Evaluating the Suitability of IEEE 802.11ah for Low-Latency Time-Critical Control Loops

Amina Seferagić, Ingrid Moerman, Eli De Poorter, and Jeroen Hoebeke

***Abstract*—A number of industrial wireless technologies have emerged over the last decade, promising to replace the need for wires in a variety of use cases. Except for customized time division multiple access (TDMA)-based wireless technologies that can achieve ultralow latency over a very limited area, wireless communication generally has reliability and latency issues when it comes to industrial applications. Closed loop communication requires high reliability (over 99%), limited jitter and latency, which poses a challenge especially over a wide area measuring in hundreds of meters. Extended coverage is promised with the advent of sub-GHz technologies, one of them being IEEE 802.11ah which is the only one that offers sufficient data rate for frequent bidirectional communication. Thus, we evaluated IEEE 802.11ah for low-latency time-critical control loops. We propose the network setup for adjusting the network dynamics to that of control loops, enabling limited jitter and high reliability. We explore the scalability of IEEE 802.11ah network hosting both control loops and monitoring sensors that periodically transmit measurements. Assigning the control loop end-nodes to dedicated restricted access window (RAW) slot results in over 99.99% successful deliveries. Furthermore, interpacket delay is concentrated around the cycle-time in the following or preceding beacon interval in case the beacon interval is at least half the value of the shortest cycle-time. Adjusting the beacon interval to the fastest control loop in the network ensures latency requirements at the cost of maximum achievable throughput and energy consumption.**

***Index Terms*—IEEE 802.11ah, IIoT, M2M communication, Wi-Fi HaLow, wireless control loop.**

I. Introduction

THE ADVENT of Industry 4.0 initiates the modernization of plants and factories. To remain competitive, factories need to *get smarter*, namely, continuously monitor their product quality, adequately synchronize the processes to optimize their efficiency, and cope with dynamic market demands by supporting more flexible and adaptive production processes. Collecting and distributing data within a plant via physical wires, as it has been done so far, brings numerous complications. Wiring is often difficult in hard-to-reach places or on mobile assets (cranes, robots, automated guided vehicles, etc.). It is expensive due to vast amount of needed materials and labor. It is also fault-prone due to degradation of wires, miswiring due to human error, etc. Besides the obvious physical benefit of reducing excessive wiring, wireless networks also introduce a number of logical benefits [1] such as "hot-swapping" between a faulty module and a backup module via a simple activation command, and facilitating "plug-n-play" automation architectures which reduce downtime [2].

However, wireless networks are not yet widely accepted by the industry as they are fundamentally unreliable. The probability that a wireless transmission (TX) will be received (RX) by the destination depends on various factors, including the amount of power used to transmit information, environmental conditions that affect the propagation characteristics of the channel, and collisions that might occur due to multiple nodes transmitting at the same time. Another problem is the need to maintain a reasonable end-to-end delay in the network. The field network in a plant connects time-critical components of machinery, such as sensors, actuators, and motors. There is also a continuous need to improve productivity and safety while at the same time reducing costs. In general this means more measurements. In many cases the most effective way to add these measurements is with wireless instruments that use an existing process control application language.

Over the last decades wireless networks have started to emerge which aim to alleviate these issues in control systems [3]. Customized time division multiple access (TDMA)-based wireless solutions, such as WirelessHP [4], OFDMAwirelesscontrol [5], Real-Time-WiFi [6], and WIA-FA [7] can achieve latency in order of μs over a very short area (cca 10 m). Such technologies can be applied on production cells, robotic cells and similar concentrated areas. Larger coverage is provided by 802.15.4- and 802.15.1-based technologies which have much larger latency (hundreds of ms or even seconds). Utilizing the 2.4-GHz ISM band, the communication range is rather limited, up to 100 m with direct line of sight, but significantly less in industrial environments. This makes them badly suited for large-scale industry processes. To cover larger areas, a multihop network is necessary with a number of disadvantages as a consequence: lower throughput and difficulties to create and maintain a network. In addition, the achievable latency and reliability in multihop networks are not in line with the strict requirements of most industry processes [8], [9]. To solve these key issues, interest has been shifted toward wireless technologies that are capable of covering larger areas (indoors and outdoors) negating the need

Manuscript received October 12, 2018; revised February 6, 2019 and April 1, 2019; accepted May 9, 2019. Date of publication May 14, 2019; date of current version October 8, 2019. This work was supported by the Intelligent Dense and Longe Range IoT Networks SBO Project funded by the Fund for Scientific Research-Flanders (FWO-V) under Grant S004017N.
(Corresponding author: Amina Seferagić.)

The authors are with the Department of Information Technology, Internet and Data Lab, Ghent University—imec, 9000 Ghent, Belgium (e-mail: amina.seferagic@ugent.be).
Digital Object Identifier 10.1109/JIOT.2019.2916579

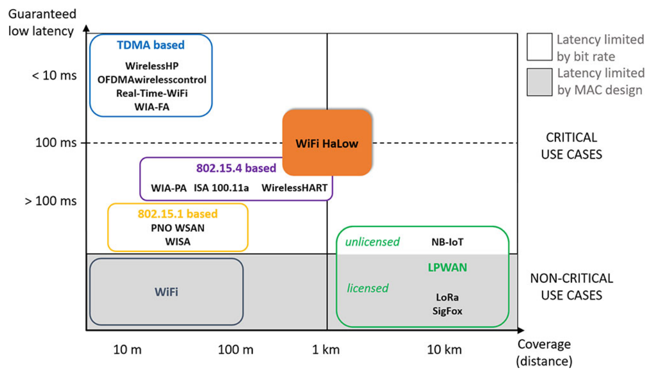

Fig. 1. IEEE 802.11ah (i.e., Wi-Fi HaLow) can cover low-latency use cases over mid-range area.

for expensive multihop networks. Sub-GHz technology satisfies this characteristic by being able to cover a range up to several kilometers due to better object penetration characteristics, whilst being even more scalable and power efficient. Different technologies have been developed that make use of the sub-GHz frequency bands (LoRaWAN, SigFox, and DASH7). These technologies are covered by the more generic term low power wide area networks (LPWANs). LPWAN technologies, such as LoRa and SigFox provide long range communication (up to 15 and 50 km, respectively), but have very low data rates (up to 50 and 0.1 kb/s, respectively). This leads to long packet transmission times in both uplink (UL) and downlink (DL). In DL, this also affects the available capacity of a gateway in serving multiple nodes in DL, as the gateway is bound to duty cycle limitations. These properties render low-latency closed loop communication infeasible. In fact, for all existing wireless technologies latency reduction is limited either by medium access control (MAC) design (Wi-Fi, LoRa, and SigFox) or by bit rate (others), as illustrated in Fig. 1. However, the new wireless standard IEEE 802.11ah [10] (branded as Wi-Fi HaLow) fills the gap when it comes to reliable and high-throughput applications over a somewhat smaller area. A single access point (AP) can provide connectivity between at most 8192 low-power devices at rates from 150 kb/s to 78 Mb/s over a range up to 1 km. It offers the same data rate for DL and UL traffic and, hence, could be used for high-throughput applications (e.g., firmware updates) and reliable monitoring (i.e., acknowledging every transmitted packet) [11].

Given that IEEE 802.11ah offers a configurable tradeoff between range, throughput, and energy efficiency, we explore the feasibility of its application to frequent actuation in closed loops where sensors and actuators are considered to be wireless devices, whereas controller is considered to be wired. The novel restricted access window (RAW) mechanism of IEEE 802.11ah on MAC layer guarantees to maximize the throughput for heterogeneous stations STAs. Therefore, we also investigate coexistence of control loops and constrained Internet of Things (IoT) devices (i.e., sensors) side by side. As the hardware supporting 802.11ah is not available at the market yet, we experimented with the beacon interval in ns-3 network simulator [12] to investigate the feasibility of in-time delivery of fast control loop traffic. We find the setups for which it is possible to serve the needs of control loops with various cycle-times, explore the scalability of such solutions, and derive best practices for network configuration depending on loops' dynamics.

The remainder of this paper is structured as follows. Section II introduces the related research on both IEEE 802.11ah and wireless control loops. Section III gives an overview of the IEEE 802.11ah features relevant for this paper. Section IV elaborates the challenges present in applying IEEE 802.11ah to control loops. Section V presents the simulation environment and the setup of performed experiments, whereas Section VI discusses the obtained results along with the theoretical limits. Section VII compares IEEE 802.11ah to both IEEE 802.11 and IEEE 802.15.4e in terms of latency in typical industrial use cases. The conclusions and perspectives are presented in Section VIII.

II. Related Work

Despite its novelty, many features of IEEE 802.11ah have already been studied in literature. Evaluations and overviews of IEEE 802.11ah gradually led to analytical models and novel solutions for performance improvement of the technology, namely, optimization of energy consumption, throughput enhancement, latency reduction, and hidden node mitigation, especially on MAC layer. In contrast to this paper, the vast majority of the studies considers wireless sensor network (WSN) scenarios with UL only traffic and optimizes the RAW mechanism.

Most of the available research that takes into account DL traffic models evaluates and/or optimizes energy consumption using traffic indication map (TIM) segmentation as summarized in Table I. Bel *et al.* [13] developed the analytical model for energy consumption that takes into account UL and DL transmission and multicast data reception. They validated their model on four use cases (agricultural monitoring, smart metering, industrial automation, and animal monitoring) experimentally evaluated in [14]. All four scenarios represent more-or-less-frequent monitoring. In addition, all four scenarios share the same DL interarrival time, that is, the time between two consecutive packets, fixed at a value of 4 min. Kureev *et al.* [15] developed a mathematical model of data transmission considering a heterogeneous network that consists of stations transmitting heavy data flows and of low-power stations rarely receiving single data packets. They study the impact of RAW and TIM segmentation on the aggregated throughput of the heavy transmitters and the average energy consumption of the low-power stations. Kim and Chang [16] proposed a way of utilizing unused association identifiers (AIDs) so as to reduce the number of unnecessary wake-ups of monitoring stations due to sharing TIM groups with controllable stations, thus reducing the energy consumption.

Ahmed *et al.* [18] proposed a quality of service (QoS)-aware priority grouping and RAW scheduling algorithm which provides QoS for the real-time event-driven traffic. They prioritize event-driven traffic over periodic traffic and assign stations to RAW according to their priority, where stations with higher

TABLE I
MAJORITY OF AVAILABLE IEEE 802.11AH RESEARCH CONSIDERING DL TRAFFIC (WITH OR WITHOUT UL) MODEL, EVALUATE, AND/OR OPTIMIZE ENERGY CONSUMPTION

Reference	Year	Traffic	T_{DL}^{min}	Objective	Beacon Interval (BI)	Validation tool
This article	2018	UL/DL	32ms	energy, latency, jitter, throughput	$9216\mu s \leq BI \leq 102.4ms$	ns-3
Bel et al. [13]	2015	UL/DL	240s	energy	$100ms \leq BI \leq 45.1s$	analytical, Matlab
Adame et al. [14]	2014	UL/DL	240s	energy	$200ms$	Matlab
Kureev et al. [15]	2017	UL/DL	400ms	energy, throughput	$400ms, 3200ms$	analytical, Matlab
Kim et al. [16]	2017	UL/DL	unknown	energy	unknown	analytical, Matlab, CVX
Badihi et al. [17]	2016	DL	150ms	energy, latency	$50ms, 100ms$	unknown simulator
Ahmed et al. [18]	2018	UL/DL (event-driven)	unknown	throughput	$100ms$	ns-3

T_{DL}^{min} - minimal packet scheduling interval in downlink.

TABLE II
IEEE 802.11AH MCSS FOR 2-MHZ BANDWIDTH, 1 SPATIAL STREAM, AND 8-μS GUARD INTERVAL

MCS	Data Rate [kbps]	TX time for 130 B [ms]	Coverage [m]
MCS0	650	2.72	920
MCS1	1300	1.92	780
MCS2	1950	1.64	660
MCS3	2600	1.52	540
MCS4	3900	1.36	420
MCS5	5200	1.32	340
MCS6	5850	1.28	300
MCS7	6500	1.28	280
MCS8	7800	1.24	200

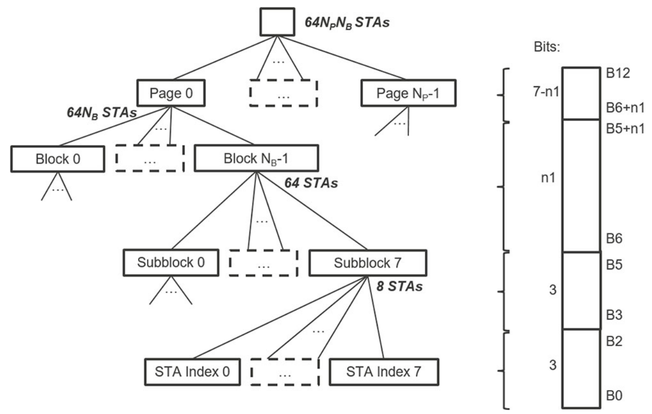

Fig. 2. Hierarchical structure of AIDs assigned by AP, which correspond to the ordinal bit numbers in traffic-indication virtual bitmap, where $2^{n_1} = N_B$.

priority get access at the beginning of an RAW. RAW scheduling for periodic stations is based on their periodicity, however, if a periodic station is assigned to RAW slot s and an event-driven station with higher priority needs access in RAW slot s, the algorithm changes the RAW assignment and assigns the event-driven stations to the RAW slot s, dropping the periodic station.

The only research so far that evaluated DL latency (aside from energy consumption) in an actuation use case for connected lighting, at the actuator side is [17]. They aim to find a number of actuators that can be served by a single AP, given that delay is within 150 ms. They used 50 and 100 ms beacon intervals divided by 1, 4, and 8 TIM groups. This paper extends [17] by considering: 1) various delay requirements, both shorter and longer, in control loops that include both sensing and actuation; 2) jitter in control loops; and 3) scalability of other monitoring-stations (UL only) operating alongside low-latency time-critical control loops (both UL and DL). Based on extensive experiments, it presents best practices for network configuration considering various dynamics of control loops, as well as coexistence of control loops and monitoring sensors in a single-hop wireless network.

III. IEEE 802.11AH OPERATION

IEEE 802.11ah supports up to 8192 associated stations per AP, a much higher value than the previous 802.11 iterations. Unlike other IEEE 802.11 models, IEEE 802.11ah stations can be configured to use only specific time slices between beacons where they are allowed to contend for the medium and communicate with the AP. The standard supports 1, 2, 4, 8, and 16-MHz channel bandwidths. However, only 1-and 2-MHz channels are available in Europe [10]. Table II summarizes the data rates, achievable ranges, and TX times for the corresponding modulation and coding schemes (MCSs) on the 2-MHz channel. TX time represents the time needed for both the transmission of a 130-byte packet and the reception of an acknowledgment (ACK). The coverage has been determined experimentally as the largest diameter $d = 2r$ of a circle around the AP on which ten evenly distributed stations can associate and successfully exchange a packet per second with the AP. Radii were varied in the increments of 10, and ten simulations with different random values were conducted for each radius setting.

There are two modes of operation defined by IEEE 802.11ah: 1) TIM mode and 2) non-TIM mode. Stations that operate in the two modes are referred to as TIM- and non-TIM stations, respectively. TIM stations have periodic access to the medium. They are typically used for high bandwidth requirements and for enabling DL access. They wake up periodically to receive the beacon indicating if there is buffered traffic at the AP. In order to prevent all the stations to wake up for the beacon, a power saving mechanism is introduced, called TIM segmentation [11].

Each station is assigned a unique 13-bit AID in the range $1-8191$ (AID 0 is reserved for group addressed traffic). The AID represents the station in a hierarchical structure as Fig. 2 illustrates. This hierarchy enables the AP to indicate in the bitmap whether a station has pending DL data buffered at the AP on multiple levels. For instance, the AP can indicate there is DL data pending for TIM group g in the delivery TIM (DTIM) beacon. All stations will check their own TIM group based on their assigned AID and only stations that

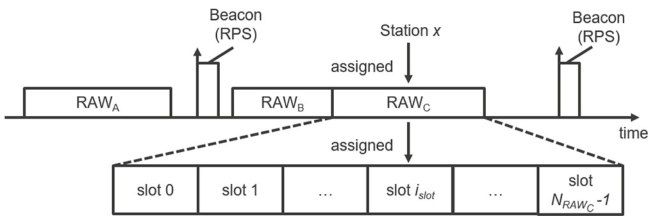

Fig. 3. RAW feature: the beacon carries a raw parameter set (RPS) element which defines the duration of RAW, the number of RAW groups within the beacon interval, their duration, the number of equal-sized slots within each group and the assigned stations.

belong to TIM group g will wake up in time for the TIM beacon of TIM group g to hear which station-index has data to expect, whereas all the remaining stations from other TIM groups can resume sleeping until the next DTIM announcement. This enables longer sleep periods for stations, which conserves energy and reduces contention.

The beacon interval T_{TIM} is announced in the DTIM beacon or during association and represents the number of IEEE 802.11 time units (TUs) of 1024 μs between two subsequent TIM beacons. The long beacon interval $T_{\text{DTIM}} = N_P N_B \cdot T_{\text{TIM}}$ is the number of TUs between two consecutive DTIM beacons. The TIM beacon for the first TIM group is broadcasted together with the DTIM beacon.

In order to reduce collisions and interference between stations, the standard introduces the RAW mechanism which could be seen as a combination of deterministic and stochastic media access control mechanisms. RAW enables reserving specific slotted time windows within a beacon interval only for specific stations assigned to the slots in the windows. During those windows, assigned stations use enhanced distributed channel access/distributed coordination function (EDCA/DCF) to access the medium within their corresponding slot (Fig. 3). RAW can be used for restricting channel access to any specified group of stations. It is useful for achieving performance improvements in dense IoT networks where a large number of stations are contending simultaneously [19].

Each RAW can be divided into equal-sized time slots referred to as RAW slots. Stations assigned to a RAW are evenly split across the RAW slots using round robin assignment. If a station belongs to an RAW, it is allowed to contend for medium access at the start of its assigned RAW slot and will not contend for medium access within any other RAW slot during that RAW. The number of slots N_{RAW}, slot format and the slot duration count C for each RAW are carried in the preceding beacon. The duration of the RAW slot T_{slot} is defined by [10]

$$T_{\text{slot}} = 500\ \mu\text{s} + C \cdot 120\ \mu\text{s}. \tag{1}$$

Although an AP can dynamically change both RAW and MCS configurations in real-time to reflect the changes in the network, it is important to note that: 1) the RAW duration must always be shorter than the beacon interval T_{TIM}, so RAW must be configured with respect to the beacon interval and 2) if cross-slot boundary (CSB) is forbidden (equals zero), the RAW slot duration must be at least as long as the packet transmission time. Hence, RAW must be configured with respect to the traffic patterns and distances in the network (i.e., packet sizes and MCSs) at all times. Otherwise, disrespecting: 1) would cause the next beacon to cut-off the latter part of RAW (that continues after the following beacon on the timeline), which would disable all the stations assigned to the cut-off slots to ever access the medium. Moreover, disrespecting 2) would disable every transmission or reception. If CSB is allowed (i.e., equals 1), a station is allowed to cross its assigned RAW slot boundary to complete the ongoing frame exchange sequence. Otherwise, a station will not transmit if the transmission would exceed the boundary of its allocated RAW slot.

IV. Control Loops Over IEEE 802.11ah: Problem Statement

Closed-loop control is typically implemented via deterministic and robust communication networks as high reliability and speed are key requirements in this type of communication. Closed-loop automation generally requires a dedicated, on site end-to-end control system with redundant communication channels to enable fail-safety. Some control is performed over the Internet but mostly at the supervisory level, for power grid distribution stations, waste-water treatment plants, etc. The infrastructure and intelligence are still localized. Nondeterminism, i.e., unpredictability in sensor reading, packet delivery or processing time, degrades performance and can lead to instability of the system. Two major issues of using wireless in control systems are communication delays and packet dropouts [20].

IEEE 802.11ah, in contrast to LPWAN technologies, provides both enough bandwidth for reliable bidirectional communication and QoS mechanisms which makes it suitable for closed-loop scenarios over a wide area. MCS8 with 2-MHz channel (7.8 Mb/s) enables a total transmission time of $T_{\text{TX}} = 1.24$ ms for 130-byte packets, including the time needed to acknowledge the transmission, whereas MCS0 (650 kb/s) can complete the transmission in $T_{\text{TX}} = 2.72$ ms.

This technology combines deterministic and stochastic medium access by using the RAW mechanism. RAWs can contribute to introducing determinism in a network, if configured accordingly. However, an arbitrary RAW configuration can also degrade network performance if RAW is not configured with respect to the traffic patterns of the end devices.

In practice, controllers are usually wired to the AP. Hence, two wireless hops are needed to complete a single cycle in a control loop in a Wi-Fi network, namely, sensor-AP and AP-actuator. Depending on the TIM and RAW setup, those two hops can be completed in a short or long time. TIM segmentation can prolong the latency by increasing the number of TIM groups, assuming a fixed T_{TIM}. Additionally, the entire RAW configuration (RAW type, number of RAW groups, and their individual configurations) greatly influences the latency. In practice, delay is present in: 1) both actuation and sensing since neither is immediate in real world; 2) processing—calculating the control value; and 3) packet delivery. The transport delay contributes to lower stability margins, therefore it must be small enough to guarantee correct operations.

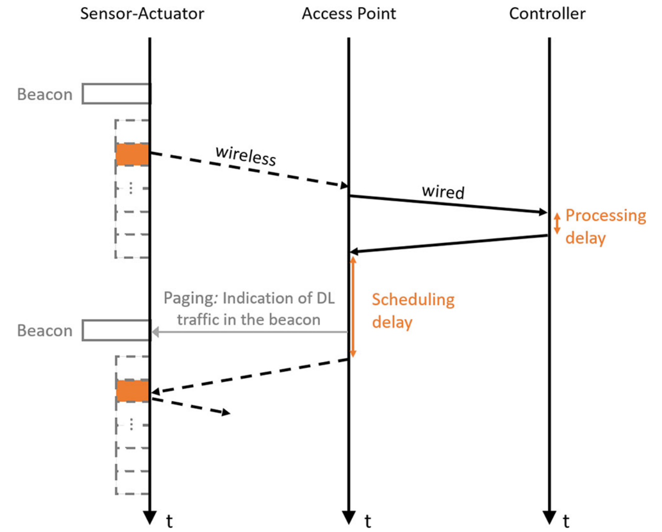

Fig. 4. Single cycle in a control loop where a sensor-actuator node is a wireless device and a controller is wired to AP cannot be completed in time less than T_{DTIM} due to the delay at the AP. Before forwarding the packet, the AP must page the 802.11ah station, i.e., inform the station that there is pending DL data waiting to be delivered through the DTIM/TIM bitmap in the beacon.

As a result, the interpacket delay (IPD) in a control loop must be smaller than its cycle-time T_{cyc}, otherwise the controlled system might get unstable. This cycle-time T_{cyc} is the time between two consecutive transmissions of measured values to the controller. Wi-Fi HaLow might be able to respond to IoT applications that imply controlling systems with cycle-time $T_{\mathrm{cyc}} > 2T_{\mathrm{DTIM}}$ for loops with a wired controller, however any faster control loop would encounter delay problems in a dense stochastic network.

Three aspects impact the design of a control loop scheduling solution with 802.11ah, as follows.

A. Contention

Different from previous IEEE 802.11 standards, each station uses two back-off states of EDCA to manage transmissions inside and outside their assigned RAW slots, respectively. At the start of an RAW slot, all stations assigned to the slot start contending for the medium. In order to prevent control loop end-nodes from backing-off and risking to miss the transmission opportunity, one RAW slot can be allocated per control loop end-node, introducing determinism to the critical stations at the cost of reducing available channel time to the noncritical stations.

B. Timing

For Generic RAW, the shortest achievable round trip time (RTT) in the ideal case is T_{DTIM} (Fig. 4). However, the cycle-time in a control loop is determined by IPD at the actuator side, not by RTT. Therefore, the shortest achievable cycle-time is T_{DTIM} only if end-points are able to reply to the received packet within the same T_{TIM}, and $2T_{\mathrm{DTIM}}$ if end-points are not able to reply to the received packet within the same T_{TIM}, but have to wait the next transmission opportunity after the next DTIM beacon. An IEEE 802.11ah network could support control loops with cycle-time T_{cyc} greater or equal to the shortest achievable IPD at the actuator side. However, T_{DTIM} can be quite long given that $T_{\mathrm{DTIM}} = n \cdot T_{\mathrm{TIM}}$ where n is the number of TIM groups in one page period and T_{TIM} is beacon interval. Increasing T_{TIM} or n increases the sleeping time of the stations and reduces energy consumption, but also increases latency as every DL packet must be indicated in the following DTIM first, and then in the corresponding TIM. Even if no segmentation was present ($n = 1$), the shortest possible IPD is greatly determined by T_{TIM}.

To support very fast control loops, T_{TIM} or n could be reduced to satisfy $T_{\mathrm{cyc}} \geq n \cdot T_{\mathrm{TIM}}$. However, even then timely delivery is not certain because generation time (Section IV-C), scheduling delay and processing delay introduce uncertainties. Moreover, processing delay can greatly influence scheduling, especially for short beacon intervals. If the AP does not get the response packet from the controller before transmitting the beacon, it cannot page the station in the beacon. Hence, the station will not know that it has pending DL data, it will not wake up in its slot (unless it has data to transmit) and the DL transmission will be delayed for an additional beacon interval. A too high UL or DL latency combined with a shorter processing delay can also lead to the same outcome.

C. Generation Time

Without loss of generality, consider a single TIM group with a beacon interval $T_{\mathrm{TIM}} = T_{\mathrm{DTIM}}$. Assuming $T_{\mathrm{cyc}} = m \cdot T_{\mathrm{TIM}}$ where $m \in \mathbb{N}$ enables scheduling the transmissions every mth beacon interval. However, given that beacon interval must be a multiple of 1024 μs and generally not all loops in the network will have cycle-times that are multiple of T_{TIM}, m can often be $m = \{p/q | p > q \wedge p \mod q \neq 0 \wedge p, q \in \mathbb{N}\}$. This means that $p \mod q$ packets out of every q packets will be delayed for the following beacon interval, whereas the rest will be scheduled every $\lfloor p/q \rfloor$th beacon interval.

V. Simulation Setup

We simulated the network in the ns-3 event-based network simulator that exhibits realistic propagation behavior (e.g., channel errors and capture effect). We used a standard log propagation loss model with values for outdoors scenarios and macro deployment [21]. We used the transmission power of 0 dBm. Transmission gain, reception gain, and noise figure were set to 0, 3, and 3 dB, respectively. As IEEE 802.11ah is an IP-based technology, we have adopted the open IETF stack for embedded devices (CoAP, UDP, and IPv4/6) to realize the control loop interactions. We analyzed the performance of control loops with IEEE 802.11ah, considering the baseline configuration shown in Table III. 130-byte packets carry a 53-byte payload, considering the overhead of all protocol headers (802.11ah, IPv4, UDP, and CoAP).

Although an IEEE 802.11ah AP can support up to 8192 connected stations, we only consider a small number of simultaneously operating stations, assuming that the AP uses some standard mechanisms to decrease the contention between the stations. The RAW configuration is fixed and does not change

TABLE III
DEFAULT PARAMETERS USED IN THE SIMULATIONS

PHY parameters	Values
Frequency [MHz]	868
TX power [dBm]	0
TX gain [dB]	0
RX gain [dB]	0
Noise Figure [dB]	6.8
Coding method	BCC
Propagation model	Outdoor, macro [21]
Error rate model	YansErrorRate
MAC parameters	**Values**
Duration of AIFS (μs)	316
Cross slot boundary	enabled
Station distribution	random
Rate control algorithm	constant
Max size of transmit queue (packets)	10
Packet size (bytes)	130
Payload size (bytes)	53
Number of monitoring sensors	50, 100
Sensors' reporting interval (s)	1
Number of control loops	1, 2, 3, 4
Control loop cycle-time T_{cyc} (ms)	32, 64, 80, 128, 160, 256, 512
Controller processing time (ms)	10, 5
Ethernet transmission delay (μs)	6.56
Ethernet data rate (Mbps)	100
Data mode (2 MHz)	MCS0, MCS8
Coverage area (m)	600, 200

in time in the use case under consideration. For latency evaluation, we configure 2 RAWs: one for monitoring sensor nodes that only report 53-byte measurements each second and do not participate in control loops, and the other with N_{CL} slots for N_{CL} sensor-actuator nodes (also referred to as control loop end-nodes) that participate in control loops. Slot duration for a control loop's RAW is set to the sum of the packet transmission time t_{TX}, short interframe space $t_{\text{SIFS}} = 160\ \mu$s, ACK transmission duration $t_{\text{ACK}} = 680\ \mu$s and a reserve of $2 \cdot 120\ \mu$s

$$T_{\text{RAW}}^{\text{CL}} = 500\ \mu\text{s} + \left\lceil \frac{t_{\text{TX}} + t_{\text{SIFS}} + t_{\text{ACK}} - 500\ \mu\text{s}}{120\ \mu\text{s}} + 2 \right\rceil \cdot 120\ \mu\text{s}. \tag{2}$$

Each control loop end-node is assigned to a dedicated RAW slot to maximize reliability and avoid contention with monitoring sensors, as well as other control loop end-nodes. Each RAW adds six bytes to the beacon, thus it is better to keep the number of RAWs on the minimum.

We vary the beacon interval from the minimal value 9216 μs for MCS0 with 2-MHz channel to the most commonly used value 102 400 μs. The minimal beacon interval is calculated as the value that can accommodate two one-slot RAW groups (one for the loop and the other for the monitoring sensors) of the shortest duration added to the maximal beacon transmission time. The shortest RAW group duration is determined as the shortest duration that can accommodate a single packet transmission for the corresponding data mode. The shortest beacon intervals for all data modes are listed in Table IV.

We conducted experiments for various control-loop cycle-times (32, 64, 80, 128, 160, 512 ms) with different beacon intervals (9216–102 400 μs) for MSC0 (over 600 m) and MCS8 (over 200 m). Each experiment was repeated ten times with different random seeds and the results in Section VI show

TABLE IV
MINIMAL BEACON INTERVAL IS DETERMINED BY THE SHORTEST DURATION OF TWO SINGLE-SLOTTED RAWS ADDED TO THE MAXIMAL BEACON TRANSMISSION TIME

Data mode (2 MHz)	Min beacon interval (μs)
MCS0	9216
MCS1	8192
MCS2, MCS3, MCS4	7168
MCS5, MCS6, MCS7, MCS8	6144

the average values of ten randomized simulations. We measured a number of metrics which include UL and DL latency, jitter, RTT, throughput, IPD at both client and server side, and energy consumption of sensor stations operating alongside control loops.

VI. PERFORMANCE EVALUATION AND DISCUSSION

The beacon interval influences the control loop dynamics in a great deal. The fastest feasible wireless control loop can only be as fast as the beaconing frequency, assuming that the controller processing time is substantially smaller than the beacon interval and that there is no contention in the sensor-actuator's RAW slot, as illustrated in Fig. 4. Otherwise, when the controller processing time has an order of magnitude of the beacon interval or the cycle-time, the jitter varies too much . In most of the available research, the beacon interval was fixed to cca. 100 ms. Given that the loop cycle-time T_{cyc} must be greater than T_{TIM} (preferably multiple times), this value is too large for control loop scenarios as not many processes change as slowly as every n hundred milliseconds. In fact, the T_{cyc} that a 802.11ah network can support in theory can be defined by the channel's capacity to accommodate all the traffic generated by loops

$$T_{\text{cyc}} \geq \frac{2(t_{\text{TX}} + t_{\text{SIFS}} + t_{\text{ACK}}) \cdot T_{\text{TIM}}}{T_{\text{RAW}}^{\text{CL}}} \tag{3}$$

where $T_{\text{RAW}}^{\text{CL}}$ is the RAW duration for a single control loop end-node [in our experiments defined by (2)].

Experiments have resulted in the least jitter when the cycle-time is about three times larger than beacon interval. This is illustrated for one setting in the boxplots in Fig. 6. Smaller beacon intervals offer better granularity and provide less jitter. As a downside, the smaller the beacon interval, the more energy is consumed and the more bandwidth is used for beaconing (Fig. 5), reducing the throughput of both monitoring sensors and loops. As shown in Fig. 6, a beacon interval of $T_{\text{TIM}} = 25.6$ ms results in only 3.1996% packets delayed for more than one beacon interval, whereas with $T_{\text{TIM}} = 102.4$ ms this is the case with 38.3503% of packets.

Significant jitter is present in IEEE 802.11ah bidirectional communication. Jitter occurs due to variable delays in various points in the loop: UL and DL latency, backoffs, processing time, possible lack of synchronization between T_{cyc} and T_{TIM}. Ideally, in wireless control loops it would be enough to reduce the beacon interval to the loop cycle-time and schedule one packet per beacon interval. This way, the loop could execute in a timely fashion assuming the controller's processing delay together with the total UL and DL latency does not exceed

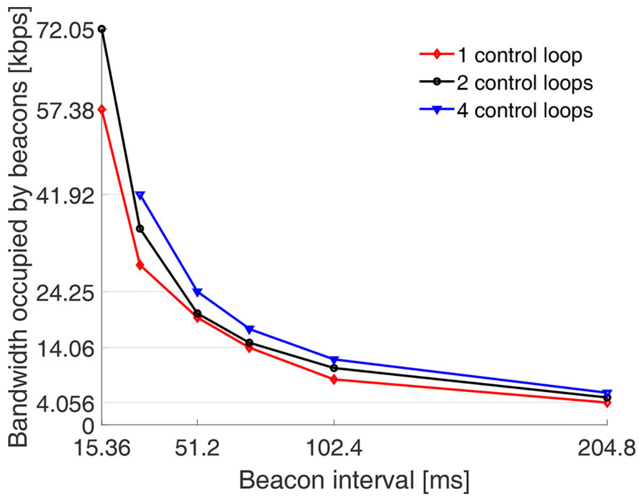

Fig. 5. Frequent beaconing uses more valuable bandwidth, reducing the throughput of useful data. The size of a beacon varies with the number of RAWs and the amount of DL traffic, i.e., the size of the TIM.

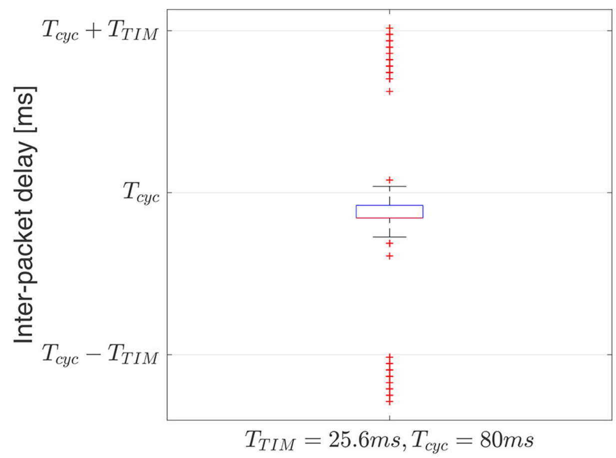

Fig. 7. Adjusting the beacon interval to the cycle-time of the fastest loop in the network $T_{\text{cyc}} = 80$ ms bounds the majority of the IPDs to the interval $(T_{\text{cyc}} - T_{\text{TIM}}, T_{\text{cyc}} + T_{\text{TIM}})$ with some minor deviation. Hence, this significantly limits the jitter. Only 0.0816% of the measured IPDs are larger than $T_{\text{cyc}} + T_{\text{TIM}}$ and 18.73% are outliers.

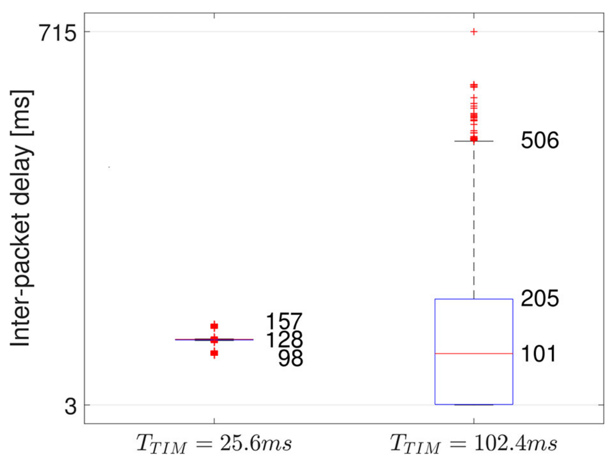

Fig. 6. Although most of the IPDs at the client side are below $T_{\text{cyc}} = 128$ ms for both measured cases, a control loop achieves much lower jitter with lower beacon interval but consumes 0.347 mW more.

T_{TIM}. However, even then, some packets cannot be delivered in the scheduled beacon intervals due to the stochastic nature of the standard and aforementioned variable delays, especially if the controller processing time is comparable to the beacon interval. Those delayed packets can then further disrupt the schedule as the sensor will continue transmitting packets on schedule and the controller will have to process and reply to those packets alongside the delayed ones, therefore introducing even more delay. Allocating an RAW per loop results in less than 1% packet loss even when $T_{\text{TIM}} = T_{\text{cyc}}$. However, we measured very high latency in this case. The more delayed packets, the more IPD diverges. As visible in the boxplot in Fig. 6 for $T_{\text{TIM}} = 102.4$ ms, more than 25% of all packets is delayed, but also 25% of all packets arrive at the actuator almost simultaneously resulting in an IPD of 3 ms. Because of the discussed nondeterminism, it is not the best practice to set the T_{TIM} in the same order of magnitude as T_{cyc}, which would work if the network was fully deterministic. It is best to leave a few beacon intervals extra to allow both endpoints in the loop to deliver their packets even if they skip the scheduled beacon interval. In other words, the loop cycle-time T_{cyc} should be at least twice the value of T_{TIM} to avoid jitter divergence.

Jitter contributes to a variable IPD, which in best case has the value of about $T_{\text{cyc}} \pm T_{\text{TIM}}$ as shown in the boxplot in Fig. 7 for $T_{\text{cyc}} = 3.125 \cdot T_{\text{TIM}}$. Adjusting the beacon interval to the fastest loop according to the rule $T_{\text{TIM}} = T_{\text{cyc}}/m$, where $m \in \mathbb{R} \wedge m > 3$, resulted in <4% IPD measurements greater than $T_{\text{cyc}} + 2T_{\text{TIM}}$ in all experiments.

Fig. 8 illustrates the behavior of loops with different cycle-times for various beacon intervals. For all experiments, the deviation of the IPD from the loop cycle-time T_{cyc} remains limited as long as: 1) the loop cycle-time T_{cyc} is at least twice as large as the beacon interval and 2) the beacon interval is at least twice as large as the controller processing time (10 ms). For all cycle-times shown in Fig. 8, the only acceptable beacon intervals are the ones for which the ordinate is zero. The IPD starts to deviate significantly as soon as the cycle-time T_{cyc} reaches $2 \cdot T_{\text{TIM}}$ in all experiments. The exception is $T_{\text{TIM}} = 9.2$ ms which is two times smaller than all simulated cycle-times, but also smaller than the controller processing time resulting in large IPD deviations. Small beacon intervals can serve well most control loops. However, small beacon intervals significantly increase the energy consumption as illustrated in Fig. 9. Fig. 9 shows the decrease of the power consumption for increasing values of the beacon interval for both MCS0 and MCS8 with 2-MHz channel.

The more loops and the more frequent loop cycles, the more bandwidth is occupied by the loops, leaving less space for sensor traffic. Given that we fixed the monitoring sensors' traffic interval to $1s$, we can evaluate how many monitoring sensors can operate without any packet loss alongside a control loop. The beacon intervals are adjusted to the control loops (the maximal beacon interval for which ordinate is zero in Fig. 8 is used) for each cycle-time, ergo power consumption of monitoring sensors decreases with the increase of cycle-time, i.e., the increase of beacon interval.

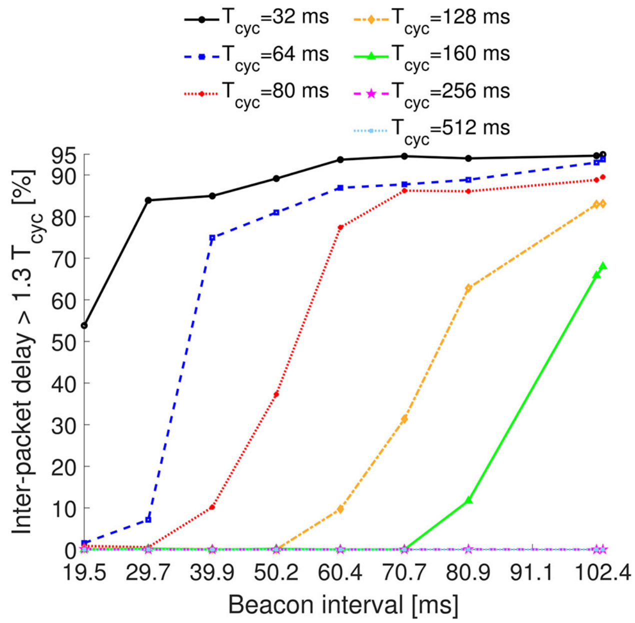

Fig. 8. When the ordinate equals zero, the jitter is limited to 30% of T_{cyc}. To limit the jitter in a control loop with a desired cycle-time T_{cyc}, one of the beacon intervals (abscissa) for which the ordinate equals zero should be used.

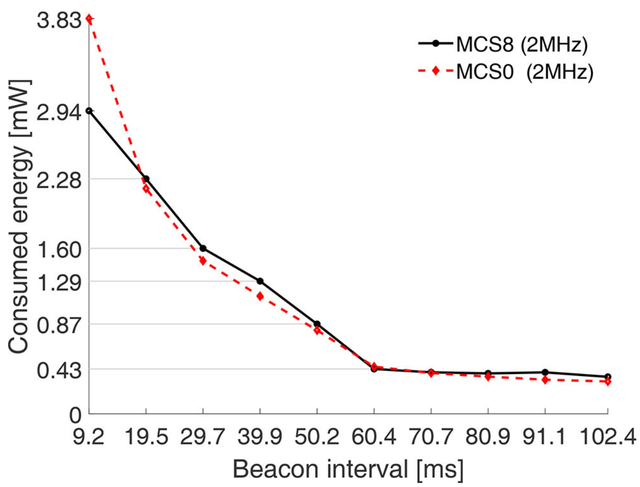

Fig. 9. Average power consumption per sensor-station that reports each second exponentially decreases with the increase of beacon interval.

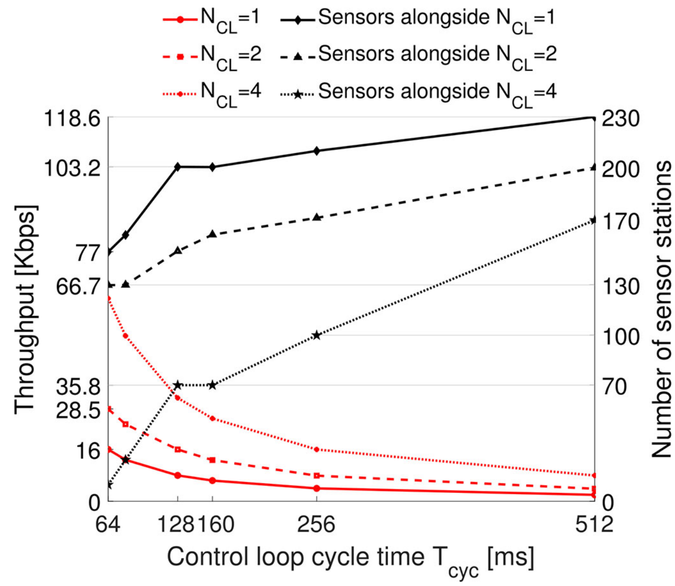

Fig. 10. Maximal achievable throughput with MCS0 that results with packet loss percentage less in order of 10^{-2}.

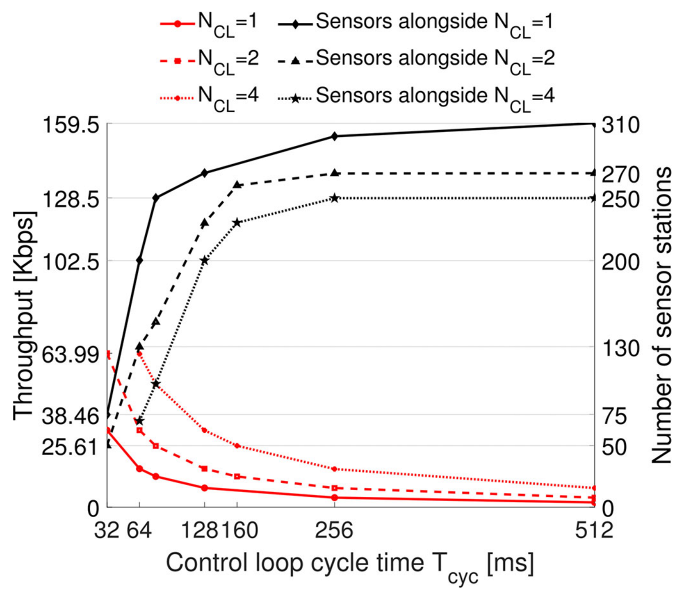

Fig. 11. Maximal achievable throughput with MCS8 that results with packet loss percentage in order of 10^{-2}.

The monitoring sensors' throughput can be calculated as $x = p_{\text{bit}} \cdot N_{\text{sensors}}/T_i$ where p_{bit} denotes the payload size in bits, N_{sensors} denotes the number of monitoring sensors and T_i denotes the traffic interval of monitoring sensors. Therefore, doubling the number of monitoring sensors while halving their reporting interval keeps the throughput at the same value. Experiments have confirmed that the network can indeed scale as described.

We evaluated the scalability of an 802.11ah network with one, two and four control loops taking into account the loop's cycle-times. We varied the number of sensor stations in increments of 10 to find the maximal monitoring sensors' density for different dynamics of the control loop for MCS0 and MCS8 using a 2-MHz channel. The maximal monitoring sensors' throughput for different dynamics of the control loop is shown in Fig. 10 for MCS0, and in Fig. 11 for MCS8. The packet loss percentage is in the order of 10^{-2} for all of the illustrated experiments. Given that we varied the number of sensor-stations in increments of 10, the error in the shown maximal throughput can be at most 5.12 kb/s. The approximate maximal number of monitoring sensors (± 5) that are able to transmit p_{bit} bits every T_i seconds with almost no packet loss can be derived from Figs. 10 and 11 as $x \cdot T_i/p_{\text{bit}}$, with x being the throughput.

VII. Practical Industrial Use Cases

The previous section has shown the feasibility of using the configuration capabilities of IEEE 802.11ah to realize low latency control loops, even in the presence of other traffic.

To put things in perspective, we consider the applicability of IEEE 802.11ah in view of two practical industrial use cases currently being solved with Wi-Fi and IEEE 802.15.4e as underlying wireless technologies. To this end, Fig. 12 compares IEEE 802.11ah's latency performance to the one of Wi-Fi (use case 1) and TSCH (use case 2) in industrial settings.

A. Industrial Wi-Fi Versus IEEE 802.1ah

The Wi-Fi use case [22] considers a large industrial stockyard surrounded by a safety fence, where a moving crane is responsible for handling goods. A programmable logic controller (PLC) is monitoring all entry points (gates) of the fence. The PLC communicates wirelessly with the crane and needs to shut down the crane immediately whenever a person enters.

Implementing this use case using Wi-Fi comes with three problems.

1) Multiple APs are needed due to the size of the stockyard, introducing delays caused by handovers.
2) Because DCF provides no control over latency in the network, the point coordination function (PCF) had to be used to control the latency. This implies that the entire channel is reserved for PCF communication (all stations must be polled frequently), thus battery-powered IoT devices cannot be supported alongside the low-latency control loops.
3) Standardized handover techniques introduce too much delay to realize low-latency control loops. To reduce handover latency to acceptable levels, proprietary extensions to the IEEE 802.11 standard were required, namely Industrial PCF (iPCF) and iPCF with Management Channel (iPCF-MC), aiming to improve and guarantee fast handover for industrial communication.

Fig. 12(a) shows that both technologies can realize 64 ms control loops, but IEEE 802.11ah mitigates the three above issues given that: 1) it avoids the handovers due to its coverage with a single AP; 2) it can support battery-powered IoT stations alongside low-latency control-loops; and 3) it is not proprietary, and thus the solution is not vendor-dependent.

B. IEEE 802.15.4e Versus IEEE 802.1ah

The second use case [23] considers IEEE 802.15.4e, also known as time-slotted channel hopping (TSCH). In this use case, a small-scale Wireless Sensor and Actuator testbed was replicated using the OpenMote-cc2538 motes in an indoor environment in a binary tree topology of depth 3. The topology consists of one backbone router (root), four monitoring nodes which can generate periodical noncritical data, a source (alarm) and a destination (actuator) mote that exchange critical application data. The source and the destination node are located on the opposite branches of the tree. The source and destination nodes have a depth of 3 and 1, respectively. 10 ms time slots with a slotframe length of 21 including 2 shared and 4 serial slots are used. The critical application generates 1 packet/s, whereas dedicated monitoring nodes send 1 packet/s to a destination in the backbone network. As Fig. 12(b) illustrates, end-to-end latency of the critical traffic rarely deviates more than 1 slotframe duration when there is no monitoring traffic, otherwise it deviates significantly more. Nevertheless, with or without monitoring traffic, long end-to-end delays make this technology generally unusable for low-latency (order of 64 ms) critical applications because of its multihop topology and long slotframes.

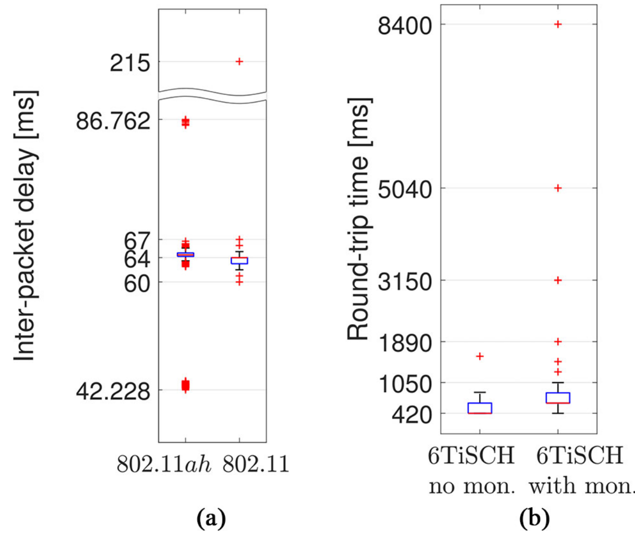

Fig. 12. Comparison of 802.11 Wi-Fi, IEEE 802.15.4e, and 802.11ah for the realization of sub-100-ms feedback loops over wide areas. (a) Use case 1: low-latency feedback loop with a crane with $T_{\text{cyc}} = 64$ ms: 802.11ah versus 802.11 Wi-Fi. Sub-100 ms feedback loops are feasible with both technologies. However, 802.11 Wi-Fi needs multiple APs in large areas where handovers introduce substantial delays. (b) Use case 2: 6TiSCH feedback loop with and without additional noncritical traffic using slotframe of 21 10-ms slots. Multihop TSCH is not suitable for sub-100-ms feedback loops over wide areas.

Both representative industrial use cases illustrate that IEEE 802.11ah can definitely bring benefits in the realization of low latency wireless control loops and can claim its role in the wireless solution landscape.

VIII. Conclusion

IEEE 802.11ah has proven to be a versatile solution for heterogeneous industrial environments. Experiments have shown that IEEE 802.11ah can meet reliability and low-latency demands up to a certain extent, allowing low-latency control loops and monitoring-stations to reliably operate side by side. The best case scenario (MCS8) resulted in 310 sensor stations transmitting 64-byte CoAP packets each second alongside a control loop with $T_{\text{cyc}} = 512$ ms. 75 monitoring sensors are feasible with a single control loop with $T_{\text{cyc}} = 32$ ms. Packet loss is 0.0208% for 3 control loops with $T_{\text{cyc}} = 32$ ms. Four control loops with $T_{\text{cyc}} = 64$ ms can reliably operate alongside 70 monitoring sensors. These results are achievable by reducing the beacon interval as illustrated in Fig. 8 to limit the latency and jitter. Allowing two or more transmission opportunities within a cycle-time provides enough robustness for at least 99.99% successful packets. Even though reducing the beacon interval enables the realization of control loops, it introduces major setbacks: increasing the energy consumption of monitoring sensors and reducing the overall throughput. In the future, we plan to alleviate the issues of frequent beaconing by enabling the critical stations to obtain access to the medium more than once within a beacon interval, while sensor stations continue operating in a standard fashion. Finally, although IEEE 802.11ah is often exempt from consideration for industrial applications, it shows promise both performance- and cost-wise for mid-range mid-latency wireless communication.

REFERENCES

[1] M. Pajic and R. Mangharam, "Embedded virtual machine for robust wireless control and actuation," in *Proc. 16th IEEE Real Time Embedded Technol. Appl. Symp. (RTAS)*, Apr. 2010, pp. 79–88.

[2] M. Pajic, S. Sundaram, G. J. Pappas, and R. Mangharam, "The wireless control network: A new approach for control over networks," *IEEE Trans. Autom. Control*, vol. 56, no. 10, pp. 2305–2318, Oct. 2011.

[3] V. K. L. Huang, Z. Pang, C.-J. A. Chen, and K. F. Tsang, "New trends in the practical deployment of industrial wireless: From noncritical to critical use cases," *IEEE Ind. Electron. Mag.*, vol. 12, no. 2, pp. 50–58, Jun. 2018.

[4] Z. Pang, M. Luvisotto, and D. Dzung, "Wireless high-performance communications: The challenges and opportunities of a new target," *IEEE Ind. Electron. Mag.*, vol. 11, no. 3, pp. 20–25, Sep. 2017.

[5] M. Weiner, M. Jorgovanovic, A. Sahai, and B. Nikolié, "Design of a low-latency, high-reliability wireless communication system for control applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 3829–3835.

[6] Y.-H. Wei *et al.*, "RT-WiFi: Real-time high-speed communication protocol for wireless control systems," *ACM SIGBED Rev.*, vol. 10, no. 2, p. 28, 2013.

[7] *Industrial Networks: Wireless Communication Network and Communication Profiles*, document IEC PAS 62948, IEC, Geneva, Switzerland, 2015.

[8] A. Frotzscher *et al.*, "Requirements and current solutions of wireless communication in industrial automation," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 67–72.

[9] A. Varghese and D. Tandur, "Wireless requirements and challenges in industry 4.0," in *Proc. Int. Conf. Contemp. Comput. Informat. (IC3I)*, Nov. 2014, pp. 634–638.

[10] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation*, IEEE Standard 802.11ah-2016, pp. 1–594, May 2017.

[11] A. Šljivo *et al.*, "Performance evaluation of IEEE 802.11ah networks with high-throughput bidirectional traffic," *Sensors*, vol. 18, no. 2, p. 325, Jan. 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/2/325

[12] L. Tian, A. Šljivo, S. Santi, E. De Poorter, J. Hoebeke, and J. Famaey, "Extension of the IEEE 802.11ah NS-3 simulation module," in *Proc. Workshop NS-3 (WNS3)*, Jun. 2018, pp. 53–60.

[13] A. Bel, T. Adame, and B. Bellalta, "An energy consumption model for IEEE 802.11 ah WLANs," *Ad Hoc Netw.*, vol. 72, pp. 14–26, Apr. 2018.

[14] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11ah: The WiFi approach for M2M communications," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 144–152, Dec. 2014.

[15] A. Kureev, D. Bankov, E. Khorov, and A. Lyakhov, "Improving efficiency of heterogeneous Wi-Fi networks with joint usage of TIM segmentation and restricted access window," in *Proc. Int. Symp. Pers. Indoor Mobile Radio Commun. (IEEE PIMRC)*, 2017, pp. 1–5.

[16] T. Kim and J. M. Chang, "Enhanced power saving mechanism for large-scale 802.11ah wireless sensor networks," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 4, pp. 516–527, Dec. 2017.

[17] B. Badihi, L. F. Del Carpio, P. Amin, A. Larmo, M. Lopez, and D. Denteneer, "Performance evaluation of IEEE 802.11ah actuators," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, 2016, pp. 1–5.

[18] N. Ahmed, D. De, and M. I. Hussain, "A QoS-aware MAC protocol for IEEE 802.11 ah-based Internet of Things," in *Proc. 15th Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, 2018, pp. 1–5.

[19] L. Tian, J. Famaey, and S. Latré, "Evaluation of the IEEE 802.11ah restricted access window mechanism for dense IoT networks," in *Proc. IEEE 17th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, 2016, pp. 1–9.

[20] P. G. Park, S. C. Ergen, C. Fischione, C. Lu, and K. H. Johansson, "Wireless network design for control systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 978–1013, 2nd Quart., 2018.

[21] A. Hazmi, J. Rinne, and M. Valkama, "Feasibility study of IEEE 802.11ah radio technology for IoT and M2M use cases," in *Proc. IEEE Globecom Workshops*, Anaheim, CA, USA, 2012, pp. 1687–1692.

[22] J. Haxhibeqiri *et al.*, "Wireless handover performance in industrial environments: A case study," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Berlin, Germany, 2016, pp. 1–4.

[23] A. Karaagac, I. Moerman, and J. Hoebeke, "Hybrid schedule management in 6TiSCH networks: The coexistence of determinism and flexibility," *IEEE Access*, vol. 6, pp. 33941–33952, 2018.

Amina Seferagić received the M.Sc. degree in electrical engineering from the University of Sarajevo, Sarajevo, Bosnia and Herzegovina, in 2016. She is currently pursuing the Ph.D. degree at the Internet and Data Lab, a core research group of imec embedded in Ghent University, Ghent, Belgium.

She has authored or coauthored seven publications in international journals or conference proceedings.

Ms. Seferagić was a recipient of two Golden Badge Awards from the University of Sarajevo and a Best Paper Award at WNS3 2018.

Ingrid Moerman received the degree in electrical engineering and the Ph.D. degree from Ghent University, Ghent, Belgium, in 1987 and 1992, respectively.

She became a part-time Professor with Ghent University in 2000, where she is coordinating the research activities on mobile and wireless networking and leading a research team of about 30 members. She has authored or coauthored over 870 publications in international journals or conference proceedings.

Dr. Moerman was a recipient of 14 awards and prizes during her career.

Eli De Poorter received the master's and Ph.D. degrees in computer science from Ghent University, Ghent, Belgium, in 2006 and 2011, respectively.

He is a Professor with Ghent University. Since 2015, he has been a Professor with the Internet and Data Lab Research Group and imec, where he coordinates multiple national and international projects. He has authored or coauthored over 140 papers published in international journals or in the proceedings of international conferences.

Jeroen Hoebeke received the master's and Ph.D. degrees in computer science from the University of Ghent, Ghent, Belgium, in 2002 and 2007, respectively.

Since 2014, he has been an Assistant Professor with Internet and Data Lab, Ghent University—imec, where he is leading research on mobile and wireless networks, Internet of Things communication solutions, and embedded communication stacks. He has coordinated and been engaged in several national and EU funded projects. He has authored or coauthored over 150 publications in international journals or conference proceedings.