Group ah (TGah) developed IEEE 802.11ah [12] as the first Wi-Fi solution optimized for IoT applications, in order to fill the gap among current low-power IoT communication technologies. The IEEE 802.11ah Wi-Fi standard was officially released in 2016. It operates in the unlicensed sub-1Ghz frequency bands, allows up to 8192 stations to connect to a single Access Point (AP), and supports transmission ranges up to 1 km with data rates ranging from 150 Kbps to 78 Mbps with one spatial stream (cf. Figure 1). Moreover, IEEE 802.11ah introduces several new mechanisms, such as Restricted Access Window (RAW), Traffic Indication Map (TIM) segmentation and Target Wake Time (TWT), aiming to increase efficiency in face of a large amount of densely deployed, energy constrained stations. These features make it an attractive standard for long-range IoT applications, such as smart metering and monitoring, backhaul aggregation, extended range hotspot and cellular offloading [13]. In smart metering and monitoring, hundreds or even thousands of sensors located over a wide area periodically transmit short packets to the AP. In backhaul aggregation, IEEE 802.11ah can be adopted to cover the backhaul connection between IEEE 802.15.4g devices and remote servers due to its higher data rate and longer transmission range. Due to the short transmission range of legacy Wi-Fi (e.g., IEEE 802.11n/ac), IEEE 802.11ah is expected to extend hotspot range and offload traffic for mobile networks in outdoor scenarios.

As indicated in Table 1, two great players in the IoT field are IEEE 802.15.4 and 5G cellular technology. IEEE 802.15.4 is a technology that supports a wide range of IoT use cases in domains such as industrial connectivity, office automation and connected home. Various IoT protocol stacks, such as ZigBee and Wi-SUN, adopt its Media Access Control (MAC) and Physical Layer (PHY) protocols. Simulations performed in [14, 15] indicate the improvement of IEEE 802.11ah over IEEE 802.15.4 in terms of association time, throughput, latency, and network coverage range in the context of IoT. Recent studies [16, 17] further showed that IEEE 802.11ah is more energy efficient than IEEE 802.15.4 due to less signalling overhead, improving the battery lifetime up to 6 times. Besides, simulation in [14] compared the performance of IEEE 802.11ah and BLE, revealing that IEEE 802.11ah benefits from a higher throughput and lower latency jitter, whereas BLE has lower activity factors (i.e., the percentage of time a device is transmitting and receiving) and expectes a longer battery lifetime. IoT communications have been envisaged as one of the key use-cases of the 5G cellular networks. Ericsson forecasts that a significant portion of the IoT applications would be served by cellular networks in the future [18]. Although 5G machine-type communication (MTC) (e.g., NB-IoT and eMTC) brings large coverage and high performance to the IoT world, it is unlikely that 5G will make other LPWAN technologies obsolete due to their performance distinction as shown in Table 1. Moreover, a study has shown introducing IEEE 802.11ah to increase the capability of coping with massive access attempts in 5G massive Machine Type Communications (mMTC) networks significantly improves the access delay [19].

1.2. Related Works with the Existing Surveys

The IEEE 802.11ah standard provides a detailed description of the protocol (i.e., message structure and sequence) to support these new features. However, it leaves decision making (e.g., parameter configuration and optimization) to developers and users, allowing them to come up with solutions for various IoT applications and performance criteria. Since 2012, even before the standard was officially released, based on the standard draft, researchers have been investigating various aspects of the IEEE 802.11ah, especially on those key features designed for high scalability and energy efficiency. In the past years, several works have surveyed IoT communication technologies. Sinha *et al.* [20] provided a comprehensive survey on NB-IoT and LoRa, including features in PHY and MAC layers, application scenarios and current status in different countries. Seferagić *et al.* [21] evaluated the suitability of various IoT communication technologies (e.g., LoRa, IEEE 802.11ah, NB-IoT, IEEE 802.15.4g) for Industrial Wireless Sensor and Actuator Networks

(IWSAN), aiming to enable engineers to choose the most suitable wireless technology for their specific IWSAN deployment. Besides a brief description on IoT communication technologies, Fuqaha *et al.* [22] provided an overview of technical details that pertain to the IoT domains, such as identification, sensing, computation, cloud and fog computing. Moreover, Ali [23] provided a survey of IoT communication technologies (e.g., SigFox, LoRa, IEEE 802.11ah and Zigbee) to explore their potential for IoT, and further discussed available open source frameworks, cloud platforms and middleware. Although some of the above works have mentioned IEEE 802.11ah, there is a lack of details. Moreover, for the surveyed IoT communication technologies, these works focus on describing their features. In this survey on IEEE 802.11ah, the main objective is to provide not only a comprehensive overview of its features, but also analysis of the existing research in which various features are utilized to meet the demanding performance criteria of a variety of IoT applications, in order help the reader to better understand the novel features of IEEE 802.11ah.

Several works have surveyed IEEE 802.11ah [24, 25, 13, 26, 27, 28]. In 2013, Sun *et al.* [24] described the standardization activity of IEEE 802.11ah, and provided a technical overview of the IEEE 802.11ah PHY and MAC layer. One year later, Adame *et al.* [25] provided a detailed description of the features related to energy efficiency. They further conducted a performance assessment of IEEE 802.11ah in Matlab for four common Machine to Machine (M2M) scenarios, i.e. agriculture monitoring, smart metering, industrial automation and animal monitoring, demonstrating that IEEE 802.11ah is energy efficient for the evaluated scenarios. In 2015, Khorov *et al.* [13] and Park *et al.* [26] presented an updated overview of major PHY and MAC layer features of IEEE 802.11ah. Based on the results obtained in a few papers and numerous internal documents of the IEEE TGah, Khorov *et al.* [13] further provided an explanation on why they were included into the standard draft and what benefits they would bring. In 2016, Baños *et al.* [27] presented a thorough evaluation of the IEEE 802.11ah in comparison to the other IEEE 802.11 standards, and further conducted an analysis of the implementation and infrastructure costs of IEEE 802.11ah. In 2017, Meera *et al.* [28] summarized the standardization events of IEEE 802.11ah, and provided the current status of IEEE 802.11ah products in the IoT market. All these previous surveys were written between 2013 and 2017 and they focus mainly on the IEEE 802.11ah standard itself, among which only [13] published in 2015 mentioned a few early research works on RAW and fast association when comparing their performance with legacy IEEE 802.11 technologies. However, a lot of research has been done since 2015, aiming to optimize IEEE 802.11ah related features for various IoT scenarios. Moreover, the IEEE 802.11ah products have started to appear on the market since 2019. As such, this is a good time to have an up-to-date survey on this topic. Instead of focusing on the IEEE 802.11ah standard itself, this paper provides a comprehensive overview and analysis of existing research on IEEE 802.11ah from various aspects, aiming to help the readers to understand how to enhance the performance of IEEE 802.11ah for various IoT scenarios, and identify open research issues that remain to be addressed in the future.

1.3. Organization

The remainder of the article is organized as follows. Section 2 provides an brief description of the most prominent IEEE 802.11ah features, both on the PHY and MAC layer. A comprehensive overview and analysis of the existing research from different perspectives, including PHY and MAC layer, simulation tools and hardware, are presented from Section 3 to 9. In Section 10, the open issues and future research are discussed. Finally, conclusions are given in Section 11.

2. IEEE 802.11ah overview

Throughout this section we highlight the important features of IEEE 802.11ah, in both the PHY layer and MAC layer. For a more detailed overview of the standard, the readers can refer to existing literatures [12, 24, 25, 13, 26, 27, 28].

2.1. PHY

IEEE 802.11ah defines an Orthogonal Frequency Division Multiplexing (OFDM) PHY in the sub-1GHz bands, based on the 10 times down-clocked operation of IEEE 802.11ac's PHY. It supports 1, 2, 4, 8, 16 MHz channel bandwidths, with 1 and 2 MHz support being mandatory. Its use of sub-1GHz frequency bands (e.g., 863 - 868 MHz in Europe, 902 - 928 MHz in North-America and 755 - 787 MHz in China) and narrow bandwidth allows it to improve coverage range (up to 1 km) with considerably less power consumption than traditional Wi-Fi technologies, which use frequencies in the 2.4 and 5 GHz bands.

For different channel width, IEEE 802.11ah utilizes different sets of modulation and coding schemes (MCSs), Number of Spatial Streams (NSS) and duration of the Guard Interval (GI),

Table 2: IEEE 802.11ah MCSs for 1, 2, 4, 8 and 16 MHz, NSS=1, GI=8 μs.

MCS Index	Modulation	Coding rate	Data rate (Kbps)				
			1 MHz	2 MHz	4 MHz	8 MHz	16 MHz
0	BPSK	1/2	300	650	1350	2925	5850
1	QPSK	1/2	600	1300	2700	5850	11700
2	QPSK	3/4	900	1950	4050	8775	17550
3	16-QAM	1/2	1200	2600	5400	11700	23400
4	16-QAM	3/4	1800	3900	8100	17550	35100
5	64-QAM	2/3	2400	5200	10800	23400	46800
6	64-QAM	3/4	2700	5850	12150	26325	52650
7	64-QAM	5/6	3000	6500	13500	29250	58500
8	256-QAM	3/4	3600	7800	16200	35100	70200
9	256-QAM	5/6	4000	/	18000	39000	78000
10	BPSK	1/2 with 2x repetition	150	/	/	/	/

resulting in various data rates. The NSS ranges from 1 to 4 to support Multiple-Input and Multiple-Output (MIMO), and the GI can be 8 or 4 μs. Table 2 lists the supported data rates and their MCS when GI and NSS are 8 μs and 1 respectively for different channel widths. Moreover, the supported data rates are proportional to the value of NSS, and increase by around 11.1% with GI of 4 μs.

IEEE 802.11ah supports three different PLCP protocol data unit (PPDU) formats, i.e., $S1G\_1M$, $S1G\_SHORT$ and $S1G\_LONG$. $S1G\_1M$ is used for channel width 1 MHz. For the other channel widths, $S1G\_SHORT$ is for Single-User (SU) transmission, and $S1G\_LONG$ is for Multi-User (MU) and SU beamformed transmissions.

2.2. MAC layer

The MAC layer of IEEE 802.11ah consists of a variety novel features to improve high scalability and energy efficiency, as highlighted in Table 3.

Table 3: A brief description of new MAC features of IEEE 802.11ah.

MAC features	**Description**	**Objective**
Fast Authentication and Association	Mitigating collision during link set-up	Scalability
RAW	Mitigating collision during data exchange	Scalability
Group Sectorization	Mitigating collision during data exchange	Scalability
TIM Segmentation	Stations waking up less for receiving beacons	Energy efficiency
TWT	Station negotiating with AP about wake-up time	Energy efficiency
Hierarchical Organization	Efficient organization of Association IDs (AIDs)	Scalability
BSS Color	Mitigating interference among OBSSs	Scalability
Short MAC header	Using 2-byte address, and containing less subfields	Reducing overhead
Response Indication Deferral (RID)	Carrier sensing when Short MAC header are used	Carrier sensing
Relay	Two-hop link between a station and the AP	Range extension

2.2.1. Fast Authentication and Association

When a network is deployed or after a power outage, all stations start to set up the link as depicted in Figure 2. A station sends the AP an authentication request (i.e., *AuthReq*) and association request (i.e., *AssocReq*), which allows the AP to learn about the station's existence and capabilities. By sending back an authentication response (i.e., *AuthResp*) and association response (i.e., *AssocResp*) to the station, the AP informs the station of the network parameters and assigns it an identifier, referred to as an AID. During the link set-up stage, stations employ the DCF for channel access, which is sufficient to provide fast link set-up in traditional Wi-Fi networks, as the number of stations is usually small. However, the link set-up can take a long time when many stations try to associate at the same time, due to collisions of the authentication and association messages. Due to the large number of devices in IoT networks, this becomes an issue in IEEE 802.11ah. To address this problem, two effective fast authentication and association control mechanisms (i.e., centralized and distributed), are proposed for IEEE 802.11ah.

In Centralized Authentication Control (CAC), the AP dynamically changes the portion of stations that are allowed to send *AuthReq* messages. Specifically, the AP sets a threshold and broadcasts it to all stations by sending beacon frames. The beacon frame is a management frame and contains the information about the network, it is transmitted periodically by the AP to an-

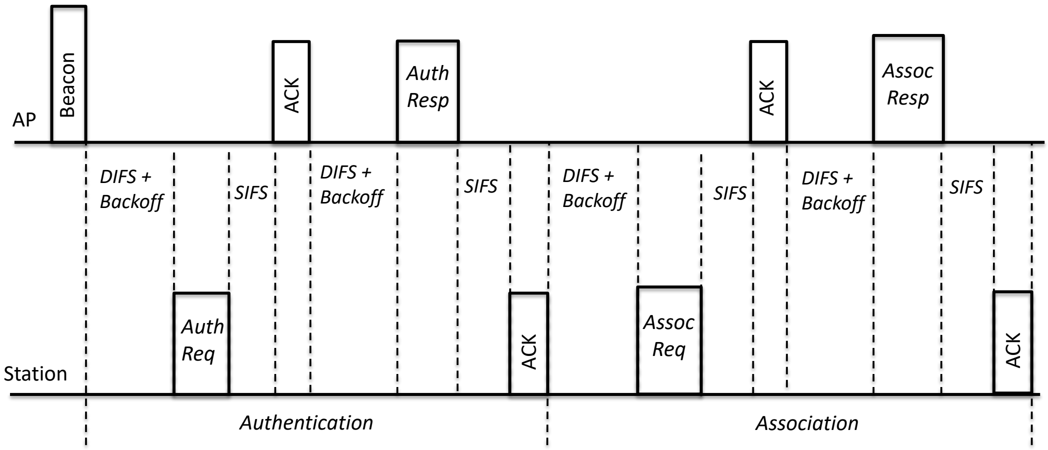


Figure 2: Illustration of IEEE 802.11ah link set-up process.

nounce the presence of a wireless network and to synchronize all the stations of the network. When a station is initialized, it generates a random value from the interval [0, 1022], and tries to send an *AuthReq* to the AP if the random value is smaller than the threshold obtained from the received beacon. Otherwise, it postpones authentication/association until the next beacon arrives. The threshold should be adjusted dynamically by the AP to limit the number of stations accessing the channel in one beacon interval, and make sure all stations can associate as fast as possible.

In Distributed Authentication Control (DAC), a beacon interval is divided into sub-intervals called Authentication Control Slots (ACSs). Stations randomly select a beacon interval and a ACS to send their *AuthReq*. If a station does not succeed to authenticate, it resends the *AuthReq* in the next m_{th} beacon interval and i_{th} ACS, the values of m and i are generated based on the truncated binary exponential backoff mechanism.

2.2.2. RAW

The station grouping mechanism, named RAW, is proposed to mitigate collisions and improve performance in dense IoT networks where a large number of stations are contending for channel access simultaneously. It is a combination of TDMA and CSMA/CA, which splits stations into groups and only allows stations assigned to a certain group to access the channel using DCF or EDCA at specific times. Figure 3 schematically depicts how RAW works. Specifically, the airtime is split into several intervals, some of which are assigned to RAW groups, while the others are considered as shared channel airtime and can be accessed by all stations. A beacon frame carries a

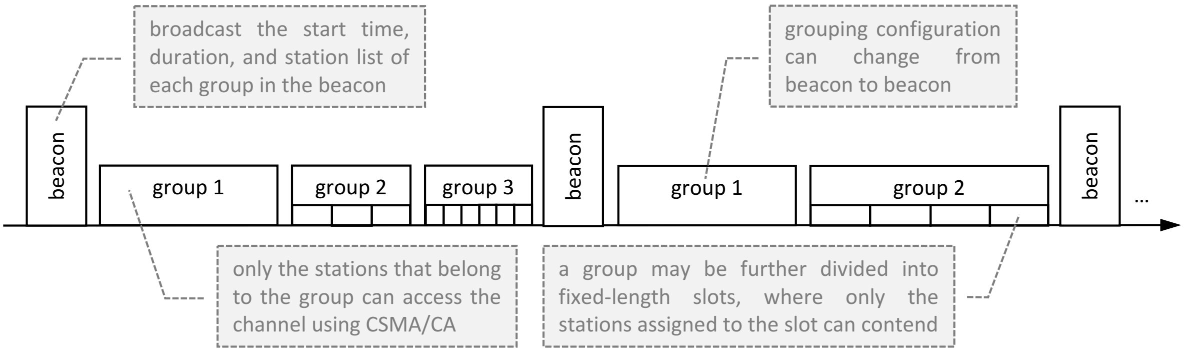

broadcast the start time, duration, and station list of each group in the beacon
grouping configuration can change from beacon to beacon
beacon
group 1
group 2
group 3
beacon
group 1
group 2
beacon
...
only the stations that belong to the group can access the channel using CSMA/CA
a group may be further divided into fixed-length slots, where only the stations assigned to the slot can contend

Figure 3: Schematic representation of the RAW mechanism.

RAW parameter set (RPS) information element that specifies the RAW related information, such as the stations belonging to the group, as well as the group start time. Stations belonging to a RAW group are required to have sequential AIDs, defined by start AID and end AID. Moreover, each RAW group consists of one or more slots, over which the stations assigned to the RAW group are evenly split (using round robin assignment). The RPS information element also contains the *number of slots, slot format* and *slot duration count* sub-fields, which jointly determine the RAW slot duration as follows:

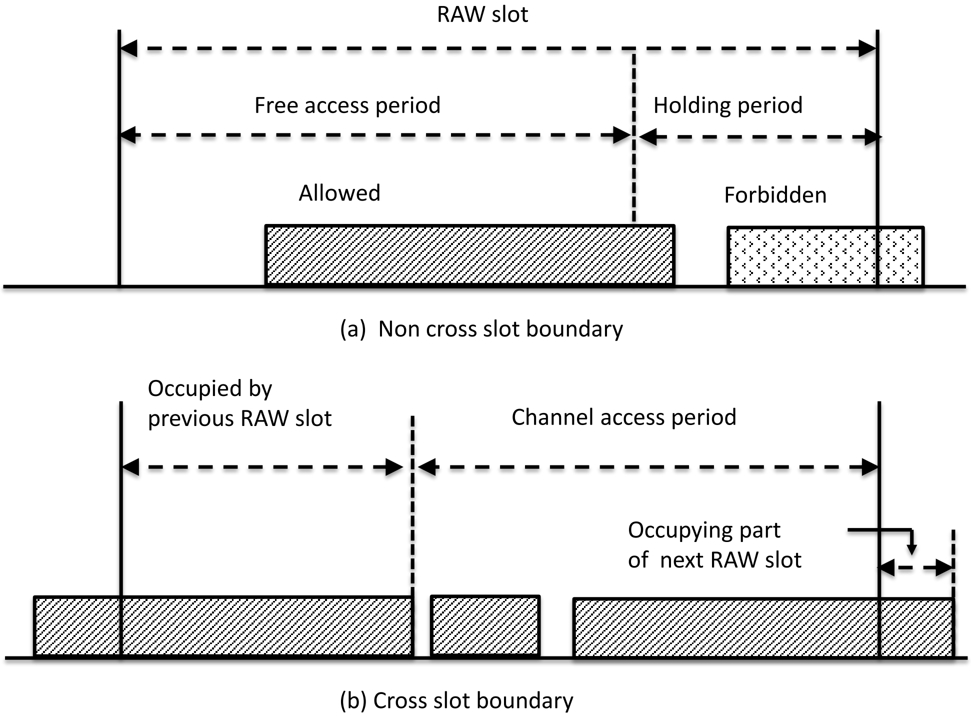
$$D = 500\ \mu s + C \times 120\ \mu s \tag{1}$$

where C represents *slot duration count* sub-field, which is either $y = 11$ or $y = 8$ bits long when the *slot format* sub-field is set to 1 or 0 respectively. The *number of slots* field is $14 - y$ bits long. When $y = 11$, each RAW consists of at most 8 slots and the maximum value of C is $2^{11} - 1 = 2047$, therefore the slot duration is up to 246.14 ms. If $y = 8$, each RAW consists of at most 64 slots and the maximum value of C is $2^8 - 1 = 255$, the slot duration is therefore limited to 31.1 ms.

Stations are mapped to slots as follows:

$$i_{slot} = (x + N_{offset}) \quad mod \quad N_{RAW} \tag{2}$$

where i_{slot} is the index of the RAW slot to which the station is mapped. N_{RAW} is the number of slots in one RAW. N_{offset} is the offset value in the mapping function to improve fairness and equals the two least significant octets of the Frame Check Sequence (FCS) field of the beacon frame, and x is determined as follows. If the RAW is restricted to stations with AID bits in the TIM element set to 1, x is the position index of the station among others. Otherwise, x is the AID of station. A detailed description of TIM element can be found in Section 2.2.4.



(a) Non cross slot boundary

(b) Cross slot boundary

Figure 4: An example of the non cross slot boundary and cross slot boundary features of RAW mechanism in IEEE 802.11ah [29].

The RPS also contains the *cross slot boundary* (CSB) sub-field. As Figure 4 depicts, stations are allowed to continue their ongoing transmissions even after the end of the current RAW slot when CSB is set to true. Otherwise, stations should not start a transmission if the remaining time in the current RAW slot is not enough to complete frame exchange. The remaining time, termed as “holding period”, should be at least equal to the Transmission Opportunity (TXOP) of the station.

Different from legacy IEEE 802.11 standards, each station uses two backoff states to manage transmissions inside and outside their assigned RAW slot respectively. The first backoff function state is used outside RAW slots, while the second is used inside. For the first backoff state, the station suspends its backoff timer at the start of each RAW, restores and resumes the backoff timer at the end of the RAW. For the second backoff state, stations start backoff with the initial backoff state inside their own RAW slot, and discard the backoff state at the end of the RAW slot. As shown in Figure 5, station 1 is inside the RAW group and assigned to slot 1, while station 2 is not included in this RAW group. Therefore, station 1 uses the first backoff state outside its RAW slot

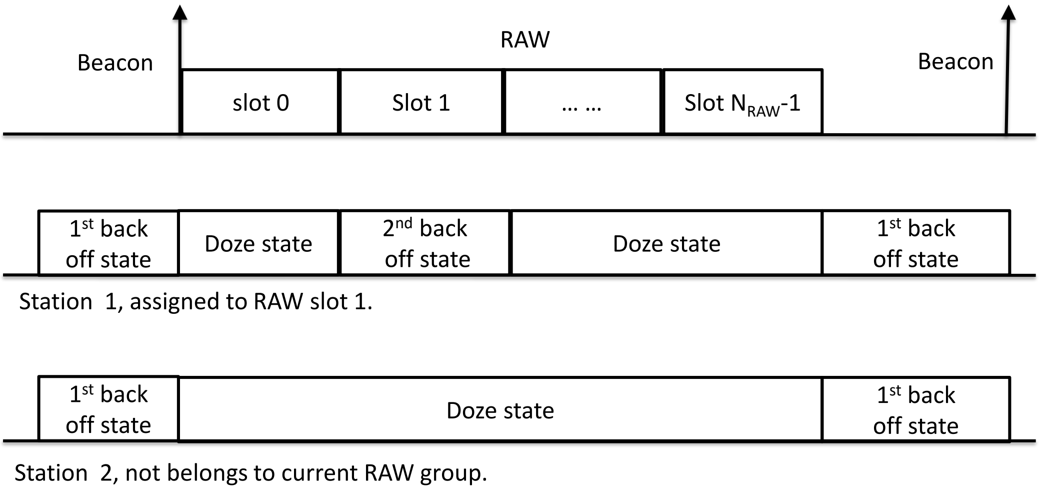


Figure 5: Illustration of the novel dual backoff procedure of IEEE 802.11ah

period and the second backoff state inside its RAW slot, while station 2 only uses the first backoff state outside the RAW group period and goes into a doze state inside the RAW group period.

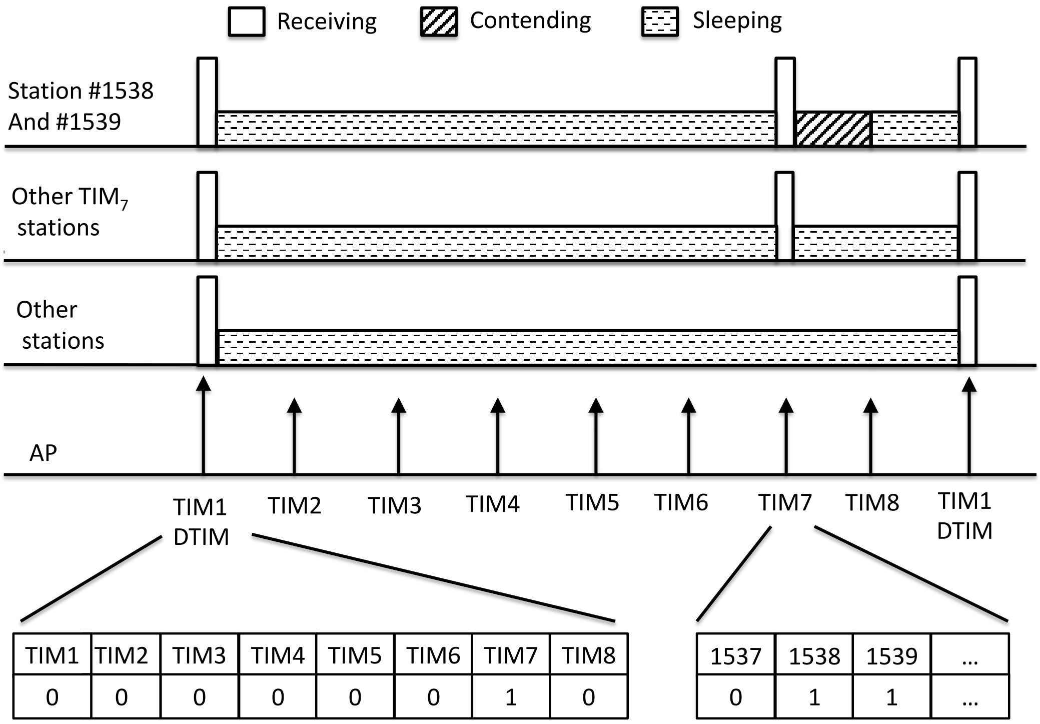
2.2.3. Group sectorization

Group sectorization is a combination of space- and time-division multiplexing. It divides the coverage area of a Basic Service Set (BSS) into sectors (i.e., geographical areas), each containing a subset of stations, aiming to mitigate hidden node problem, contention or interference. The sectorization is achieved by the AP transmitting or receiving through a set of antenna beams to cover different sectors of the BSS. Besides, the AP may alternate the sectorized beacons and the omnidirectional beacons, and all stations in the BSS can transmit regardless of their geographical locations during the omni beacon interval.

Group sectorization can be considered as a simplified version of RAW, as stations are grouped only based on location. The difference is that it allows more than one sectors to be active at the same time, and is only suitable for APs and stations with directional antennas.

2.2.4. TIM segmentation

For stations in Power Save (PS) mode, a TIM element is included in each beacon frame, named TIM beacon, to indicate a set of stations for which the AP has buffered packets. If no buffered packets are destined for a station, it returns to the doze state. Otherwise, it sends a PS-Poll frame to retrieve the buffered packets. However, for stations that have little downlink traffic from the



TIM1	TIM2	TIM3	TIM4	TIM5	TIM6	TIM7	TIM8
0	0	0	0	0	0	1	0

1537	1538	1539	…
0	1	1	…

Figure 6: Example of the TIM segmentation mechanism [25].

AP, receiving every beacon frame is not energy efficient and becomes the bottleneck of the whole power management framework.

To address this issue, an advanced power saving mechanism is introduced, called TIM segmentation, which splits the TIM information into N segments (i.e., TIM groups), and the information of each TIM group is carried by its corresponding TIM beacon. Delivery Traffic Indication Map (DTIM) beacons are for TIM group-level signaling, and TIM beacons are for station-level signaling. All stations wake up periodically to receive the DTIM beacon and check whether the AP has pending data for their own TIM group. If so, stations wake up again to listen to their corresponding TIM beacon, otherwise resume sleeping until the next DTIM announcement. As shown in Figure 6, the DTIM beacon shows that the AP only has pending data for TIM group 7. Therefore, stations of TIM group 7 wake up later to listen to the corresponding TIM beacon, and other stations resume sleeping until the next DTIM announcement. Moreover, when the beacon for TIM group 7 is received, as it indicates that the AP has pending data for station 1538 and 1539, other stations of TIM group 7 resume sleeping while these two stations contend for channel access in order to retrieve the data from the AP.

2.2.5. TWT

For stations transmitting data sporadically, power consumption can be further reduced by TWT. In TWT, stations can negotiate with the AP a series of time instances, called TWT Service Period (SP), about when they should wake up to exchange frames. Therefore they are not required to wake up even for receiving beacons and can stay in a power-saving state for very long periods of time. Either the AP or a station starts TWT negotiation. The AP or TWT station can end the TWT by transmitting a tear-down frame.

The main TWT parameters are *target wake time, minimum wake duration, wake interval, flow type*. *Target wake time* indicates when the first TWT interval begins, *minimum wake duration* is the minimum value of TWT SP, *TWT wake interval* equals to the average time between successive TWT SPs, and *flow type* indicates whether a trigger packet should be sent before transmitting data packets during SP.

2.2.6. Hierarchical Organization

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

To support large scale networks, the maximal AID value is increased to 8191 in IEEE 802.11ah. To simplify operations with such a huge number of associated stations, the hierarchical organization mechanism is proposed to organizes stations by 13-bit AIDs according to a four-level structure, including 2-bit pages, 5-bit blocks, 3-bit subblocks and 3-bit stations. Stations are divided into N_p pages of N_b blocks each, each block contains 8 subblocks of 8 stations each. These values of N_p and N_b are variable and can be configured by network operators. An example of AID hierarchical configuration is depicted in Figure 7. Grouping stations with similar characteristics using the four-level structure reduces overhead when referring to stations.

2.2.7. BSS color

Dense deployment of IEEE 802.11 networks can lead to Overlapping Basic Service Sets (OBSSs), resulting in interference among stations from different BSSs and degraded network performance. To solve the OBSS problem, a novel feature named BSS Color is introduced into IEEE 802.11ah.

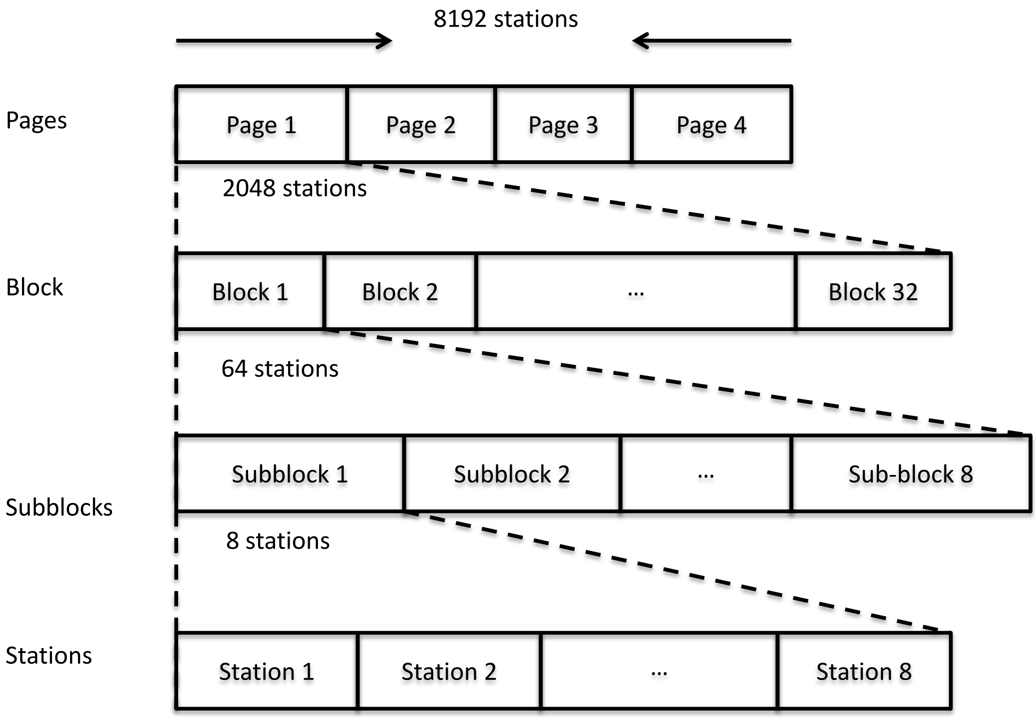


Figure 7: An example of IEEE 802.11ah AID hierarchical configuration.

In BSS Color, each BSS is assigned to a unique color, and such information is encoded in the PHY header of each packet. During packet reception, if a station detects the packet has a different BSS color from its own, it terminates the ongoing packet reception process to reduce power consumption and interference.

2.2.8. Short MAC header

In legacy IEEE 802.11 networks, the MAC frame header contains at most four 6-byte MAC addresses, leading to a total header length of 40 bytes. Thus, for a 100-byte payload, the MAC header overhead is 40%. For smaller payload, the overhead is even higher. To reduce the overhead, IEEE 802.11ah defines a new backward incompatible format of shortened headers for data, management and control frames, with a length of from 10 to 24 bytes, depending on the context. In the short MAC frame headers, the Duration/ID field, Quality of Service (QoS) and High Throughput (HT) fields are excluded, and the 6-bytes address field is replaced by a 2-bytes Short IDentifier (SID) field. Both legacy and short MAC frame headers are supported by IEEE 802.11ah.

2.2.9. Response Indication Deferral

As the short MAC header contains no Duration/ID field, which is required by Net Allocation Vector (NAV) for virtual carrier sensing, a novel channel access mechanism called Response Indication Deferral (RID) is introduced in IEEE 802.11ah. In the PHY header, there is a 2-bits *response indication* field that defines four types of responses, i.e., the ways of calculating the value of the RID timer. Right after the reception of the PHY header of a frame, the station sets the RID timer based on the value of the *response indication* field and starts counting down until the values of the RID timer comes down to 0, indicating the channel becomes idle.

2.2.10. Relay

To support IoT scenarios with large coverage, IEEE 802.11ah extends the transmission range between an AP, referred to as the root AP , and stations with a relay. A relay logically consists of a relay AP and a relay station. The relay AP is associated to stations, and the relay station is associated to a root AP. For downlink transmission (i.e. from the root AP to a station), the packets are transmitted by the root AP to the relay station, the relay station forwards the packets to the relay AP , which then transmits the packets to the station, and vice versa for uplink transmission. To simplify the forwarding mechanism, the relay is limited to a two-hop link between a station and the root AP .

3. Current Research on PHY

The IEEE TGah has proposed IEEE 802.11ah propagation loss models for outdoor and indoor environments [30, 31], based on the 3rd Generation Partnership Project (3GPP) spatial channel model and IEEE Task Group n (TGn) MIMO channel models, respectively. Using the propagation loss models, the transmission range, throughput, bit error rate (BER), etc. of IEEE 802.11ah have been studied in [32, 33, 34]. Hazmi et al. [32] studied the link budget, data rate versus transmission range, showing that transmission range of 1 km with data rate 150 kbps can be achieved. They also proposed packet size design method in different channel scenarios when fast fading is mainly characterizing the system environment. Li *et al.* [33] presented a comparison between IEEE 802.11g and IEEE 802.11ah in indoor environment, demonstrating IEEE 802.11ah has larger coverage, consumes much less power and slightly lower latency than IEEE 802.11g. Moreover, Khan *et al.* [34] conducted an in-depth performance analysis of BER and throughput

Table 4: Existing research on IEEE 802.11ah PHY layer.

Reference	Scenarios	Description
[30, 31]	indoor and outdoor	Proposing standard propagation loss models for IEEE 802.11ah.
[32]	indoor and outdoor	Studying the data rate, coverage using the standard mode.
[33]	indoor	Studying the coverage, latency and power using the standard mode.
[34]	outdoor	Studying the BER and throughput using the standard mode.
[35]	UAV	Incorporating the MultiCode MultiCarrier CDMA into the PHY layer.
[36]	urban outdoor	Adjusting the propagation loss model based on empirical models.
[37]	suburban outdoor	Adjusting the the propagation loss model based on measurement.
[38]	indoor, urban outdoor, suburban outdoor	Validating the propagation loss model based on measurement.

for various MCSs, showing higher MCS provide higher throughput but poor BER performance. Recently, Khan *et al.* [35] further incorporated the MultiCode MultiCarrier Code Division Multiple Access (CDMA) into the PHY layer of IEEE 802.11ah, in order to meet the differential requirements of range and throughput for Unmanned Aerial Vehicle (UAV) communication.

Aust et al. [36] analyzed the IEEE 802.11ah propagation path loss model for urban areas and compared the initial path loss attenuation and slopes with empirical path loss models, namely the Lee model and the Hata model. As such, they proposed to adjust the the IEEE 802.11ah model with the results obtained from their study. Moreover Bellekens *et al.* [37] proposed a more realistic propagation loss model by evaluating several path loss models of IEEE 802.11ah in real scenarios based on a large scale sub-urban measurement campaign, and further re-evaluated the throughput and BER with the new model. Recently, Koninck *et al.* [38] conducted a measurement campaign on a heterogeneous set of smart city-relevant deployment environments (i.e.,urban, suburban and indoor), and argued that current propagation models are highly accurate for IEEE 802.11ah.

In summary, as shown in Table 4, the above research studied the achievable transmission range, throughput and BER of IEEE 802.11ah in different environments (i.e., propagation loss models, UAV communication) and for different MCS, and further updated the propagation loss models. The results demonstrate that IEEE 802.11ah is capable of providing a reliable communication link for various IoT scenarios.

Table 5: Existing research on fast authentication and association.

Type	Reference	Description
CAC	[39]	Adjusting the association threshold based on the transmission queue.
	[40]	Constant step for threshold incremental/decremental.
	[41, 42, 43]	Adaptive step for threshold incremental/decremental.
	[44]	Retransmission based on retry counts and adaptive steps based on network size.
	[43]	Slotted-CSMA/CA for *AuthReq*, contention-free TDMA slot for subsequent process.
	[45]	Postpones sending *AuthResp*, and contention free for *AssocReq* transmission.
	[46]	Mathematical model for determining best group size.
DAC	[47]	Mathematical model for determining the number of ACSs.
	[42]	Performance evaluation with various parameters settings.

4. Current Research on Fast Authentication and Association

Several studies have been conducted to reduce the link set-up time in large scale networks, as listed in Table 5, with most of them focus on CAC and a few pay attention to DAC.

4.1. CAC

The high efficiency of CAC requires selecting the appropriate authentication threshold. However, the standard does not specify an authentication threshold management algorithm. Wang *et al.* [39] came up with the idea of adjusting the threshold based on the transmission queue size of the AP. The reason behind this idea is straightforward. When a large number of stations transmit an *AuthReq* to the AP, it cannot gain enough channel airtime to successfully transmit an *AuthResp* back to these stations. Therefore, its transmission queue keeps increasing. In contrast, when less stations attempt to send an *AuthReq*, the AP gains enough channel airtime to successfully transmit the piggybacked *AuthResp*. The IEEE 802.11ah implementation in the ns-3 network simulator provided an initial and naive implementation of this idea [40]. It increases the threshold by 50 when the transmission queues has less than 10 packets, otherwise decreasing the threshold by 50. Even using such a simple approach, the results already showed a significantly decreased link set-up time, especially for a large number of stations.

Several more advanced algorithms have been proposed based on the above idea [41, 42, 43]. Bankov *et al.* [41] proposed the Up and Down algorithms to adaptively select a threshold according to the transmission queue size of the AP. Both the Up and Down algorithms work in three modes: waiting, studying and working. In the Up algorithm, the AP initially starts in the waiting mode, maintaining the maximum threshold. When *AuthResp* packets appear in the queue, the AP sets the threshold to 1 and switches to the studying mode. In the studying mode, after each beacon interval, the AP increases the threshold value by Δ, and doubles Δ each beacon interval until the queue becomes nonempty. In this case, the AP halves Δ and switches to the working mode. In the working mode, the AP increases Δ by one until *AuthResp* appears in the queue again, and increases the threshold value by Δ if the queue is empty. Finally, when the threshold reaches its maximal value, the AP switches back to the waiting mode. The Down algorithm has the same waiting and working modes, but the studying mode is arranged differently. Instead of increasing the threshold value by Δ, it halves the threshold value when the queue is nonempty. Both of them outperform the ones with fixed increment values, and the Up algorithm is slightly less efficient than Down, but consumes channel resources in a less aggressive way. Moreover, two enhanced versions are proposed in [42, 43]. Bankov *et al.* [42] further improved the Up and Down algorithms by adjusting the threshold based on both the history of the threshold and Δ value, making the algorithm more robust to the varying network conditions. In more recent work [43], the AP increases the threshold and Δ based on both the queue size and the number of successful *AuthReq/AssocReq* handshakes in the previous beacon interval. Recently, Yin *et al.* [44] proposed a new association mechanism named FASUS to improve the association performance. In FASUS, the association request/response is retransmitted based on retry counts instead of timers to avoid unnecessary retransmission, and the steps used for adjusting the threshold is dynamically changed by speculating the number of stations in the network.

Instead of adjusting the authentication threshold as specified by the standard, alternative approaches for CAC have been proposed as well [43, 45, 46]. Shahi *et al.* [43] proposed a hybrid slotted-CSMA/CA–TDMA (HSCT) MAC protocol. In HSCT, contention-based slotted-CSMA/CA allows devices to send an *AuthReq* via randomly selected backoff slots, whereas contention-free TDMA permits those devices to send/receive the subsequent *AssocReq/AssocResp* via an individually allocated TDMA slot. Bankov *et al.* [45] proposed a virtual carrier sense approach to provide contention-free access. The main idea is, after receiving the *AuthReq*, the AP sends an ACK but postpones sending the *AuthResp* at least until the next beacon, and the AP also sets its duration field to forbid all other stations from transmitting frames before the intended station starts the *AssocReq* transmission. Sthapit *et al.* [46] built a mathematical model for the authentication/association process, showing that there exists a best group size that results in minimal association time. However, the assumption of constant successful transmission probability and the AP knowing the number of stations is not realistic for the link set-up process.

4.2. DAC

Bankov *et al.* also [47] described a simple mathematical model for DAC to determine the number of ACSs to minimize the link set-up time, given the beacon interval and number of stations. However, the model assumes contention-free access inside each ACS, which simplifies calculations but not realistic.

Besides investigating CAC in [42], Bankov *et al.* also conducted extensive simulations on DAC and showed that there is not a set of parameters that can minimize the link set-up time for all possible numbers of stations. In some scenarios, the DAC is essentially insensitive to some of its parameters. Moreover, the results showed that CAC outperformed DAC in general. However, such an advantage of CAC comes at the cost of complexity and the need for the AP to constantly track the link set-up process.

5. Current Research on RAW

As the IEEE 802.11ah standard does not specify how to configure the RAW grouping parameters, user-defined optimal RAW configurations are required in order to obtain high performance in terms of throughput, latency or energy consumption for the given network conditions.To provide an optimal solution for RAW configurations, three approaches are usually involved, including parameter evaluation, modeling and optimization. During evaluation, the impact of the RAW related parameters and network conditions on performance is analysed qualitatively, which is considered as the foundation for the latter approaches. Subsequently, a RAW performance model is usually built to represent relations between the output performance and input parameters in a quantitative way. Finally, an optimization algorithm usually utilizes a RAW performance model to determine the optimal RAW configuration for the given network conditions, based on the pursued performance metrics. In the remainder of this section, details of related research on parameter evaluation, modeling and optimization are presented, respectively.

5.1. RAW performance evaluation

RAW performance is evaluated in [48, 49, 50]. Zhao *et al.* [48] evaluated RAW in terms of energy efficiency, showing that increasing the number of RAW groups significantly improves energy efficiency for sensor stations. Tian *et al.* [49] evaluated the influence of the number of stations, traffic load and traffic distribution on the optimal values of number of RAW groups and their duration, proving that with appropriate grouping, the RAW mechanism substantially improves throughput, latency and energy efficiency. Furthermore, the results suggest that the optimal grouping strategy depends on many parameters, and intelligent RAW group adaptation is necessary to maximize performance under dynamic conditions. Qutab *et al.* [50] analyzed the performance of the RAW mechanism in the non-cross slot boundary case under various possible holding schemes, which define how the station should count its backoff within the holding period.

5.2. RAW performance modeling

As DCF and EDCA are employed inside RAW, the RAW models are mainly developed based on their backoff process, by taking into account the characteristics of RAW, including the reset of the backoff function state at the beginning of the RAW slots (referred to as backoff reset), the channel handover among RAW slots (referred to as handover) and backlogged packets due to the intermittent channel access of RAW slots (referred to as backlogged packets). The existing RAW models consider either saturated state or unsaturated state. If each station always has pending packets to transmit, then the network is in saturated state, otherwise unsaturated state. In the remainder of this subsection, details of related research are presented.

5.2.1. Saturated state

For leagcy IEEE 802.11, without considering the details of the stochastic backoff process, a mean value analysis-based modeling approach was adopted by [51, 52], evaluating the average value of network variables, such as transmission probability, collision probability and packet service time. Based on the mean value analysis approach, Zheng *et al.* [53, 29] proposed an analytical model to track the throughput under saturated traffic for both cross and non-cross slot boundary, taking RAW slot handover into account. The results show that the RAW slot handover can cause the throughput to fluctuate, and such impact is more prominent in the non-cross slot boundary case than the cross slot boundary case. Based on the Markov chain approach, Raeesi *et al.* [54] provided an analytical model of throughput and energy efficiency for cross slot boundary, which was later extended to support multi-AP scenarios in [55].

Due to the reset of the backoff function at the beginning of the RAW slot, the channel contention and collision probability change with time. However, the above models all consider the steady state of the network, i.e., the contention success probability does not change over time. By taking into account the backoff reset feature of RAW, a mathematical model for saturated state was developed by Khoro *et al.* [56] based on Bianchi model, which is a discrete-time Markov chain model for the throughput under saturated state by considering the details of the stochastic backoff process [57]. The model estimates throughput and energy consumption of RAW with cross slot boundary, studying how channel contention changes over time and how the stations from one RAW slot affect the performance of the next RAW slot. The results show that, under the same RAW configuration, cross slot boundary obtains higher throughout but less energy efficiency than non-cross slot boundary. However, comparing the power consumption of two RAW configurations with which maximal throughput is obtained for cross and non-cross slot boundary respectively, the one for cross slot boundary consumes less power.

5.2.2. Unsaturated state

For IoT scenarios, network with the unsaturated traffic is more common in reality, as IoT devices usually have few data to send. The existing research has considered different traffic patterns for unsaturated state, such as periodic traffic where each station sends one packet per fixed interval, or packet arrivals following a Bernoulli or Poisson distribution.

Some works [58, 59] assumed each station sends one packet per RAW slot interval. Khorov *et al.* [58] presented a model to calculate the successful packet transmission probability for a given RAW group duration for non-cross slot boundary. Santi *et al.* [59] extended this model to calculate the time occupied by different states (i.e., receive, transmit, idle, collision, sleep) for a given RAW group duration, which were subsequently used to calculate energy consumption. The results show that more RAW slots achieve better energy efficiency at the cost of increasing the latency. Both models take into account the backoff reset feature of RAW, which results in channel contention varying over the time.

Chang *et al.* [60] took a step further, supporting more diverse traffic demands by allowing stations to have different packet transmission intervals. They used the results of two extreme cases (i.e., saturated traffic and one packet sent per RAW interval) to extrapolate a regression-based analytical model that can accurately predict the successful transmission probability of diverse traffic loads. However, the model considers the network state is steady.

Instead of assuming ideal channel that does not have communication errors and all stations have the same characteristics (i.e., homogeneous stations), Tian *et al.* [61, 62] applied surrogate modelling to RAW in order to support more realistic scenarios. A surrogate model [63] is an efficient mathematical representation of a black box system. It is based on supervised learning (e.g., Kriging or neural networks), and is especially suitable for tasks with a large input space, as an accurate model can be trained with relatively few adaptively sampled data points. By feeding realistic simulation results into the surrogate modelling toolbox, a surrogate model does not suffer from the same restrictive assumptions as existing analytical models. Homogeneous stations are supported by the model for throughput and energy consumption in [61]. Moreover, a throughput model for heterogeneous stations in terms of MCS and packet size was proposed in [62], by using average transmission time that is jointly determined by MCS and packet size as an input parameter of the surrogate model, and packet receiving rate (i.e., number of packets received per second) as the output parameter which can be accordingly converted to throughput with packet size.

For unsaturated traffic patterns that follow a Bernoulli arrival distribution, Ometov *et al.* [64] developed a RAW model for cross slot boundary using a Markov chain. Moreover, assuming packet arrivals follow a Poisson process and non-ideal channel conditions which takes into account communication errors, Ali *et al.* [65] proposed a throughput model based on Markov chain and M/G/1 queuing model. The results reveal that, with high packet arrival rate, the backoff time of stations increase significantly and the network performance becomes unstable. Furthermore, Ali *et al.* [66, 67] evaluated performance of RAW with EDCA on differentiated QoS. They presented a Markov chain and M/G/1 queuing model to evaluate the performance of RAW for non-cross slot boundary. The analysis evaluates the feasibility of the coexistence of priority and non-priority traffic in IoT devices without degrading network performance, revealing that RAW can support QoS traffic at low traffic load condition. Other than [58, 59, 60], works in [64, 65, 66, 67] take into account the backlogged packets due to the intermittent channel access of RAW groups. However, they assume steady state inside a RAW slot.

Table 6: Existing research on RAW modeling

Reference	Traffic	Objective	RAW characteristics			Network heterogeneity			Non-ideal channel
			backoff reset	handover	backlogged packets	transmission interval	packet sizes	MCSs	
[53, 29]	saturated	throughput		X	X				
[54, 55]	saturated	throughput, energy			X				
[56]	saturated	throughput, energy	X	X	X				
[58]	periodic	successful trans. probability	X						
[59]	periodic	energy	X						
[60]	periodic	successful trans. probability				X			
[61]	periodic	throughput, energy	X	X	X				X
[62]	periodic	packet receiving rate	X	X	X		X	X	X
[64]	bernoulli arrivals	throughput			X				
[65]	poisson arrivals	throughput			X				X
[66, 67]	poisson arrivals	QoS			X				X

5.2.3. Conclusion

In Table 6, we list the existing RAW models, and categorize them based on various aspects, including the traffic type, objective, considered RAW characteristics (including backoff reset, handover and backlogged packets), network heterogeneity in terms of transmission interval, packet size and MCSs, and the channel conditions. The X mark indicates that the responding feature is supported by the model.

Based on the above analysis, we derive the following conclusions on RAW modeling. First, since it is trained with realistic simulation results of RAW based on supervised learning approaches, the surrogate model, compared to analytic models, can more accurately represent the RAW behaviour and support more complex network scenarios. While only the analytic model presented in [60] supports heterogeneous traffic, allowing stations to have different packet transmission intervals. Second, as backoff reset, handover and backlogged packets are the unique characteristics that makes RAW different from DCF and EDCA, the analytic models presented in [53, 29] and [56] can more precisely represent RAW behaviour. Third, RAW performance modeling with QoS has not received much attention, as [66, 67] are the only ones that address this issue so far.

5.3. RAW performance optimization

RAW performance optimization determines the number of RAW groups, the duration of each group, and how to divide stations among them. To provide readers with a clear view on existing RAW optimization algorithms, we categorize them into several types based on the direct objectives of the algorithms, including *1)* energy efficiency, *2)* throughput, *3)* latency, *4)* collisions and successful transmission probability, *5)* fairness, *6)* QoS and *7)* hidden nodes. It is worth noting that it does not necessarily mean an algorithm can only optimize the performance of a single objective, as these objectives are not necessarily contradictory or even related in certain scenarios. For instance, an algorithm aiming for high energy efficiency may also achieve low latency or high throughput, and such performance often results from low collisions probability, or high success transmissions probability.

5.3.1. Energy efficiency

Wang *et al.* [68] assumed one station sends a packet per RAW group interval and formulated energy efficiency as a function of the number of devices and number of RAW slots using probability theory. By applying a Hill Climbing approach, they found an optimal set of number of devices and number of RAW slots to maximize energy efficiency. Wang *et al.* [69] further presented a retransmission scheme that utilizes the next empty slot to retransmit packets lost due to collisions, and reformulated the energy efficiency function by applying probability theory and a Markov Chain. Moreover, a fast algorithm for the retransmission scheme was proposed to maximize energy efficiency using a Gradient Descent approach. Both the above algorithms allow a station to randomly choose a RAW slot to contend for the channel, which is not in accordance with the RAW specification.

Kai *et al.* [70] designed a traffic distribution based grouping scheme to balance the energy efficiency of different groups in large scale networks, where stations have heterogeneous traffic demand. By adopting the Markov chain model, they formulated the energy efficiency optimization as a max-min problem. A heuristic traffic-sensor mapping algorithm (HTMA) was subsequently presented to properly assign stations to groups in order to make the traffic demands of each group appropriate, under a given number of groups and group duration.

Beltramelli *et al.* [71] proposed a hybrid contention-reservation mechanism with two distinct phases. In the contention phase, each station send a trigger frame to the AP, indicating whether it has pending packets for uplink traffic. In the data transmission phase, the AP assigns a RAW slot to each of the stations that has pending packets to send, leading to contention-free transmission.

5.3.2. Throughput

Nawaz *et al.* [72] presented a method in which a RAW group is divided into two sub-groups and the duration of RAW slots in each sub-group is chosen according to the number of stations in the RAW slots. The idea of choosing a duration based on the number of stations improves throughput when stations have the same traffic load. However, unevenly allocating duration among RAW slots in a single RAW group contradicts the IEEE 802.11ah RAW specification.

Considering stations in the network have heterogeneous packet transmission intervals, Chang *et al.* [73] proposed an algorithm to balance the traffic load among groups to improve channel utilization (i.e., the ratio of channel time used for data transmission to the total channel time). They first conducted some motivating simulations to examine the effect of heterogeneous traffic demands on performance. Subsequently, they formulated the problem of distributing the traffic load into groups as an integer programming model, and proposed a greedy algorithm to properly allocate stations into RAW groups, under a given RAW group number and beacon interval. To make the algorithm more effective, they reformulated the load balancing problem with a regression-based analytical RAW model of successful transmission probability [60], which was extrapolated using the results of two extreme cases (i.e., saturated traffic and one packet sent per RAW interval).

Considering heterogeneous packet transmission intervals and such intervals may slowly change over time, Tian *et al.* [74] proposed the Traffic-Aware RAW Optimization Algorithm (TAROA) to adapt the RAW parameters in real time based on the current traffic conditions. Following the additive-increase multiplicative-decrease principle, TAROA introduces a traffic estimation method to predict the packet transmission interval of each station only using packet transmission information obtained by the AP during the past beacon intervals. TAROA further derives the optimal number of stations of a RAW group by using the simulation results under saturated state as an alternative to the RAW model. Based on the derived optimal number and estimated traffic, a heuristic algorithm is proposed to assign stations to groups in order to maximize the throughput. Tian *et al.* [75] proposed a more accurate traffic estimation method by exploiting the "More Data" header field and cross slot boundary feature, and integrated it into an enhanced version of TAROA, referred to as Enhanced Traffic-Aware RAW Optimization Algorithm (E-TAROA). In addition, Ahmed *et al.* [76] proposed a method in which the AP predicts the traffic transmission interval by dividing RAW into contention and reservation phases, and schedules the transmission of subsequent frames before their arrivals. The three algorithms support homogeneous stations only, i.e., all stations use the same MCS and packet size.

Tian *et al.* [61, 77] further proposed a Model-Based RAW Optimization Algorithm (MoROA) with the trained surrogate RAW model, which has a better estimation on the actual performance of a specific RAW configuration, to determine the optimal RAW configuration in real time through multi-objective optimization using the interior-point method. Its objective weight allows to attain either a throughput increase, fairness improvement, energy saving, or a weighted solution in between. MoROA supports heterogeneous networks in terms of MCS and packet size, by introducing multiple RAW groups and assigning all homogeneous stations into a single RAW group. TAROA, the algorithm presented in [76] and MoROA are the only RAW related algorithms so far that support traffic estimation and dynamic traffic.

5.3.3. Latency

Khorov *et al.* [78] studied the usage of RAW in a scenario of emergency alerts. In such a scenario, multiple sensors are entrusted to react to the same emergency event, and it is enough to receive an alert message from any of these sensors. They first presented an easy-to-calculate mathematical model of alert delivery, which was adopted from the model of [58]. In order to make the model feasible to calculate with the limited computational resources of an AP, they assumed that stations do not try to retransmit. Such a simplification is based on the observation that, with very high probability, the successful alert delivery happens on the first transmission attempt of some emergency sensor. Subsequently, they used the model to dynamically reconfigure RAW parameters, i.e., number of RAW slots and RAW group duration, to minimize consumed channel timeshare while providing satisfactory reliability and delivery delay for an alert message.

In order to provide reliable packet delivery with a constrained deadline, reservation-based channel access is adopted by Madueno *et al.* [79]. They proposed an adaptive access mechanism supporting traffic patterns including periodic, on-demand (i.e., poisson arrival), and alarm reporting that corresponds to traffic generated by an event in which all affected devices are activated almost simultaneously. The proposed method is based on a periodically reoccurring pool of time slots, whose size is proactively determined based on the reporting activity. They split the reservation phase into two parts, i.e., the preallocated and the common pool. The preallocated pool consists of a fixed number of reservation slots, with each dedicated to a group of stations. The size of the common pool changes dynamically based on the number of collisions observed in the preallocated pool in order to identify traffic patterns and active stations, which will be assigned to contention-free RAW slots in data transmission phase. As such, it is able to provide efficient and reliable packet delivery with different traffic patterns within constrained deadlines. Furthermore, it provides a rationale for modeling the inter-arrival time in alarm events by using the Beta distribution.

Similar to [79], Charania *et al.* [80] proposed a delay and energy aware RAW formation (DEARF) scheme, where Delay Sensitive Machine type Devices (DSMDs) coexist with other non-Delay Sensitive Machine type Devices (non-DSMDs). DEARF utilized four successive RAWs to provide contention-free data transmission for DSMDs and contention-based data transmission for non-DSMDs. First, the Contention Indication (CI) RAW is used to indicate to the AP that DSMDs have data to send. Second, the Delay Information Indication (DII) RAW contains only contention free slots, allowing DSMDs to send the AP a small control packet carrying the information of packet delay requirements and time of arrival. Third, the DSMDs Resource Allocation (DRA) RAW assigns contention free slots to these DSMDs, allowing them to transmit data frames. Finally, the Non-DSMDs Resource Allocation (NRA) RAW are used by non-DSMDs contending for the channel to transmit data frame. As such, the DEARF scheme is able to improve reliability for DSMDs and energy efficiency for both DSMDs and non-DSMDs.

5.3.4. Collisions or successful transmission probability

Several station grouping algorithms for mitigating the collision probability have been proposed in [81, 82, 83, 84], and an algorithm aiming to maximize the successful transmissions probability was proposed in [85].

Ogawa *et al.* [81] allowed a station to randomly select its AIFS value from a given range, then allocated stations into groups based on their AIFS values. Huang *et al.* [82] proposed the Registration-based Collision Avoidance (RCA) mechanism. In RCA, a station first generates a backoff value, then attaches it to the *AssocReq* frame and sends to the AP. Based on the recorded backoff values of all stations, the AP schedules the data transmission of the stations to avoid collisions and reduce the time wastage during the backoff countdown process. Similarly, Nabuuma *et al.* [83, 84] proposed to allow stations to set their backoff counters using the position of their AIDs in the group, and developed an analytical model to determine the upper bound of network throughput.

These solutions require modification on the DCF and EDCA mechanism inside RAW [81, 82, 83, 84]. It is assumed that the AP knows the AIFS value of stations in [81] , which is not the case in reality. Moreover, stations access the channel in a deterministic manner instead of a random way in [82, 83, 84], such approaches only work when traffic is known in advance, and bring about unfairness issues.

Park *et al.* [85] proposed an algorithm to estimate the number of devices based on the observed number of successful transmissions using the maximum likelihood estimation method, and further determined the number of RAW slots for a fixed number of devices and RAW group duration to maximize the successful transmissions probability. However, the algorithm is developed under the same assumption as [68, 69], i.e., a station randomly chooses a RAW slot to contend for the channel, which contradicts the IEEE 802.11ah RAW specification.

5.3.5. Fairness

Several algorithms have been proposed to improve the fairness of throughput among the competing stations and aggregate network throughput based on different network characteristics, including data rate [86, 87], traffic patterns [88], and channel coefficients that provide a frequency-time description of the channel [89].

When stations are grouped without considering their physical data rate, for the same packet length, a lower data rate station occupies the channel for a longer time as compared to a higher data rate station. Therefore, the throughput of higher data rate stations are down-equalized to that of lower data rate stations, and the aggregate network throughput is degraded. To resolve this problem, Sangeetha *et al.* [86] presented analytical models for saturated state under data rate based grouping, and further designed an algorithm to group stations based on their data rate with the proposed model, in order to improve fairness and aggregate network throughput. Similarly, Mahesh *et al.* [87] presented an analytical model for saturated state when stations have different data rates, and group stations with the same data rate.

Considering a network where stations have different traffic patterns, Lakshmi *et al.* [88] first divided stations into different groups, ensuring the transmission intervals and payload sizes of all stations in each group are the same. Based on the weight (i.e., the aggregate transmission time requirement) of each group, they formulated fair grouping in IEEE 802.11ah networks as an optimization problem, and developed a heuristic method to solve it in real-time. Moreover, to further ensure fair channel utilization by the nodes in each group, they proposed a weight-based contention window selection method to dynamically adjusts the contention windows of each node. However, it requires modifications to the backoff process.

Considering the heterogeneity of channel coefficients, Jahromi *et al.* [89] applied the Max-Min fairness criterion to the per-station throughput to increase the overall network performance with better fairness. They formulated the fairness issue as a non-convex integer programming problem, and applied the Ant Colony Optimization method to find the solution.

5.3.6. QoS

Initial works on QoS using RAW are presented in [90, 91], they simply assigned appropriate channel time to groups based on their priorities. Ahmed *et al.* [90] proposed a QoS-aware priority grouping to reduce collisions and ensure required bandwidth for rare but critical event-driven stations. It identifies stations into periodic and non-periodic (critical event-driven) types, and divides them into different groups according to their priority. If any overlap occurs between periodic stations and critical stations, the algorithm always ensures transmission of critical stations by freezing the periodic stations. However, there is a lack of details on the freezing mechanism. Mahesh *et al.* [91] divided the devices into several groups based on their transmission requirements and assigns each group a priority. As such, the group of devices with higher priority is allowed to access the channel for more time than the lower priority devices.

5.3.7. Hidden nodes

By allocating hidden nodes into orthogonal RAW groups, the simultaneous transmissions of hidden nodes can be eliminated and thus hidden node collisions can be avoided.

Park *et al.* [92] conducted several simulations on random station grouping, demonstrating that it is a simple but very effective way to mitigate the hidden node problem in a large outdoor network using RAW. Dong *et al.* [93] simply divided the coverage area into several segments and assigned each segment a RAW slot. Stations are allocated into the corresponding RAW slot based on their location. These two algorithms assume the hidden nodes information or stations' location is already known by the AP.

Using the timing of arriving packets, Damayanti *et al.* [94] proposed a collision mitigation scheme. First, it detects the collision chain, and lets the AP broadcast a collision chain indication

(CCI) to only allow the devices that have transmitted a frame before (but failed due to collision) to keep contending for the channel. The devices contending after CCI reception piggyback the transmission time of the previous transmission attempt on the next transmission frame, so that the AP can construct a table of carrier-sensitivity among devices using the timing of arriving packets. Subsequently, based on the constructed carrier-sensitivity table, they proposed a grouping algorithm to perform both initial grouping and regrouping. Similarly, Yoon *et al.* [95] proposed to add a subfield in the PS-poll frame to record transmission time, which allows stations to detect hidden nodes using the timing of arriving packets as well. Based on this detection scheme, a hidden node matrix is created that is subsequently used by a heuristic algorithm to minimize the probability of hidden nodes pairs sharing the same RAW slot.

Zhu *et al.* [96] utilized the ACK frames to detect hidden nodes. Specifically, for a downlink transmissions from the AP to station A, if station B cannot hear the ACK from station A to the AP, then station B considers station A as its hidden node and informs the AP. As such, the AP is able to create a table of the potential hidden nodes in the network. Subsequently, the AP regroups the stations into different contention groups according to either a centralized Viterbi-like algorithm or a decentralized iterative updating manner, reducing hidden nodes pairs to a predefined threshold. Similarly, Wang *et al.* [97] utilized the *AssocResp* frame to detect hidden nodes and generate a hidden relationship matrix during association. They further proposed a greedy algorithm that always assigns a node to a group with the least hidden node pairs. However, this distributed way of grouping stations is not in accordance with the RAW specification.

Ghasemiahmadi *et al.* [98] proposed a Received Signal Strength (RSS) based grouping strategy to solve the hidden node problem. In this scheme, the AP randomly chooses the group heads that transmit pilots at fixed intervals. A node measure the sensed power of these pilots and choose to join the group whose pilot has the highest RSS. As such, nodes in the same group can be close enough that the probability of having a hidden node is very low.

Instead of only minimizing the hidden node pairs sharing the same transmission slot, [99] presents the only algorithm so far that takes the traffic of hidden nodes into account. Assuming the hidden node pairs and traffic are known, they formulated an NP-hard 0/1 integer linear programming, and proposed an approximation algorithm to find the solution in a fast way.

Table 7: Existing research on RAW optimization algorithms.

Objective	Reference	Additional evaluated metrics	Method	Traffic	Network heterogeneity	Comments
Energy	[68]		probability theory, hill climbing.	periodic		In [68, 69], stations randomly choose a RAW slot, contradicting RAW specification.
	[69]	delivery ratio	markov chain, gradient descent.	periodic		
	[70]		markov chain, max-min.	periodic	transmission interval	
	[71]	latency	contention reservation	poisson arrival		
Throughput	[72]		set partitioning	saturated state		[72] splits RAW slot unevenly, contradicting RAW specification. [74, 75, 77, 76] supports traffic estimation, and dynamic traffic.
	[73]		greedy algorithm	periodic	transmission interval	
	[60]	fairness	regress model, greedy algorithm.	periodic	transmission interval	
	[74, 75]	latency, energy.	multiplicative decrease.	periodic	transmission interval	
	[76]	energy, latency	contention, reservation	periodic, saturated state.	transmission interval	
	[77]	energy	surrogate model, interior-point.	periodic	transmission interval, packet sizes, MCSs.	
Latency	[78]	delivery ratio	markov chain	alarm traffic		[78] considers the first successful transmitted packet.
	[79]	false alarm ratio	probability theory, channel reservation.	periodic, poisson arrival, alarm.	traffic pattern	
	[80]	energy, deadline miss ratio.	probability theory, channel reservation.	poisson arrival		
Collisions probability	[81]	throughput, energy, latency.	AIFS value based			Use modified backoff process to mitigate collisions inside RAW.
	[82]	throughput, delivery ratio.	registered backoff value based			
	[83, 84]	throughput, latency.	deterministic backoff value based			
Successful transmission probability	[85]	throughput, energy, latency.	maximum likelihood			Same assumption as [68, 69]
Fairness	[86, 87]	throughput	markov chain, heuristic method.	saturated state	MCSs	Fairness of throughput among individual stations.
	[88]	throughput, energy, latency.	heuristic method	periodic	transmission interval, packet sizes.	
	[89]	throughput	max-min		channel coefficients	
QoS	[90]	throughput	set partitioning	periodic, event-driven	traffic pattern	Simply assign group duration based on priorities. [90] lacks of details.
	[91]	throughput	set partitioning	periodic	transmission interval, MCSs.	
Hidden nodes	[92]	energy, latency, delivery ratio.	random grouping			Splitting stations among groups under fixed group number. Group duration is not taken into account. [98] contradicts RAW specification; [92, 93, 99] assumes hidden nodes pairs or stations' location are known by the AP.
	[93]	throughput	location based			
	[94, 95]	throughput, energy, latency.	timing of arriving based			
	[96]	throughput, energy, latency.	ACK based			
	[97]	throughput, energy, latency.	*AssocResp* based			
	[98]	throughput	RSS based			
Hidden traffic	[99]	delivery ratio	linear programming			

5.3.8. Conclusion

In Table 7, we highlight the existing RAW algorithms from various aspects, including objective, additional evaluated metrics, method, traffic type, network heterogeneity (i.e., stations have different transmission intervals,traffic patterns, packet sizes, MCSs, and channel coefficients), etc. As for the traffic type, the event-driven traffic usually follows a certain pattern (e.g., poisson arrival), while the alarm traffic refers to the traffic generated by an emergency event and all affected devices are activated almost simultaneously.

Based on the above description and analysis, we derive the following conclusions on RAW optimization algorithms. First, as IEEE 802.11ah is designed for IoT scenarios, most of the algorithms consider machine-type traffic, i.e., periodic, event-driven (e.g, possion arrival) and alarm traffic. For periodic traffic, some works [74, 75, 77] support the scenarios where the transmission interval slowly changes over time. Second, homogeneous networks, as well as heterogeneous networks in terms of transmission interval have been widely investigated. A few algorithms support diverse MCSs and packet sizes, and channel coefficient is considered in [89]. Third, utilizing RAW to provide differentiated QoS for different stations and applications is at a very early stage, as the current QoS related algorithms simply assign longer duration to groups of higher priority. Fourth, existing collision probability related algorithms merely utilize the backoff counter or AIFSN values to mitigate collisions inside RAW, which are either unrealistic or require modification to the mechanism. Fifth, existing hidden nodes related algorithms focus on reducing the number of hidden nodes with a fixed number of RAW groups. Only [99] takes traffic load into account. Sixth, current algorithms mainly focus on single AP network scenarios, which have laid a solid foundation for future studies on multi-AP network scenarios and range extension using relays.

6. Current Research on TIM Segmentation

Several studies have investigated the performance of TIM segmentation from various aspects. As highlighted in Table 8, some of them focus on utilizing TIM segmentation to reduce the energy consumption for downlink traffic [100, 101, 102, 103], while others are interested in the joint usage of TIM segmentation and RAW for supporting both uplink an downlink traffic [104, 105, 106, 107], aiming to provide differentiated network services.

Ji *et al.* [100] presented a three-level hierarchical TIM compression coding structure to decrease

Table 8: Existing research on TIM Segmentation.

Traffic	Reference	Objective	Description
Downlink	[100]	energy, throughput	TIM coding to decrease the TIM bitmap size.
	[101]	energy, latency	Performance analysis through experiments.
	[102, 103]	energy, latency	Dynamically changes the membership of nodes.
Downlink, uplink	[104]	energy	Building an analytical model of RAW and TIM.
	[105]	energy, throughput	Using RAW to set up a protected interval for TIM stations.
	[106]	energy, throughput, latency	Performance analysis of RAW and TIM through experiments.
	[107]	energy, throughput, latency, reliability	Performance analysis of RAW and TIM through experiments.

the TIM bitmap size, reducing the TIM beacon overhead in terms of energy consumption and throughput.

Badihi *et al.* [101] analyzed the performance of the TIM segmentation mechanism in an actuation use case for connected lighting from the perspective of latency and power consumption in the downlink direction, under various network configurations. The results show a tradeoff exists between the latency and power consumption, lower latency can be achieved using shorter DTIM intervals at the cost of higher power consumption. Moreover, it reveals that the power consumption of stations with very low downlink traffic frequency is dominated by beacon frame receptions, which is a major issue for TIM segmentation. To address the this issue, Kim *et al.* [102, 103] proposed a method that dynamically changes the membership of nodes. They assigned a primary and a secondary AID to a station. As such the station belongs to two different TIM groups, allowing it to switch between the groups and rearrange its traffic to maximize overall sleeping time without causing delay to data delivery.

Considering a RAW group consisting of one downlink TIM segment and one uplink segment, Bel *et al.* [104] presented an analytical model for the energy consumption. The model is able to provide an estimation of the average energy consumed by a station and predict its battery lifetime, based on a set of closed-form equations. In addition, this model can be used as a tool to understand the effects of the RAW and TIM segmentation parameters on energy consumption, and to find a suitable network configuration for a given application.

For a heterogeneous network consisting of a high number of low-power stations with sporadic traffic and several powered stations with saturated traffic, Kureev *et al.* [105] proposed using RAW to set up a protected interval during which only a subset of low-power stations transmit their PS-Polls to retrieve downlink packets indicated by TIM elements. While the rest of beacon interval can be used for uplink transmission. A simple and accurate mathematical method was further developed to set up the parameters in order to reduce power consumption for low-power stations, and increase throughput for the other stations.

Considering co-existing high-throughput video streaming traffic and large-scale reliable sensing traffic, Seferagic *et al.* [106] investigated how RAW and TIM segmentation influence scalability, throughput, latency and energy efficiency in the presence of bidirectional TCP/IP traffic. The experimental results enable the fine tuning of RAW and TIM segmentation parameters for throughput-demanding reliable applications (i.e., video streaming, firmware updates) on one hand, and very dense low-throughput reliable networks with bidirectional traffic on the other hand.

Seferagic *et al.* [107] further explored the scalability of IEEE 802.11ah networks hosting both control loops and monitoring sensors. They extended the work of [101] by considering (i) various delay requirements, both shorter and longer, in control loops that include both sensing and actuation, (ii) jitter in control loops and (iii) scalability of monitoring stations (uplink only) operating alongside low-latency time-critical control loops (both uplink and downlink). The experiments reveal that, assigning the control loop end-nodes to dedicated RAW time slots result in over 99.99% successful deliveries, and adjusting the TIM beacon interval can ensures latency requirements of control loop at the cost of reduced throughput and energy efficiency. This demonstrates that IEEE 802.11ah can meet reliability and low-latency demands up to a certain extent.

7. Current Research on Network Security

Several studies have investigated the network security issues of IEEE 802.11ah from various aspects. As highlighted in Table 9, [108, 109] utilize phase encryption to enhance the security of the PHY layer, [110, 111, 112] improve the security at the link setup stage, while [113] focuses on medium access and presents a performance model under selfish attacks.

The phase encryption is a type of encryption at the PHY layer, in which the modulated symbol data is adjusted by changing phases and amplitudes in the transmitter, while the phase decryption is the reverse process in the receiver. To enhance the security of IEEE 802.11ah at the PHY layer, by applying Coordinate Rotation Digital Computer algorithm to calculate the amplitude, phase, sine, and cosine, Hoang *et al.* [108, 109] developed a low complexity hardware circuit for phase encryption and decryption for a variety of high complex modulation types (i.e., from 16 to 256 QAM) of the IEEE 802.11ah physical transceiver.

By integrating the Fast Initial Link Setup (FILS) scheme specified in the IEEE 802.11ai standard into IEEE 802.11ah networks, Zhang *et al.* [110, 111] proposed the Fast Key Re-authentication (FKR) scheme, in order to simplify the process of the authentication and key generation while keeping the same security level of the FILS. FKR accelerates the re-authentication process by employing a single station's nonce for the introduction of the randomness to the system. The AP's nonce can be calculated with the station's nonce for the hash function to be used in the next authentication round. Due to the single nonce introduced in every round of authentication, the protocol is able to shorten the authentication process to only two messages. Based on the IEEE 802.11 key management with the IEEE 802.1X authentication mechanism, Kim *et al.* [112] proposed a new Authentication and Key Management (AKM) mechanism for IEEE 802.11ah networks, in order to establish a security association between a resource-constrained IoT station and an AP. A station-side authentication server (SAS) is introduced to allow stations to delegate most of the burden of authentication and key derivation to it. As such, stations only need to verify mutual authenticity with the AP by using basic encryption and decryption functions. Moreover, the security algorithms used for deriving the session key are independent of the IoT stations and thus can be replaced with other algorithms without affecting the IoT stations.

For IEEE 802.11ah networks that are under selfish attack, in which selfish nodes gain advantage on channel access by using a backoff configuration (e.g. smaller contention window) that is not compliant with the standard, Liew *et al.* [113] proposed an evolutionary game model for channel access where the throughput is modelled as the player payoff. The model is able to predict the performance with a given number of selfish players and their backoff configuration, and shows that the increase of selfish nodes poses a severe concern for resource availability of the honest nodes.

8. Miscellaneousness

8.1. TWT

Some early works have been published on TWT [114, 59, 115, 116]. As RAW can be used for protecting TWT stations from collisions with other stations during the TWT SP, Zhang [114]

Table 9: Existing research on network security.

Reference	Target	Description
[108, 109]	PHY layer	Developing a hardware circuit of phase encryption and decryption.
[110, 111]	link setup	Introducing single station's nonce in every round of authentication.
[112]	link setup	Introduced an authentication server for authentication and key derivation.
[113]	medium access	Developing an evolutionary game model for networks under selfish attack.

proposed to interleave TWT stations. As such, their TWT SP can be covered by a single RAW, reducing the RAW indication overhead while minimizing the transmission latency. Santi *et al.* [59] implemented the TWT feature in the IEEE 802.11ah ns-3 simulator [40] and evaluated its performance, showing that the sleeping time dominates the battery life when having longer transmission intervals and the beacon reception affects the energy consumption significantly. Santi *et al.* [115] further studied the energy consumption of the co-existence of RAW and TWT stations. The results showed that the presence of RAW stations can have a negative effect on the energy efficiency of TWT stations, and a proper channel access scheduling can mitigate this negative effect without degrading throughput performance of RAW stations. One of the problems of TWT is the clock drift, as it results in devices ceasing to strictly comply with the schedule, therefore missing the scheduled transmission time, which increases active time and thus power consumption. To solve this problem, Bankov *et al.* [116] studied the packet delivery ratio, energy consumption and latency of TWT uplink data transmissions in the presence of the clock drift for two TWT flow types. In the first flow type, a sensor transmits a packet to the AP after waking up. In the second flow type, a station transmits a packet only after receiving a trigger frame from the AP. The results show that the second flow type is more energy efficient, while the first flow type has better performance in terms of packet delivery ratio and latency.

8.2. Sectorized grouping

A few works have focused on sectorized grouping [117, 118, 119]. Bhandari *et al.* [117] proposed a method in which the AP first broadcasts beacons to different geographical locations by utilizing simple sectorized beams. Subsequently, the stations of each sector are further divided into different RAW groups uniformly within the sectors. While Ngo *et al.* [118] suggested the AP works in directional mode and beamforms in the direction of 2 sectors, therefore stations of different sectors can access the channel at the same time without causing collisions. Ngo *et al.* [119] further proposed a four-way handshake to avoid hidden nodes inside the sectors, and a three-way handshake to prevent the stations from polling the AP at the same time.

8.3. New channel contention approaches

Several new channel contention mechanisms have been proposed to mitigate channel collisions in IEEE 802.11ah networks [120, 121, 122]. Cheng *et al.* [120] proposed a channel-aware contention window adaption (CA-CWA) algorithm. Using the maximum likelihood estimation method, CA-CWA first estimates the current network congestion level represented by channel busyness ratio (the percentage of time that a station senses the channel is busy during a certain time interval). Subsequently, it dynamically adapts the contention window based on the network congestion level, to support applications with strict deadline constraints in IEEE 802.11ah. To support unpredictable and time-critical alarm events (e.g., fire alarm), Zhang *et al.* [121] proposed a standard-compliant timer mechanism called Limited Local Extension (LLE). In LLE, when a sensor with a pending alarm-report detects an alarm-report sent by another sensor, it extends its own backoff timer by a random duration to avoid collision. Different from the existing BEB, Gopinath *et al.* [122] proposed a backoff algorithm with appropriate integer sequences to resolve channel contention. With m backoff stages in total, a station resets its CW to the initial CW value when a successful transmission occurs before the middle backoff stages $i = (m/2 - 1)$, otherwise it resets its CW with the CW value of the previous backoff stage.

8.4. Mobility management

Research presented in [123] analysed the influence of Random Walk, Gauss-Markov, and Random Waypoint mobility models on IEEE 802.11ah with different traffic pattern schemes. The results suggest that the overall performance of the network is decreasing along with the increasing number of RAW slots, and RAW slot duration.

For a multi-Radio Access Technology (RAT) device that implements both IEEE 802.11ah and a LPWAN technology (e.g., NB-IoT or LoRa), an vertical handover between these two wireless technologies is required in order to benefit from larger coverage of LPWAN and higher throughput of IEEE 802.11ah. Instead of performing vertical handover based on periodic listening for beacons, Santi *et al.* [124] proposed an approach to allow the RAT device, which moves away from or toward an area covered by an IEEE 802.11ah AP, to decide whether or not to wake up for listening for beacons based on its location. The results show that, the proposed location-based approach improves energy consumption of the RAT device by 100 times, and remains similar link set-up time.

8.5. Relaying

Studies on extending the transmission range using relays are presented in [125, 126]. Kocan *et al.* [125] provided a comprehensive analysis of IEEE 802.11ah on the level of achievable range extension through the implementation of half-duplex decode and forward (DF) relay stations (RS) in communication between an AP and an end-stations (ST). Assuming a Rician fading channel between AP and ST, and a Rayleigh fading channel on the RS – ST link, it analytically derives results on achievable ranges for the most robust MCSs, both for downlink and uplink transmission. Ali *et al.* [126] proposed to extend the operating range of a UAV communication network using IEEE 802.11ah. It considers a UAV network with a Ground Control Substation (GCS) and two tiers of UAV nodes. The nodes in the first and second tier work as relay nodes and non-relay nodes, respectively. GCS allocates RAW slots to relay nodes, and relay nodes further allocates RAW slots to non-relay nodes, in order to reduce the contention among nodes and keep them in doze mode as much as possible. Ahmed *et al.* [127] proposed to dynamically allocate non-interfering channels and MCSs to stations, and designed a hybrid channel access mechanism with a combination of contention and reservation, in order to improve the throughput and latency for multi-hop scenarios.

8.6. Network slicing

Network Slicing in Radio Access Technologies (RATs) is a novel approach to dividing the wireless network into isolated logical slices which are defined following their requirements and features in a service-driven way. Libório *et al.* [128] applied the network slicing concept to IEEE 802.11ah networks. A Virtual Network Slicing Broker (VNSB) is proposed, which is a Virtual Network Function (VNF) instantiated inside a Software Defined Network (SDN) controller. The VNSB communicates with an IEEE 802.11ah network AP via a southbound Application Program Interface (API). It first obtains the slicing templates which describes the services features and respective QoS restrictions, based on information from the northbound API. Subsequently, the VNSB uses the data flow reported by the AP to compute network performance per slice and therefore recompute the RAW parameters over time, in order to reallocate available resources between slices, improving network capacity and maintaining the network QoS performance.

8.7. Dynamic frequency allocation

Pandya *et al.* [129] presented an interference aware dynamic frequency allocation scheme for OBSS to improve channel utilization. The main idea is to allow each AP to employ multiple frequency sub-bands and associate nodes to these sub-bands dynamically. Specifically, it first quantifies the active interference from other nodes, with respect to the load presented by these nodes. If an intra- or inter-BSS node actively generates high interference, the node is allocated to a frequency sub-band where interference caused by it is less significant.

8.8. Coexistence in sub-1GHz bands

Liu *et al.* [130] presented coexistence techniques that can achieve fair spectrum sharing between IEEE 802.11ah and IEEE 802.15.4g networks. An energy detection clear channel assessment method was proposed to enable IEEE 802.11ah devices to detect ongoing IEEE 802.15.4g packet transmissions. Moreover, they introduced a backoff mechanism for IEEE 802.11ah devices to avoid interfering with the IEEE 802.15.4g packet transmission process.

The IEEE 802.11ah technology operates at the sub-1GHz bands that are subject to various coexistence regulations set by the authorities. In Europe, devices in the sub-1GHz bands must comply with the maximum duty cycle limit of 2.8%, provided that they support Listen Before Talk (LBT) [131]. The duty cycle is defined as the percentage of the maximum transmitter “on” time on one carrier frequency, measured over a one hour period. Hazmi *et al.* [132] investigated the challenges of such duty cycle limitations and its effect on the IEEE 802.11ah network performance from the uplink transmission perspective. The obtained results show that, in the presence of the tight coexistence requirements at the sub-1GHz bands, IEEE 802.11ah can provide efficient support for the most important use cases, such as home/building automation and healthcare, where the traffic of an individual station or node is strongly unsaturated.

Shafiq *et al.* [133] considered a Cognitive Radio (CR) scenario where a secondary network co-located with a primary network, using the IEEE 802.11ah and IEEE 802.11af protocol respectively. The secondary users (SUs) exploit the licensed channels whenever the legitimate primary

Table 10: Related research on IEEE 802.11ah Hardware Prototypes.

Reference	Outcome	Description
[134, 135, 136]	prototype	Building a prototype using Software Defined Radio (SDR).
[137]	prototype	Building a prototype using Digital Signal Processor (DSP).
[138, 139]	chip	Developing the transmitter and receiver.
[140]	receiver structure	Proposing a receiver structure for high interference environments.

users (PUs) are inactive, and meanwhile, secondary users are obligated to immediately vacate the channel once PUs become active. To avoid collisions between SUs and PUs, especially hidden PUs, they introduced a carrier sense Restricted Access Collision and Interference Resolutions (RACIR) protocol for CR-based IEEE 802.11ah networks. RACIR first introduces a decentralized group split algorithm to distribute the participating stations into multiple groups based on a probabilistic estimation method to resolve collisions. Second, in order to avoid hidden PUs, both transmitter and receiver conduct carrier sensing. Once active PUs are detected, a transmitter or receiver broadcasts a jam signal to stop transmission and invoke a blocking state for a predefined time, in order to vacate the channel for PUs.

9. Prototypes, Products and Simulators

9.1. Hardware Prototypes

Several IEEE 802.11ah hardware prototypes for the PHY have been developed [134, 135, 137, 138, 139, 140, 136], as highlighted in Table 10. Aust *et al.* [134] built a real-time MIMO-OFDM testing platform for evaluating narrow-band sub-1GHz transmission characteristics. Aust *et al.* [135] further proposed a SDR platform for IEEE 802.11ah experimentation, operating at the 900 MHz band, and used it to perform an over-the-air protocol performance assessment. Moreover, Tschimben *et. al* [136] implemented a prototype based on two software defined radios (i.e., USRP X310s with UBX-40 daughterboards) and a GNU Radio model (i.e., gr-ieee802-11). Casas *et al.* [137] introduced an architecture for a programmable IEEE 802.11ah Wi-Fi modem based on Cadence-Tensilica DSP. Ba *et al.* [138] developed a fully digital polar IEEE 802.11ah transmitter. With a 1 voltage supply, it achieves more than 10 times power reduction compared to the state-of-the-art OFDM transceivers. Without any complicated PA pre-distortion techniques, it passes all the PHY requirements of the mandatory modes of IEEE 802.11ah with 4.4% EVM, while consuming 7.1mW with 0dBm output power. The second generation fully-digital polar transmitter (TX) was released, and a receiver was developed as well, by Ba *et al.* one year later [139]. The new transmitter improves the EVM to -31dB with 10 dB spectral mask margin while the receiver achieves 6 dB noise figure for the sub-1GHz bands from 755 MHz to 928 MHz. As the performance of receiver that uses Least Square (LS) channel estimator and Viterbi decoder degrades in high interference environment, Bishnu *et al.* [140] proposed a robust generic OFDM based receiver structure for high interference environments. The proposed receiver is based on non-parametric maximum likelihood channel estimation followed by a Viterbi decoder, whose branch metric is updated based on the distribution of residual errors.

9.2. Products

In industry, several companies, such as Methods2Business, Morse Micro and Newracom, are working on commercial IEEE 802.11ah chipsets. A few products have been brought into the market recently, such as NRC7292 (Newracom) [141], M2B7011/ M2B7211 (Methods2Business) [142], and more are expected to come in the near future. Based on the openly published data sheet [143], the NRC7292 operates at 750 - 950 MHz frequency band, with 1, 2, 4 MHz channel bandwidths being supported. It contains external RF front end module which can increase transmission power up to 23 dBm, supporting data rate from 15 Kbps to 15 Mbps. Moreover, the legacy low power mode and TWT are implemented.

9.3. Simulators development

A software simulator, which can accurately represent the behaviour of IEEE 802.11ah and support scalable, repeatable experiments in a resource efficient way, is essential to conduct accurate IEEE 802.11ah performance evaluation and validating the related algorithms. There are several simulators available for running experiments on IEEE 802.11ah, including Matlab, OMNeT++, and ns-3. Both OMNeT++ and ns-3 are open source, discrete-event network simulators for wired and wireless networks. On the one hand, OMNeT++ has extensive Graphical User Interface (GUI) support, and allows building network topologies graphically. Therefore, it provides easy definition of network simulation scenarios. In contrast, ns-3 uses command line interfaces for simulation which is less user friendly. However, ns-3 has finer simulation granularity than OMNeT++, leading to more accurate simulation results [144].

The IEEE 802.11ah module of Matlab focuses on PHY, supports IEEE 802.11ah waveform generation including modulation/demodulation, channel coding, signal transmission/reception, and channel modeling [145]. An early implementation of the IEEE 802.11ah RAW feature was done in the OMNeT++ simulator by Raeesi *et al.* [54]. However, the software was not made available as open source.

The IEEE 802.11ah module implemented in the ns-3 network simulator, supports a wide range of features in both PHY and MAC layers [40, 146]. As ns-3 is designed in a modular way and already supports several IEEE 802.11 technologies [147], the IEEE 802.11ah module is implemented by modifying several components. At PHY, the corresponding components (i.e., InterferenceHelper, ErrorRateModel, WifiPhy, YansWifiPhy and Propagation LossModel) are revised to support MCS 0 to 9 at all supported bandwidths from 1 to 16 MHz, three types of PPDU formats, and a variety of sub-1GHz propagation loss models. At the MAC layer, the corresponding components (i.e., MacHigh, DcaTxop, EdcaTxopN, DcfManager and WifiRemoteStationManager) are modified and two new componments (i.e., S1gFrame Header and RAWConfiguration) are created, in order to support the AID hierarchical organization, fast association, RAW, TIM segmentation and adaptive MCS. The implementation is modular, allowing it to be easily extended with additional IEEE 802.11ah-specific features, and has been made available as open source [148]. Moreover, a user-friendly interactive visualization and post-processing tool was developed for IEEE 802.11ah, called ahVisualizer [149], enabling much faster and easier data analysis and monitoring of ns-3 simulations.

10. Open issues and future research directions

A lot of research has been done in the past years on various aspects of IEEE 802.11ah. The existing research has made great contributions towards a scalable low-power Wi-Fi solution for IoT applications. However, there are still some open research issues that can be addressed.

10.1. Heterogeneous networks

Current research mainly focuses on homogeneous networks (i.e., all the stations have the same parameters), or heterogeneous networks mainly in terms of transmission interval. Only a few works consider a single network with stations that have different MCSs [62, 77, 86, 91], packet sizes [62, 77, 88], or channel coefficients [89]. However, in reality, the heterogeneity of the network can be more complex. More research is needed in the scope of heterogeneous networks where not only transmission intervals, but also other parameters (e.g., MCS, bandwidth, transmission power, traffic patterns and rate control) vary from station to station. Moreover, future research needs to take into account the dynamics of the network, i.e., the parameters of stations change over time or stations join and leave the network dynamically.

The optimization of heterogeneous networks can be resolved in three steps, including parameter screening, modeling and grouping. For parameter screening, a combinatorial design method called locating array [150] can be applied to identify the sensitive parameters that have significant impact on performance, the insensitive parameters that have trivial impact, and the two-way interactions between parameters. Based on the screening results, by ignoring the insensitive parameters and taking the two-way interactions into account, performance models can be built using surrogate modeling with experimental or realistic simulation results of a set of training data points, and validated with experimental results of a set of test data points. Finally, based on the performance models and the dynamics of the network, an optimization problem can be formulated to derive an appropriate station grouping strategy, in order to satisfy the required performance metrics.

10.2. Quality of service

The current algorithms on utilizing RAW to provide QoS are in early stage, as they only built RAW models on EDCA or simply assign longer duration to groups of higher priority [66, 67, 90, 91]. In addition, a few research works consider the joint usage of RAW and TIM segmentation to provide two differentiated network services for certain scenarios, revealing there is a trade-off between different performance objectives [104, 105, 106, 107]. Therefore, it is still an open issue to leverage IEEE 802.11ah to support network scenarios where different types of stations and applications with varying QoS requirements co-exist, such as low latency for critical services, high energy efficiency for low-power IoT devices, and stable throughput for data streaming applications. Designing such an algorithm is challenging especially when the network resource is limited as the approaches for meeting each of the performance requirement may affect each other. For instance, deterministic latency could result in lower channel utilization and therefore lower throughput. Similarly, lower latency achieved by shorter beacon intervals could lead to higher power consumption.

A combination of RAW, TIM segmentation, TWT and other features might be a potential solution. Firstly, the appropriate features that can be utilized for each performance requirement should be determined. For example, RAW can be chosen for deterministic latency, stable throughput or traffic with different priorities, TIM segmentation or TWT can be selected for low-power IoT devices depending on the traffic (e.g., downlink or uplink, frequent or sporadic). Secondly, the airtime assigned to each feature can be derived by formulating an multi-objective optimization problem with certain constraints.

10.3. Multi-AP scenario

The existing research mainly focuses on a single AP network (i.e., BSS). However, multi-AP scenarios are quite common in reality, which should be considered in future work. Compared to a single BSS, dealing with the interference among the neighbouring BSSs is more challenging for both the link set-up and data exchange phases, as it does not only suffer from the hidden node problem but also the exposed node problem in which the transmissions are suppressed unnecessarily by sensing signals that are actually ignorable.

The inter-AP coordination or non-coordination can be applied to interference avoidance, as both of them have been successfully applied to legacy Wi-Fi networks [151, 152]. The coordination supports ease of management and often results in better performance, as the network is observed and managed by a central control unit. However, due to stringent beacon frame timing constraints, it may be only possible over larger time frames and not at the start of each beacon interval. On the other hand, the uncoordinated methods are more scalable and applicable, especially for dense uncoordinated small cell deployments, making it more attractive for IoT scenarios.

10.4. Coexistence in sub-1GHz bands

IEEE 802.11ah operates at sub-1GHz bands in 1, 2, 4, 8 and 16 MHz channel bandwidths. As such, it spans over larger frequency spectrum in comparison to other sub-1GHz technologies (e.g. LoRa, SigFoX, 802.15.4g), and they are likely to interfere with each other. Given their low power nature and wide area coverage, as well as different PHY and MAC characteristics (i.e., chirp spread spectrum, ultra-narrow band, OFDM, etc.), they may ~~impact each other~~experience mutual degradation in different ways. For example, in Europe, LoRa and 802.15.4g partly share the frequency spectrum with IEEE 802.11ah. A limited research on interference between 802.15.4g and IEEE 802.11ah has demonstrated that fair spectrum sharing between them can be achieved [130]. However, considering long transmission times of LoRa and the back-off mechanisms of

IEEE 802.11ah, coexistence issues are expected, but not explored yet. In addition, interferes that do not comply to EU duty cycle regulations (e.g. communication between a crane operator and the construction team on the ground) may highly congest the shared radio bands in that location. More research is needed in the context of sub-1GHz technology coexistence, including detection and identification of the interfering technologies in the shared spectrum, as well as the interference mitigation strategies in order to manage coexisting networks in the future when sub-1GHz bands become highly congested, much like 2.4GHz shared spectrum is at present.

To minimize the mutual degradation in the shared spectrum, it is vital to be able to identify the presence of interfering technologies, and to correctly classify them [153, 154], as well as to make use of appropriate mitigation strategy for the case in question. Innovation in interference mitigation strategies will likely focus on PHY/MAC reconfiguration mechanisms (such as automatic selection of robust coding schemes, increasing error-correction codes, etc.) designed for improving coexistence. Additionally, more scalable coexistence solution may include inter-technology negotiation, exchange and coordination of MAC schedules between the coexisting technologies, which would require innovative technology-agnostic signalling.

10.5. Time-Sensitive Networking

Some wireless technologies have been aiming to provide Time-Sensitive Networking (TSN)-compliant capabilities defined by the IEEE 802.1 TSN task group [155], such as 5G New Radio (NR) for factory automation [156, 157], w-SHARP [158] and Wireless High-Performance (WirelessHP) [159]. Although several studies demonstrated that they can achieve sub-millisecond or millisecond latency, these technologies are greatly limited in range (in the order of 10 m) and are only suitable for localized communication solutions such as a single robotic cell with a dedicated Programmable Logic Controller (PLC). However, in process automation, a plant typically has (as) few PLCs (as possible) regulating various processes, which can span over hundreds of meters or even kilometers. Wiring is thus very expensive and deployment can take months due to the large area. IEEE 802.11ah has the potential to be optimized for this domain [21]. Although it cannot guarantee as low latency as the aforementioned technologies, it could be applied to process automation with somewhat slower dynamics (e.g., recycling plants, oil refineries etc.).

Lack of determinism in legacy IEEE 802.11 technologies makes it challenging to comply with the time-critical requirements of industrial applications. However, study has shown that the delay and jitter of a Wi-Fi system can be improved [160]. IEEE 802.11ah introduces novelties on its MAC layer and combines legacy stochastic medium access with deterministic via RAW time-slotting, which opens additional possibilities for research and case-studies in this domain. Making use of RAW, TIM segmentation and dual back-off mechanisms could be instrumental in adapting IEEE 802.11ah to the TSN paradigm.

10.6. Real-life validation

Given the non-availability of certified hardware for research in the past years, the research on IEEE 802.11ah is based on IEEE 802.11ah PHY prototypes, mathematical models and simulation. The novel PHY and MAC mechanism of IEEE 802.11ah was mainly validated in lab environments so far. With IEEE 802.11ah products coming to the market recently [141, 142], validation of theoretical and simulation results in practical deployments would motivate a quicker adoption of this technology in real IoT deployments.

11. Conclusion

IEEE 802.11ah is considered as a promising next generation Wi-Fi technology for large-scale and low-power IoT applications. This article provides a comprehensive overview and analysis of the research trends in IEEE 802.11ah, consisting of three contributions. First, we presented a brief description of the IEEE 802.11ah standards, including both the PHY layer and MAC layer, especially highlighting the novel features of the standard. Second, the existing research is comprehensively reviewed and analyzed from various perspectives, such as the targeted features, research objective, applicable scenarios, strengths and shortcomings. The relevant hardware prototypes, products and simulators are introduced as well. Third, the remaining issues and future research directions have been discussed.

In summary, IEEE 802.11ah combines the advantages of Wi-Fi and low-power communication technologies, supports high data rate and is able to meet the demanding performance criteria of a variety of IoT applications with tailored approaches, such as large scale networks, low power and QoS. For example, for large-scale IoT networks dominated by uplink traffic, the RAW feature can be utilized to highly reduce collisions by tuning corresponding parameters (e.g., RAW group duration, RAW slot number, station number), thus leading to higher throughput, energy efficiency, or lower latency. For IoT networks with low-power stations and downlink traffic, TIM segmentation can be adopted to achieve low energy consumption. For networks with sporadical traffic, the power consumption can be further reduced by applying TWT to allow stations to wake up at the designated time. Moreover, for IoT networks with more complex traffic demand or QoS requirements, a combination of RAW, TIM segmentation, TWT and other features can be jointly applied. Moreover, IEEE 802.11ah supports IP connectivity, operates at worldwide license free bands and has simplified network infrastructure. Its shortcoming is the shorter transmission range compared to most of the LPWAN technologies, and incompatibility with legacy IEEE 802.11 technologies. We believe that with the advent of more available off-the-shelf products, IEEE 802.11ah networks will play an important role in IoT and be widely deployed in the future.

Acknowledgement

Part of this research was funded by the Flemish FWO SBO S004017N IDEAL-IoT (Intelligent DEnse And Long range IoT networks) project, National Key Research and Development Program of China (No. 2019YFB1802500), and National Natural Science Foundation of China (No. 61702547, No. 6180249). Serena Santi is funded by the Flemish FWO under grant number 1S82120N.

References

[1] W. Kassab, K. A. Darabkh, A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations, Journal of Network and Computer Applications 163 (2020) 102663.

[2] P. K. Verma, R. Verma, A. Prakash, A. Agrawal, K. Naik, R. Tripathi, M. Alsabaan, T. Khalifa, T. Abdelkader, A. Abogharaf, Machine-to-Machine (M2M) communications: A survey, Journal of Network and Computer Applications 66 (2016) 83 – 105.

[3] IEEE standard for local and metropolitan area networks–part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006) (2011) 1–314.

[4] C. Gomez, J. Oller, J. Paradells, Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology, Sensors 12 (12) (2012) 11734–11753.

[5] U. Raza, P. Kulkarni, M. Sooriyabandara, Low power wide area networks: An overview, IEEE Communications Surveys Tutorials 19 (2) (2017) 855–873.

[6] M. I. Hussain, Z. I. Ahmed, N. Sarma, D. K. Saikia, An efficient TDMA MAC protocol for multi-hop wifi-based long distance networks, Wireless Personal Communications 86 (4) (2016) 1971–1994.

[7] R. Patra, S. Nedevschi, S. Surana, A. Sheth, L. Subramanian, E. Brewer, Wildnet: design and implementation of high performancewifi based long distance networks, in: NSDI'07 Proceedings of the 4th USENIX conference on Networked systems design and implementation, 2007, pp. 7–7.

[8] M. Ridolfi, S. Van de Velde, H. Steendam, E. De Poorter, WiFi ad-hoc mesh network and MAC protocol solution for UWB indoor localization systems, in: 2016 Symposium on Communications and Vehicular Technologies (SCVT), 2016, pp. 1–6.

[9] M. Murad, A. M. Eltawil, A simple full-duplex MAC protocol exploiting asymmetric traffic loads in wifi systems, in: 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017, pp. 1–6.

[10] G. Wang, Y. Qin, Mac protocols for wireless mesh networks with multi-beam antennas: A survey, in: K. Arai, R. Bhatia (Eds.), Advances in Information and Communication, Springer International Publishing, Cham, 2020, pp. 117–142.

[11] S. Han, Y. Liang, Q. Chen, B. Soong, Licensed-assisted access for LTE in unlicensed spectrum: A MAC protocol design, IEEE Journal on Selected Areas in Communications 34 (10) (2016) 2550–2561.

[12] IEEE standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless LAN MAC and PHY specifications amendment 2: Sub 1 GHz license exempt operation, IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016) (2017) 1–594doi:10.1109/IEEESTD.2017.7920364.

[13] E. Khorov, A. Lyakhov, A. Krotov, A. Guschin, A survey on IEEE 802.11ah: An enabling networking technology for smart cities, Computer Communications 58 (2015) 53–69. doi:10.1016/j.comcom.2014.08.008.

[14] L. F. Del Carpio, P. Di Marco, P. Skillermark, R. Chirikov, K. Lagergren, Comparison of 802.11ah, BLE and 802.15. 4 for a home automation use case, International Journal of Wireless Information Networks 24 (3) (2017) 243–253.

[15] N. Ahmed, H. Rahman, M. Hussain, A comparison of 802.11ah and 802.15.4 for IoT, ICT Express 2 (3) (2016) 100 – 102, special Issue on ICT Convergence in the Internet of Things (IoT).

[16] J. Famaey, The long life of iot devices: Comparing the energy consumption of sub-1ghz wireless technologies, accessed: 2020-05-10.
URL https://www.researchgate.net/publication/338920462_The_Long _Life_of_IoT_Devices_Comparing _the_Energy_Consumption_of_Sub-1GHz_Wireless_Technologies

[17] Wi-Fi HaLow Technology Overview (2020), accessed: 2020-05-10.
URL https://www.wi-fi.org/downloads-registered-guest/WiFi_HaLow_Technology_Overview_20200518 _0.pdf/36879

[18] C. Kuhlins, B. Rathonyi, A. Zaidi, M. Hogan, Cellular networks for massive IoT, Ericsson White Paper (2020).

[19] Q. Pan, X. Wen, Z. Lu, W. Jing, L. Li, Cluster-based group paging for massive machine type communications under 5G networks, IEEE Access 6 (2018) 64891–64904.

[20] R. S. Sinha, Y. Wei, S.-H. Hwang, A survey on LPWA technology: LoRa and NB-IoT, ICT Express 3 (1) (2017) 14 – 21.

[21] A. Seferagić, J. Famaey, E. De Poorter, J. Hoebeke, Survey on wireless technology trade-offs for the industrial Internet of Things, Sensors 20 (2) (2020) 488.

[22] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Communications Surveys and Tutorials 17 (4) (2015) 2347–2376. doi:10.1109/COMST.2015.2444095.

[23] A. Ali, G. A. Shah, M. O. Farooq, U. Ghani, Technologies and challenges in developing machine-to-machine applications: A survey, Journal of Network and Computer Applications 83 (2017) 124 – 139. doi:https://doi.org/10.1016/j.jnca.2017.02.002.
URL `http://www.sciencedirect.com/science/article/pii/S1084804517300620`

[24] W. Sun, M. Choi, S. Choi, IEEE 802.11ah: A long range 802.11 WLAN at Sub-1GHz, Journal of ICT Standardization 2 (2) (2013) 83–108.

[25] T. Adame, A. Bel, B. Bellalta, J. Barcelo, M. Oliver, IEEE 802.11ah: the WiFi approach for M2M communications, IEEE Wireless Communications 21 (6) (2014) 144–152. doi:10.1109/MWC.2014.7000982.

[26] M. Park, IEEE 802.11ah: Sub-1GHz license-exempt operation for the Internet of Things, IEEE Communications Magazine 53 (9) (2015) 145–151. doi:10.1109/MCOM.2015.7263359.

[27] V. Baños-Gonzalez, M. S. Afaqui, E. Lopez-Aguilera, E. Garcia-Villegas, IEEE 802.11ah: A technology to face the IoT challenge, Sensors 16 (11) (2016). doi:10.3390/s16111960.

[28] M. S. Meera, S. N. Rao, A survey of the state of the art of 802.11ah, in: 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2017, pp. 1–4.

[29] L. Zheng, M. Ni, L. Cai, J. Pan, C. Ghosh, K. Doppler, Performance analysis of group-synchronized DCF for dense IEEE 802.11 networks, IEEE Transactions on Wireless Communications 13 (11) (2014) 6180–6192. doi:10.1109/TWC.2014.2337315.

[30] R. Porat, TGah channel model, accessed: 2020-05-07.
URL `https://mentor.ieee.org/802.11/dcn/11/11-11-0968-04-00ah-channel-model-text.docx.`

[31] E. Garcia-Villegas, Corrections to tgah channel model, accessed: 2020-05-07.
URL `https://mentor.ieee.org/802.11/dcn/15/11-15-0425-00-00ah-corrections-to-tgah-channel-model.pptx.`

[32] A. Hazmi, J. Rinne, M. Valkama, Feasibility study of IEEE 802.11ah radio technology for IoT and M2M use cases, in: 2012 IEEE Globecom Workshops, IEEE, 2012, pp. 1687–1692. doi:10.1109/GLOCOMW.2012.6477839.

[33] M. Li, D. Wang, Indoor coverage performance comparison between IEEE 802.11g and IEEE 802.11ah of wireless nodes in M2M network, in: Proceedings of the 1st International Conference on Internet of Vehicles, Springer International Publishing, 2014, pp. 211–217. doi:10.1007/978-3-319-11167-4.

[34] S. Khan, M. Zeeshan, Performance and throughput analysis of IEEE 802.11ah for multiband multimode operation, in: 2018 21st International Symposium on Wireless Personal Multimedia Communications (WPMC), IEEE, 2018, pp. 150–155.

[35] S. Khan, M. Zeeshan, Y. Ayaz, Implementation and analysis of multicode multicarrier code division multiple access (mc–mc cdma) in ieee 802.11ah for uav swarm communication, Physical Communication 42 (2020) 101159. doi:https://doi.org/10.1016/j.phycom.2020.101159.

[36] S. Aust, T. Ito, Sub 1GHz wireless LAN propagation path loss models for urban smart grid applications,

in: 2012 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2012, pp. 116–120. doi:10.1109/ICCNC.2012.6167392.

[37] B. Bellekens, L. Tian, P. Boer, M. Weyn, J. Famaey, Outdoor IEEE 802.11ah range characterization using validated propagation models, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.

[38] T. De Koninck, S. Santi, F. Lemic, J. Famaey, Experimental validation of IEEE 802.11ah propagation models in heterogeneous smarty city environments, in: IEEE Global Communications Conference (Globecom), 2020.

[39] H. Wang, Supporting authentication/association for large number of stations, accessed: 2020-05-07. URL `https://mentor.ieee.org/802.11/dcn/12/11-12-0112-04-00ah-supporting-of-the-authentication-association-for-large-number-of-stations.pptx`

[40] L. Tian, S. Deronne, S. Latré, J. Famaey, Implementation and validation of an IEEE 802.11ah module for ns-3, in: Proceedings of the Workshop on Ns-3 (WNS3), 2016, pp. 49–56. doi:10.1145/2915371.2915372.

[41] D. Bankov, E. Khorov, A. Lyakhov, E. Stepanova, Fast centralized authentication in Wi-Fi halow networks, in: 2017 IEEE International Conference on Communications (ICC), IEEE, 2017, pp. 1–6.

[42] D. Bankov, E. Khorov, A. Lyakhov, E. Stepanova, L. Tian, J. Famaey, What is the fastest way to connect stations to a Wi-Fi HaLow network?, Sensors 18 (9) (2018) 2744.

[43] N. Shahin, R. Ali, Y.-T. Kim, Hybrid slotted-CSMA/CA-TDMA for efficient massive registration of IoT devices, IEEE Access 6 (2018) 18366–18382.

[44] W. Yin, P. Hu, W. Wang, J. Wen, H. Zhou, FASUS: A fast association mechanism for 802.11ah networks, Computer Networks 175 (2020) 107287. doi:https://doi.org/10.1016/j.comnet.2020.107287.

[45] D. Bankov, E. Khorov, A. Lyakhov, The study of the centralized control method to hasten link set-up in IEEE 802.11ah networks, in: Proceedings of European Wireless 2015; 21th European Wireless Conference, VDE, 2015, pp. 1–6.

[46] P. Sthapit, J.-Y. Pyun, Station grouping strategy for minimizing association delay in IEEE 802.11ah, IEICE Transactions on Communications 100 (8) (2017) 1419–1427.

[47] D. Bankov, E. Khorov, et al., The study of the distributed control method to hasten link set-up in IEEE 802.11ah networks, in: 2016 XV International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY), IEEE, 2016, pp. 13–17.

[48] Y. Zhao, O. N. C. Yilmaz, A. Larmo, Optimizing M2M energy efficiency in IEEE 802.11ah, in: IEEE Globecom Workshops (GC Wkshps), 2015, pp. 1–6. doi:10.1109/GLOCOMW.2015.7414004.

[49] L. Tian, J. Famaey, S. Latré, Evaluation of the IEEE 802.11ah restricted access window mechanism for dense IoT networks, in: IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016. doi:10.1109/WoWMoM.2016.7523502.

[50] M. Qutab-ud din, A. Hazmi, B. Badihi, A. Larmo, J. Torsner, M. Valkama, Performance analysis of IoT-enabling IEEE 802.11ah technology and its RAW mechanism with non-cross slot boundary holding schemes, in: IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015. doi:10.1109/WoWMoM.2015.7158204.

[51] Y. Tay, K. C. Chua, A capacity analysis for the IEEE 802.11 mac protocol, Wireless networks 7 (2) (2001)

159–171.

[52] R. Zhang, R. Ruby, J. Pan, L. Cai, X. Shen, A hybrid reservation/contention-based mac for video streaming over wireless networks, IEEE Journal on Selected Areas in Communications 28 (3) (2010) 389–398.

[53] L. Zheng, L. Cai, J. Pan, M. Ni, Performance analysis of grouping strategy for dense IEEE 802.11 networks, in: IEEE Global Communications Conference (GLOBECOM), pp. 219–224. doi:10.1109/GLOCOM.2013.6831074.

[54] O. Raeesi, J. Pirskanen, A. Hazmi, T. Levanen, M. Valkama, Performance evaluation of IEEE 802.11ah and its restricted access window mechanism, in: IEEE International Conference on Communications Workshops (ICC), 2014, pp. 460–466. doi:10.1109/ICCW.2014.6881241.

[55] O. Raeesi, J. Pirskanen, A. Hazmi, J. Talvitie, M. Valkama, Performance enhancement and evaluation of IEEE 802.11ah multi-access point network using restricted access window mechanism, in: IEEE International Conference on Distributed Computing in Sensor Systems, 2014, pp. 287–293. doi:10.1109/DCOSS.2014.18.

[56] E. Khorov, A. Lyakhov, R. Yusupov, Two-slot based model of the IEEE 802.11ah restricted access window with enabled transmissions crossing slot boundaries, in: 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE, 2018, pp. 1–9.

[57] G. Bianchi, Performance analysis of the IEEE 802.11 distributed coordination function, IEEE Journal on selected areas in communications 18 (3) (2000) 535–547.

[58] E. Khorov, A. Krotov, A. Lyakhov, Modelling machine type communication in IEEE 802.11ah networks, IEEE International Conference on Communication Workshop (ICCW) (14) (2015) 1149–1154. doi:10.1109/ICCW.2015.7247332.

[59] S. Santi, L. Tian, E. Khorov, J. Famaey, Accurate energy modeling and characterization of IEEE 802.11ah RAW and TWT, Sensors 19 (11) (2019) 2614.

[60] T.-C. Chang, C.-H. Lin, K. C.-J. Lin, W.-T. Chen, Traffic-aware sensor grouping for IEEE 802.11ah networks: Regression based analysis and design, IEEE Transactions on Mobile Computing 18 (3) (2018) 674–687.

[61] L. Tian, M. Mehari, S. Santi, S. Latré, E. De Poorter, J. Famaey, IEEE 802.11ah restricted access window surrogate model for real-time station grouping, in: IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2018, pp. 1–9.

[62] L. Tian, E. Lopez-Aguilera, E. Garcia-Villegas, M. T. Mehari, E. De Poorter, S. Latré, J. Famaey, Optimization-oriented RAW modeling of IEEE 802.11ah heterogeneous networks, IEEE Internet of Things Journal 6 (6) (2019) 10597–10609.

[63] D. Gorissen, I. Couckuyt, P. Demeester, T. Dhaene, K. Crombecq, A surrogate modeling and adaptive sampling toolbox for computer based design, J. Mach. Learn. Res. 11 (2010) 2051–2055.

[64] A. Ometov, N. Daneshfar, A. Hazmi, S. Andreev, L. F. D. Carpio, P. Amin, J. Torsner, Y. Koucheryavy, M. Valkama, System-level analysis of IEEE 802.11ah technology for unsaturated MTC traffic, International Journal of Sensor Networks 26 (4) (2018) 269–282.

[65] M. Z. Ali, J. Misic, V. B. Misic, Efficiency of restricted access window scheme of IEEE 802.11ah under non-ideal channel condition, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 251–256.

[66] M. Z. Ali, J. Misic, V. B. Misic, Differentiated QoS to heterogeneous IoT nodes in IEEE 802.11ah RAW mechanism, in: 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, 2018, pp. 1–6.

[67] M. Z. Ali, J. Mišić, V. B. Mišić, Performance evaluation of heterogeneous IoT nodes with differentiated QoS in IEEE 802.11ah RAW mechanism, IEEE Transactions on Vehicular Technology 68 (4) (2019) 3905–3918.

[68] Y. Wang, Y. Li, K. K. Chai, Y. Chen, J. Schormans, Energy-aware adaptive restricted access window for IEEE 802.11ah based smart grid networks, in: IEEE International Conference on Smart Grid Communications (SmartGridComm), 2015, pp. 581–586. doi:10.1109/SmartGridComm.2015.7436363.

[69] Y. Wang, K. K. Chai, Y. Chen, J. Schormans, J. Loo, Energy-aware Restricted Access Window control with retransmission scheme for IEEE 802.11ah (Wi-Fi HaLow) based networks, in: 2017 13th Annual Conference on Wireless On-Demand Network Systems and Services, WONS 2017 - Proceedings, 2017, pp. 69–76. doi:10.1109/WONS.2017.7888774.

[70] C. Kai, J. Zhang, X. Zhang, W. Huang, Energy-efficient sensor grouping for IEEE 802.11ah networks with max-min fairness guarantees, IEEE Access 7 (2019) 102284–102294.

[71] L. Beltramelli, P. Österberg, U. Jennehag, M. Gidlund, Hybrid MAC mechanism for energy efficient communication in IEEE 802.11ah, in: Industrial Technology (ICIT), 2017 IEEE International Conference on, 2017. doi:10.1109/ICIT.2017.7915550.

[72] N. Nawaz, M. Hafeez, S. A. R. Zaidi, D. C. McLernon, M. Ghogho, Throughput enhancement of restricted access window for uniform grouping scheme in IEEE 802.11ah, in: 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–7. doi:10.1109/ICC.2017.7996899.

[73] T.-C. Chang, C.-H. Lin, K. C.-J. Lin, W.-T. Chen, Load-balanced sensor grouping for IEEE 802.11ah networks, in: 2015 IEEE global communications conference (GLOBECOM), IEEE, 2015, pp. 1–6.

[74] L. Tian, E. Khorov, S. LatrÃ©, J. Famaey, Real-time station grouping under dynamic traffic for IEEE 802.11ah, Sensors 17 (7) (2017). doi:10.3390/s17071559.
URL http://www.mdpi.com/1424-8220/17/7/1559

[75] L. Tian, S. Santi, S. Latré, J. Famaey, Accurate sensor traffic estimation for station grouping in highly dense IEEE 802.11ah networks, in: 15th ACM Conference on Embedded Networked Sensor Systems Workshops (SenSys), 2017.

[76] N. Ahmed, M. I. Hussain, Periodic traffic scheduling for IEEE 802.11ah networks, IEEE Communications Letters (2020) 1–4.

[77] L. Tian, M. T. Mehari, S. Santi, S. Latré, E. De Poorter, J. Famaey, Multi-objective surrogate modeling for real-time energy-efficient station grouping in IEEE 802.11ah, Pervasive and Mobile Computing 57 (2019) 33–48.

[78] E. Khorov, A. Lyakhov, I. Nasedkin, R. Yusupov, J. Famaey, I. F. Akyildiz, Fast and reliable alert delivery in mission-critical Wi-Fi HaLow sensor networks, IEEE Access 8 (2020) 14302–14313.

[79] G. C. Madueno, C. Stefanovic, P. Popovski, Reliable and efficient access for alarm-initiated and regular M2M traffic in IEEE 802.11ah systems, IEEE Internet of Things Journal 3 (5) (2016) 673–682.

[80] N. F. Charania, M. K. Giluka, B. R. Tamma, A. Franklin, DEARF: Delay and energy aware RAW formation scheme to support delay sensitive M2M traffic in IEEE 802.11ah networks, arXiv preprint arXiv:1709.03723

(2017).

[81] K. Ogawa, M. Morikura, K. Yamamoto, T. Sugihara, IEEE 802.11ah based M2M networks employing virtual grouping and power saving methods, IEICE Transactions on Communications E96-B (12) (2013) 2976–2985.

[82] C.-M. Huang, R.-S. Cheng, Y.-M. Li, The registration-based collision avoidance mechanism for IEEE 802.11ah, in: International Symposium on Pervasive Systems, Algorithms and Networks, Springer, 2019, pp. 240–255.

[83] H. Nabuuma, E. Alsusa, M. W. Baidas, AID-based backoff for throughput enhancement in 802.11ah networks, International Journal of Communication Systems 32 (7) (2019).

[84] H. Nabuuma, E. Alsusa, Enhancing the throughput of 802.11ah sectorized networks using AID-based backoff counters, in: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2017, pp. 1921–1926.

[85] C. W. Park, D. Hwang, T.-J. Lee, Enhancement of IEEE 802.11ah MAC for M2M communications, IEEE Communications Letters 18 (7) (2014) 1151–1154. doi:10.1109/LCOMM.2014.2323311.

[86] U. Sangeetha, A. Babu, Fair and efficient resource allocation in IEEE 802.11ah wlan with heterogeneous data rates, Computer Communications 151 (2020) 154–164.

[87] M. Mahesh, B. S. Pavan, V. P. Harigovindan, Data rate based grouping to resolve performance anomaly of multi-rate IEEE 802.11ah IoT networks, IEEE Networking Letters (2020) 1–5.

[88] L. R. Lakshmi, B. Sikdar, Achieving fairness in IEEE 802.11ah networks for IoT applications with different requirements, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.

[89] H. Mosavat-Jahromi, Y. Li, L. Cai, A throughput fairness-based grouping strategy for dense IEEE 802.11ah networks, in: 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2019, pp. 1–6.

[90] N. Ahmed, D. De, M. I. Hussain, A QoS-aware MAC protocol for IEEE 802.11ah-based Internet of Things, in: 2018 Fifteenth International Conference on Wireless and Optical Communications Networks (WOCN), IEEE, 2018, pp. 1–5.

[91] M. Mahesh, V. Harigovindan, Restricted access window-based novel service differentiation scheme for group-synchronized DCF, IEEE Communications Letters 23 (5) (2019) 900–903.

[92] M. Park, IEEE 802.11ah: Energy efficient MAC protocols for long range wireless LAN, in: IEEE International Conference on Communications (ICC), 2014, pp. 2388–2393. doi:10.1109/ICC.2014.6883680.

[93] M. Dong, Z. Wu, X. Gao, H. Zhao, An efficient spatial group restricted access window scheme for IEEE 802.11ah networks, in: Sixth International Conference on Information Science and Technology (ICIST), 2016, pp. 168–173. doi:10.1109/ICIST.2016.7483405.

[94] W. Damayanti, S. Kim, J.-H. Yun, Collision chain mitigation and hidden device-aware grouping in large-scale IEEE 802.11ah networks, Computer Networks 108 (2016) 296–306. doi:10.1016/j.comnet.2016.09.006.

[95] S. G. Yoon, J. O. Seo, S. Bahk, Regrouping algorithm to alleviate the hidden node problem in 802.11ah networks, Computer Networks 105 (2016) 22–32. doi:10.1016/j.comnet.2016.05.011.

[96] Z. Zhu, Z. Zhong, Z. Fan, A station regrouping method for contention based IEEE 802.11ah wireless LAN, in: 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications

(WiMob), IEEE, 2017, pp. 1–6.

[97] R. Wang, M. Lin, Restricted access window based hidden node problem mitigating algorithm in IEEE 802.11ah networks, IEICE Transactions on Communications (2018) 2017EBP3462.

[98] M. Ghasemiahmadi, Y. Li, L. Cai, RSS-based grouping strategy for avoiding hidden terminals with GS-DCF MAC protocol, in: 2017 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2017, pp. 1–6.

[99] C.-C. Hu, Approximation algorithms of minimizing hidden pairs in 802.11ah networks, IEEE Access 7 (2019) 170742–170752.

[100] B. Ji, S. Chen, K. Song, C. Li, H. Chen, Z. Li, Throughput enhancement schemes for IEEE 802.11ah based on multi-layer cooperation, in: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), 2015, pp. 1112–1116. doi:10.1109/IWCMC.2015.7289238.

[101] B. Badihi, L. F. D. Carpio, P. Amin, A. Larmo, M. Lopez, D. Denteneer, Performance evaluation of IEEE 802.11ah actuators, in: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), 2016, pp. 1–5. doi:10.1109/VTCSpring.2016.7504414.

[102] T. Kim, J. M. Chang, Enhanced power saving mechanism for large-scale 802.11ah wireless sensor networks, IEEE Transactions on Green Communications and Networking 1 (4) (2017) 516–527.

[103] T. Kim, Optimal resource scheduling for energy-efficient next generation wireless networks, Ph.D. thesis, Iowa State University (2018).

[104] A. Bel, T. Adame, B. Bellalta, An energy consumption model for IEEE 802.11ah WLANs, Ad Hoc Networks 72 (2018) 14–26.

[105] A. Kureev, D. Bankov, E. Khorov, A. Lyakhov, Improving efficiency of heterogeneous Wi-Fi networks with joint usage of TIM segmentation and restricted access window, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–5.

[106] A. Šljivo, D. Kerkhove, L. Tian, J. Famaey, A. Munteanu, I. Moerman, J. Hoebeke, E. De Poorter, Performance evaluation of IEEE 802.11ah networks with high-throughput bidirectional traffic, Sensors 18 (2) (2018) 325.

[107] A. Seferagić, I. Moerman, E. De Poorter, J. Hoebeke, Evaluating the suitability of IEEE 802.11ah for low-latency time-critical control loops, IEEE Internet of Things Journal 6 (5) (2019) 7839–7848.

[108] D. L. Hoang, T. H. Tran, Y. Nakashima, Performance evaluation of 802.11ah physical layer phase encryption for IoT applications, in: 2018 International Conference on Advanced Technologies for Communications (ATC), 2018.

[109] D. L. Hoang, T. H. Tran, Y. Nakashima, Hardware implementation of CORDIC based physical layer phase decryption for IEEE 802.11ah, in: Proceedings of the 7th International Conference on Communications and Broadband Networking, ICCBN 2019, Association for Computing Machinery, New York, NY, USA, 2019, p. 17–21.

[110] L. Zhang, M. Ma, Performance and security enhancements to fast initial link setup in IEEE 802.11ah wireless networks, in: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018, pp. 1–6.

[111] L. Zhang, M. Ma, FKR: An efficient authentication scheme for IEEE 802.11ah networks, Computers & Security

88 (2020) 101633.

[112] K. Ki-Wook, H. Youn-Hee, M. Sung-Gi, An authentication and key management mechanism for resource constrained devices in IEEE 802.11-based iot access networks, Sensors 17 (10) (2017) 2170.

[113] J. T. Liew, F. Hashim, A. Sali, M. F. A. Rasid, K. Cumanan, Performance evaluation of backoff misbehaviour in IEEE 802.11ah using evolutionary game theory, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–7.

[114] X. Zhang, Enhancing IEEE 802.11ah for the Internet of Things, Ph.D. thesis, The University of Hong Kong (2018).

[115] S. Santi, L. Tian, J. Famaey, Evaluation of the co-existence of raw and twt stations in ieee 802.11ah using ns-3, in: Proceedings of the 2019 Workshop on Next-Generation Wireless with Ns-3, WNGW 2019, Association for Computing Machinery, New York, NY, USA, 2019, pp. 9–12.

[116] D. Bankov, E. Khorov, A. Lyakhov, E. Stepanova, Clock drift impact on target wake time in IEEE 802.11 ax/ah networks, in: 2018 Engineering and Telecommunication (EnT-MIPT), IEEE, 2018, pp. 30–34.

[117] S. Bhandari, S. K. Sharma, X. Wang, Device grouping for fast and efficient channel access in IEEE 802.11ah based IoT networks, in: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2018, pp. 1–6.

[118] Q. T. Ngo, D. N. M. Dang, Q. Le-Trung, D. K. Lam, A novel directional MAC in restricted access window for IEEE 802.11ah networks, in: 2019 26th International Conference on Telecommunications (ICT), IEEE, 2019, pp. 167–171.

[119] Q. T. Ngo, D. N. M. Dang, Q. Le-Trung, An extreme power saving directional MAC protocol in IEEE 802.11ah networks, IET Networks 9 (4) (2020).

[120] Y. Cheng, H. Zhou, D. Yang, CA-CWA: Channel-aware contention window adaption in IEEE 802.11ah for soft real-time industrial applications, Sensors 19 (13) (2019) 3002.

[121] X. Zhang, K. L. Yeung, LLE: A timer extension mechanism for alarm-triggered traffic in IEEE 802.11ah WLANs, in: 2017 IEEE International Conference on Communications (ICC), IEEE, 2017, pp. 1–6.

[122] A. J. Gopinath, B. Nithya, Mathematical and simulation analysis of contention resolution mechanism for IEEE 802.11ah networks, Computer Communications 124 (2018) 87–100.

[123] R. N. Muktiarto, D. Perdana, R. M. Negara, Performance analysis of mobility impact on IEEE 802.11ah standard with traffic pattern scheme, International Journal of Communication Networks and Information Security 10 (1) (2018) 139–147.

[124] S. Santi, F. Lemic, J. Famaey, On the Feasibility of Location-based Discovery and Vertical Handover in IEEE 802.11ah, in: 2020 IEEE Wireless Communications and Networking Conference (WCNC), 2020.

[125] E. Kocan, B. Domazetovic, M. Pejanovic-Djurisic, Range extension in IEEE 802.11ah systems through relaying, Wireless Personal Communications 97 (2) (2017) 1889–1910. doi:10.1007/s11277-017-4334-9.

[126] M. Z. Ali, J. Misic, V. B. Misic, Extending the operational range of UAV communication network using IEEE 802.11ah, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.

[127] N. Ahmed, S. Misra, Channel access mechanism for IEEE 802.11ah-based relay networks, in: ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–6.

[128] P. P. Libório, C. T. Lam, B. Ng, D. L. Guidoni, M. Curado, L. A. Villas, Network slicing in ieee 802.11ah, in: 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), IEEE, 2019, pp. 1–9.

[129] B. Pandya, T.-D. Chiueh, Interference aware coordinated multiuser access in multi-band WLAN for next generation low power applications, Wireless Networks 25 (4) (2019) 1965–1981.

[130] Y. Liu, J. Guo, P. Orlik, Y. Nagai, K. Watanabe, T. Sumi, Coexistence of 802.11ah and 802.15.4g networks, in: 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6. doi:10.1109/WCNC.2018.8376972.

[131] M. Saelens, J. Hoebeke, A. Shahid, E. De Poorter, Impact of eu duty cycle and transmission power limitations for sub-ghz lpwan srds: an overview and future challenges, EURASIP Journal on Wireless Communications and Networking 219 (2019).

[132] A. Hazmi, L. F. Del Carpio, A. Goekceoglu, B. Badihi, P. Amin, A. Larmo, M. Valkama, et al., Duty cycle challenges of IEEE 802.11ah networks in M2M and IoT applications, in: European Wireless 2016; 22th European Wireless Conference, VDE, 2016, pp. 1–7.

[133] M. Shafiq, M. Ahmad, A. Irshad, M. Gohar, M. Usman, M. Khalil Afzal, J.-G. Choi, H. Yu, Multiple access control for cognitive radio-based IEEE 802.11ah networks, Sensors 18 (7) (2018). doi:10.3390/s18072043.

[134] S. Aust, R. V. Prasad, I. G. M. M. Niemegeers, Performance study of MIMO-OFDM platform in narrow-band Sub-1GHz wireless LANs, in: 11th International Symposium on Modeling & Optimization in Mobile, Ad Hoc & Wireless Networks (WiOpt), IEEE, 2013, pp. 89–94.

[135] S. Aust, R. V. Prasad, Advances in wireless M2M and IoT: Rapid SDR-prototyping of IEEE 802.11ah, in: IEEE Local Computer Networks Conference, 2014.

[136] S. Tschimben, K. Gifford, R. Brown, IEEE 802.11 ah SDR Implementation and Range Evaluation, in: 2019 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2019, pp. 1–6.

[137] R. A. Casas, V. Papaparaskeva, R. Kumar, P. Kaul, S. Hijazi, An IEEE 802.11ah programmable modem, in: IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015. doi:10.1109/WoWMoM.2015.7158203.

[138] A. Ba, Y.-H. Liu, e. a. van den Heuvel, Johan, 26.3A 1.3nJ/b IEEE 802.11ah fully digital polar transmitter for IoE applications, in: IEEE International Solid-State Circuits Conference, 2016, pp. 440–441. doi:10.1109/ISSCC.2016.7418096.

[139] A. Ba, K. Salimi, P. Mateman, P. Boer, J. van den Heuvel, J. Gloudemans, J. Dijkhuis, M. Ding, Y.-H. Liu, C. Bachmann, G. Dolmans, K. Philips, A 4mW-RX 7mW-TX IEEE 802.11ah fully-integrated RF transceiver, in: Radio Frequency Integrated Circuits Symposium (RFIC), 2017 IEEE, IEEE, 2017, pp. 232–235.

[140] A. Bishnu, V. Bhatia, Receiver for IEEE 802.11ah in interference limited environments, IEEE Internet of Things Journal 5 (5) (2018) 4109–4118.

[141] Newracom Corp., Products, accessed: 2020-05-10.
URL `http://newracom.com/product/nrc7292/`.

[142] Methods2business Corp., Products, accessed: 2020-05-10.
URL `http://www.methods2business.com/products`.

[143] Newracom Corp., Product-brief-nrc7292, accessed: 2020-05-10.
URL http://newracom.com/wp-content/uploads/2019/01/Product-Brief-NRC7292.pdf.

[144] M. Živković, B. Nikolić, J. Protić, R. Popović, A survey and classification of wireless sensor networks simulators based on the domain of use, Adhoc & Sensor Wireless Networks 20 (2014).

[145] IEEE 802.11ah waveform generation, accessed: 2020-05-07.
URL https://www.mathworks.com/help/wlan/examples/802-11ah-waveform-generation.html.

[146] L. Tian, A. Šljivo, S. Santi, E. De Poorter, J. Hoebeke, J. Famaey, Extension of the IEEE 802.11ah ns-3 simulation module, in: Proceedings of the 10th Workshop on Ns-3, WNS3 '18, ACM, New York, NY, USA, 2018, pp. 53–60. doi:10.1145/3199902.3199906.

[147] ns-3 network simulator, accessed: 2020-09-29.
URL https://www.nsnam.org.

[148] IEEE-802.11ah-ns-3, accessed: 2020-05-07.
URL https://github.com/imec-idlab/IEEE-802.11ah-ns-3.

[149] A. Šljivo, D. Kerkhove, I. Moerman, E. De Poorter, J. Hoebeke, Interactive web visualizer for IEEE 802.11ah ns-3 module, in: Proceedings of the 10th Workshop on ns-3, 2018, pp. 23–29.

[150] R. Compton, M. T. Mehari, C. J. Colbourn, E. De Poorter, V. R. Syrotiuk, Screening interacting factors in a wireless network testbed using locating arrays, in: 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 650–655.

[151] S. Chieochan, E. Hossain, J. Diamond, Channel assignment schemes for infrastructure-based 802.11 WLANs: A survey, IEEE Communications Surveys Tutorials 12 (1) (2010) 124–136.

[152] F. Wilhelmi, S. Barrachina-Muñoz, B. Bellalta, C. Cano, A. Jonsson, G. Neu, Potential and pitfalls of multi-armed bandits for decentralized spatial reuse in WLANs, Journal of Network and Computer Applications 127 (2019) 26 – 42. doi:https://doi.org/10.1016/j.jnca.2018.11.006.

[153] A. Shahid, J. Fontaine, M. Camelo, J. Haxhibeqiri, M. Saelens, Z. Khan, I. Moerman, E. De Poorter, A convolutional neural network approach for classification of lpwan technologies: Sigfox, LoRa and IEEE 802.15. 4g, in: 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 2019, pp. 1–8.

[154] J. Fontaine, A. Shahid, R. Elsas, A. Seferagić, I. Moerman, E. De Poorter, Multi-band sub-GHz technology recognition on NVIDIA's Jetson Nano, in: 2020 IEEE 92nd Vehicular Technology Conference (IEEE VTC), IEEE, 2020.

[155] Time-Sensitive Networking (TSN) Task Group, https://1.ieee802.org/tsn/.

[156] J. Sachs, G. Wikstrom, T. Dudda, R. Baldemair, K. Kittichokechai, 5G radio network design for ultra-reliable low-latency communication, IEEE network 32 (2) (2018) 24–31.

[157] J. Farkas, B. Varga, G. Miklós, J. Sachs, 5G-TSN integration meets networking requirements for industrial automation, Ericsson technology review (2019).

[158] O. Seijo, I. Val, J. A. Lopez-Fernandez, w-SHARP: Implementation of a high-performance wireless time-sensitive network for low latency and ultra-low cycle time industrial applications, IEEE Transactions on Industrial Informatics (2020).

[159] M. Luvisotto, Z. Pang, D. Dzung, High-performance wireless networks for industrial control applications: New targets and feasibility, Proceedings of the IEEE 107 (6) (2019) 1074–1093.

[160] E. Genc, L. F. Del Carpio, Wi-Fi QoS enhancements for downlink operations in industrial automation using TSN, in: 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS), IEEE, 2019, pp. 1–6.