ACCEPTED FROM OPEN CALL

WiFi HaLow for Long-Range and Low-Power Internet of Things: System on Chip Development and Performance Evaluation

Il-Gu Lee, Duk Bai Kim, Jeongki Choi, Hyungu Park, Sok-Kyu Lee, Juphil Cho, and Heejung Yu

Abstract

For Internet of Things (IoT) applications in the sub-1 GHz unlicensed band, the IEEE 802.11ah technology, also called WiFi HaLow, has been standardized. To achieve long-range and low-power features of IoT networks, the physical (PHY) and medium access control (MAC) layer functions in the previous WiFi standards are amended in the IEEE 802.11ah standard. In this article, the PHY and MAC technologies in IEEE 802.11ah are investigated, and the technical features are described by comparing it with other IoT systems. Additionally, a system on chip, which integrates a digital baseband, RF transceiver, analog-to-digital converter/digital-to-analog converter, processor, and memory with the external connection interface, is implemented. To verify the feasibility of long-range and low-power WiFi for IoT services, field tests in both indoor and outdoor environments are conducted. The power-save mode operation and power consumption are presented. Through various field tests and measured data, the feasibility of WiFi HaLow is verified as a long-range, high-throughput, and low-power IoT solution.

Introduction

Recently, Internet of Things (IoT) technologies have become essential in various applications and have driven new value creation and innovative changes. IoT network technologies connect people with each other, people with things, and things with each other, and enable them to interact [1]. The emerging IoT applications have increased the demand for high-quality multimedia transmission. They require high-throughput and long-range data transmission as well as low power consumption and high efficiency. Existing narrowband sensor network solutions cannot overcome the limitations on data rate, quality of service (QoS), and energy efficiency [2]. For the existing wireless local area network (WLAN) and wireless personal area network (WPAN) technologies, such as WiFi and Bluetooth, additional efforts are required to run various IoT applications due to their limited communication ranges. Therefore, a new broadband IoT networking technology is required to meet various requirements of IoT applications, including high throughput, wide coverage, and energy efficiency [3].

In the future, long-range, low-power IoT technologies are also expected to be widely used in broadband IoT services in smart factories, smart grids, and smart cities for various functions, such as remote metering of gas, electricity, and water, remote weather and disaster monitoring, environmental observation, and remote management of security, healthcare, welfare, transportation, and logistics [4]. These changes will lead to an increasing number of low-power, low-cost IoT devices and services that require wider service coverage and higher data rates in all industries [5]. Recently, the WLAN ecosystem has expanded due to the increased use of smartphones and smart home appliances, which have become indispensable in daily life. Through IEEE international standardization, these developments have resulted in a high degree of technical perfection, providing potential advantages to and candidates for IoT connectivity technology [6].

IEEE 802.11ah is an IoT connectivity technology that enables low-power, high-data-rate communications using the license-exempt band of sub-1 GHz [7]. The channel characteristics of sub-1 GHz, such as long-distance propagation and excellent transmittance and diffraction rates for obstacles, can enable IEEE 802.11ah to substantially increase the number of supporting stations per access point (AP) to more than 8000 with a coverage of 1 km or more. These characteristics are advantageous to infrastructure construction costs [8]. Accordingly, IEEE 802.11ah has been standardized for IoT use cases, which demand low-cost, low-power, and long-range communications.

The contribution of this article is summarized as follows:

- A system on chip (SoC) to be fully compliant with the IEEE 802.11ah standard is implemented. To the best of the authors' knowledge, this chipset is the world's first full SoC that includes a digital baseband and analog/radio frequency (RF) transceiver.
- The feasibility of the IEEE 802.11ah technology is verified by performing extensive field tests in indoor and outdoor environments. The test results show that the IEEE 802.11ah technology can provide high throughput even in outdoor long-distance communication.
- A power saving mechanism for IEEE 802.11ah is introduced for energy-efficient operation in IoT applications. Based on the

The PHY and MAC technologies in IEEE 802.11ah are investigated, and the technical features are described by comparing it with other IoT systems. Additionally, a system on chip, which integrates a digital baseband, RF transceiver, analog-to-digital converter/digital-to-analog converter, processor, and memory with the external connection interface, is implemented.

Il-Gu Lee is with, Sungshin University; Duk Bai Kim, Jeongki Choi, Hyungu Park, and Sok-Kyu Lee are with Newracom Inc.; Juphil Cho is with Kunsan National University; Heejung Yu (corresponding author) is with Korea University (Sejong).

Digital Object Identifier: 10.1109/MCOM.001.2000815

0163-6804/21/$25.00 © 2021 IEEE

The IEEE 802.11ah technology, which supports higher data rates compared with other communication technologies (Bluetooth, Zigbee, Sigfox, LoRa, and so on), is garnering attention as an IoT connectivity technology for high-capacity data transmission in low-power, low-cost broadband sensor network applications.

measured power consumption, we estimated the battery lifetime in different operation modes. It is shown that IEEE 802.11ah can achieve high energy efficiency which is enough for IoT applications.

The rest of this article is organized as follows. The following section summarizes IEEE 802.11ah. We then present the design and implementation. Following that, the test results and open issues are discussed. Finally, our conclusion is drawn in the final section.

IEEE 802.11AH System Overview

System Overview

For physical (PHY) layer transmission technology, IEEE 802.11ah, also referred to as *WiFi HaLow*, employs multiple-input multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM), which is suitable for ultra-high data rates and supports multiple bandwidths and streams to increase the data rate up to 347 Mb/s depending on the application. Furthermore, IEEE 802.11ah can provide wide-area WLAN services based on its propagation characteristics, which can extend the service coverage of the frequency band below 1 GHz [9]. Additionally, the coverage can be further extended using narrow bandwidth transmission modes and coding gain through the symbol repetition method. To improve transmission and energy efficiency, system specifications for the medium access control (MAC) layer have been designed to provide efficient packet structure, beacon signal, and protocol for IoT applications that demand long-range and low-power communications in wide area networks [10]. This structurally optimized energy-efficient specification has attracted attention as an alternative to Bluetooth. The IEEE 802.11ah standard specifies the minimum performance requirements for service coverage extending up to 1 km and for data rates of 100 kb/s or more. Thus, extended service coverage of up to 1–2 km can be supported compared to existing WLAN technologies, which have much lower coverage, and the network capacity can accommodate more than 8000 devices. Moreover, power-saving features potentially increase battery life up to 5–10 years. This enables IEEE 802.11ah to be used in applications such as smart grids, sensor networks, and machine-to-machine (M2M) communications that require low-power operations, as well as in applications that require high-speed data transmission over long distances, including cellular offloading and wide-area WLAN services.

Main Features of the PHY Layer

The PHY layer design of the 2, 4, 8, and 16 MHz bandwidth modes of IEEE 802.11ah are the 1/10 down-clocked versions of the 20, 40, 80, and 160 MHz modes of the IEEE 802.11ac standard. By decreasing the clock frequency, the overall operating frequency is lowered and the time interval is scaled up without any change in the system parameters. For example, the IEEE 802.11ah 2 MHz and IEEE 802.11ac 20 MHz bandwidth modes both have 64 subcarriers, of which 52 are data subcarriers and 4 are pilot subcarriers. Thus, the subcarrier spacing of IEEE 802.11ah is reduced to 1/10 of that of IEEE 802.11ac. In addition to these basic modes, IEEE 802.11ah introduces a 1 MHz bandwidth mode to enhance frequency utilization and extend service coverage. In this mode, a modulation method is added that repeats the symbol twice and transmits it to achieve a 3 dB gain. Consequently, when comparing the minimum data rate modes of IEEE 802.11ah and IEEE 802.11g operating at the same transmit power in the 2.4 GHz industrial, scientific, and medical (ISM) band, we can obtain a 24.5 dB link budget gain. In the total link budget gain, the sub-1 GHz link budget gain is 18.5 dB (free space path loss gain of 8.5 dB + noise bandwidth gain of 10 dB), and the 1 MHz bandwidth mode gain is 6 dB (1/2 bandwidth gain of 3 dB + 2 × repetition coding gain of 3 dB) [11]. In IEEE 802.11ah-based short-range communication applications that utilize its advantages in terms of link budget, even if the transmit power is 0 dBm or lower, a wider service coverage than in conventional WLAN technologies can be ensured while enabling low-power operations. For this reason, the IEEE 802.11ah technology, which supports higher data rates compared to other communication technologies (Bluetooth, Zigbee, Sigfox, LoRa, etc.), is garnering attention as an IoT connectivity technology for high-capacity data transmission in low-power, low-cost broadband sensor network applications.

Main Features of the MAC Layer

As IEEE 802.11ah can accommodate thousands of stations in a wide band, enhanced distributed channel access (EDCA)-based channel access methods increase the possibility of degrading performance and energy efficiency because of the channel access contention between hidden nodes and peripheral devices. To alleviate this problem, the following technologies were designed for the IEEE 802.11ah MAC protocol to accommodate a large number of stations in a broadband network and to increase energy efficiency.

Restricted Access Window (RAW): The RAW allocates a RAW slot (i.e., a designated channel access interval) to each station and restricts the station's channel access to this slot. This divides the collision domain, thereby reducing the collision probability among stations [12]. In addition, the AP transmits a synchronization frame to the station in the RAW slot and can improve battery life.

Target Wake Time (TWT): The TWT allows the AP to immediately transmit data stored in a buffer without latency when a station awakes from sleep mode [13]. To accommodate a large number of stations, the traffic information of the traffic indication map (TIM) is hierarchically structured. This allows stations to use their traffic information structured in the TIM based on the association ID assigned to them during the association process. Thus, the scheduled access method improves latency and throughput and increases battery life by reducing unnecessary collisions. Energy efficiency can also be improved through a power-saving technique that lengthens sleep mode and awakens the station.

Efficient MAC Frame: As IEEE 802.11ah has a relatively low throughput compared to conventional WiFi standards, the transmission efficiency is reduced when using the same MAC frame structure in existing WiFi standards. This is because the bandwidth is reduced to 1/10; thus, the time required to transmit the same amount of data using

Category	BLE	Zigbee	HaLow
Worldwide de facto standard	Bluetooth SIG	IEEE 802.15	IEEE 802.11ah
Frequency	2.4 GHz	2.4 GHz, sub-1 GHz	Sub-1 GHz
Data rate	1 Mb/s, 270 kb/s	250 kb/s	15 Mb/s
Service coverage	< 50 m	< 100 m	< 1.5 km
Modulation	GFSK	BPSK, OQPSK	OFDM
Access mechanism	Frequency hopping	Listen before talk	Listen before talk
Main topology	Star	Mesh	Star/relay
Power consumption [14]	17,280 mJ/MB (TX power 21.6 mW for 1 Mb/s to transmit a 100-byte data frame)	57,600 mJ/MB (TX power 18 mW for 0.25 Mb/s rate to transmit a 100-byte data frame)	14,400 mJ/MB (TX power 54 mW for 3 Mb/s rate to transmit a 100-byte data frame)
Benefits of HaLow compared to its alternative	• Better range • Higher throughput • IP networking scalability (number of stations per AP) • Wi-Fi security: Wi-Fi protected access (WPA) and Wi-Fi protected setup (WPS)) • Better power consumption	• Higher throughput • IP networking • WFA certified multi-vendor interoperability • Better range, low-latency single-hop whole home coverage • Wi-Fi security (WPA and WPS) • Better power consumption	

TABLE 1. Comparison of HaLow and alternatives.

the same modulation and coding scheme (MCS) becomes 10 times longer. Accordingly, the MAC frame-shortening technology has been introduced.

Comparison with Other IoT Systems

Table 1 shows a comparison between IEEE 802.11ah HaLow and alternative systems in terms of various aspects. The Bluetooth Low Energy (BLE) and Zigbee systems have limitations such as short radio reach, low data rates, and high power consumption. Even though several solutions are available in the IoT market, no one technology has dominated because of the diversity and complexity of wireless sensor network applications and user requirements [14].

WiFi technology has established a strong connected ecosystem, which is essential for smart device wireless interfaces, and it is used both in daily life and in numerous industries. WiFi technology is emerging as a strong candidate for IoT applications. Because it supports high data rates in fixed or low-speed mobile environments, it allows channels to be efficiently utilized through the media access contention of distributed nodes in unlicensed bands. This distributed channel access method also has the advantages of network scalability, maintenance and repair convenience, and price competitiveness, and it is widely used in homes, businesses, and hotspots. Accordingly, its application range is increasing [15].

The traditional WiFi technologies, such as IEEE 802.11a/b/g/n/ac, have been widely used in mobile devices and consumer electronics until recently, providing high-speed data communication services to terminals within tens of meters. Because the transmission distance is very limited, it is difficult to use these technologies for low-power, low-cost, and broadband IoT networks. For example, IEEE 802.11b/g/n operating at 2.4 GHz provides high-throughput services, especially in a home environment. However, it can accommodate only a few clients with large power consumption in a relatively small area.

Implementation

System Architecture Design

The chip is implemented in a 40 nm complementary metal oxide semiconductor (CMOS) process. Figure 1 shows the chip-level fabrication layout of the chip's implementation. The IEEE 802.11ah SoC implemented in this study is a single chip that integrates a digital baseband, wireless RF transceiver, analog-to-digital converter (ADC)/digital-to-analog converter (DAC), processor, power management unit (PMU), and memory with the external connection interfaces. It is fully compliant with the IEEE 802.11ah specifications, and it is prepared in accordance with the upcoming WiFi Alliance (WFA) extended range ah (ERah) certification. This chip provides data rates from 150 kb/s to 15 Mb/s using 1, 2, and 4 MHz channel bandwidths, and supports a range of uses from low-power sensors, such as low-speed sensors, to high-performance applications, such as high-speed and high-definition surveillance cameras. An ARM processor is embedded in the chip to provide high processing performance. It has a dual-core structure comprising a Cortex-M0-based communication processor and a Cortex-M3-based application processor. To accommodate various IoT applications, various peripheral device interfaces are supported. The device also offers enough memory to selectively support AP and station functions.

The RF transceiver is integrated with support for pre-power amplifiers, fractional-*N* synthesizers, and various commercially available external front-end module (FEM) devices, and has a design optimized for the sub-1 GHz band. The receiver includes an internal digital gain control stage that provides a low noise figure of 4 dB and a wide dynamic range of at least 100 dB, which supports 10 dB lower receiver sensitivity and 20 dB higher maximum input power level compared to standard requirements. The transmitter provides a gain control range of at least 30 dB and a maximum transmit power of 0 dBm.

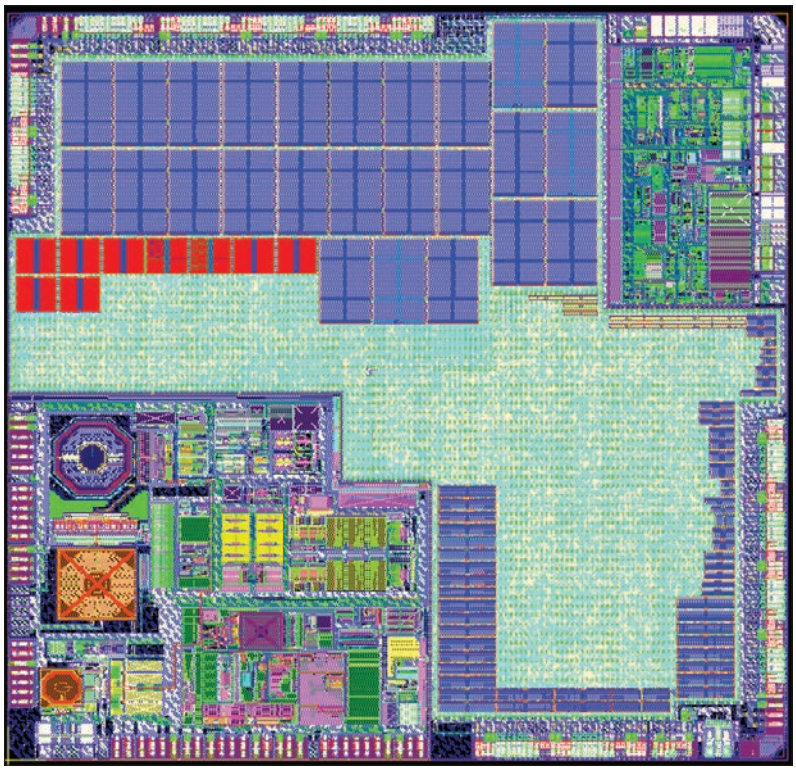

FIGURE 1. Fabrication layout of the implemented IEEE 802.11ah SoC.

Digital Baseband and Transceiver Design

The implemented IEEE 802.11ah chipset supports binary phase shift keying (BPSK), quadrature PSK (QPSK), 16-quadrature amplitude modulation (16-QAM), and 64-QAM modulation schemes in a single stream mode and provides a data rate of up to 15 Mb/s. It supports short guard intervals (up to 4 μs) and 1, 2, and 4 MHz channel bandwidths in both short and long frame formats in the specified standard. A dual-mode single chip was implemented that selectively supports AP and station modes.

To improve the efficiency of broadband IoT networks, RAW avoidance, TWT, and differentiated EDCA parameters were implemented. Furthermore, non-TIM operations, dynamic association ID (AID) assignment, and TWT were implemented to improve power consumption efficiency. A relay operation mode is also supported to extend service coverage. To expand the number of stations that can be accommodated in a single basic service set (BSS), the multicast AID authentication control standard is followed. Energy limited (EL) operations are sent and received at specific times, enabling low-cost, low-power IoT applications.

The RF transceiver is designed with a direct conversion transceiver architecture and includes both the pre-power amplifier and the entire radio front-end circuit, including the low noise amplifier (LNA) and low dropout (LDO). Radio calibration interfaces, that is, transmit signal strength indicator (TSSI), transmit local oscillator feed through (LOFT), transmission and receiving IQ imbalance, low pass filter, phase locked loop, BIAS current, and sigma-delta ADC, are provided in the digital baseband.

In the digital baseband, after the training signal is transmitted to the transceiver, the signal input is analyzed through the feedback loop, and the calibration parameter is optimized. In the frequency bands from 750 to 950 MHz, the 1, 2, and 4 MHz channel bandwidths are supported. The receiver (RX) noise figure is less than 4 dB, and the RX gain range is at least 100 dB. The RX input intercept point 3 (IIP3) is −17 dBm at the LNA maximum gain. In the transmitter (TX) pre-amplifier, the maximum linear output power is 0 dBm, and the TX gain range is 30 dB. A 10-bit ADC/DAC is used, and a −34 dB error vector magnitude (EVM) at 0 dBm transmit power with 64-QAM modulation is ensured. The integrated RF phase locked loop (PLL) phase error is less than 0.7°.

The RF/analog transceiver operated in the 750 to 950 MHz frequency range, included a fully integrated preamplifier, and supported a 30 dB TX gain control range with linear TX output power up to 0 dBm. It also included an external amplifier, supporting transmission power up to 23 dBm. The RX had an input range of 105 dB from 5 to 110 dBm.

Challenges in SoC Design

In the SoC design, the most challenging aspect is to minimize the power consumption with small chip size. To support long-range and high-throughput applications, the SoC includes two CPU cores and enough internal memory. Because the other IoT technologies support low data rate (e.g., less than 1 Mb/s) with narrow bandwidth, CPU and memory requirements can be minimized. However, IEEE 802.11ah supports data rates from 150 kb/s to 15 Mb/s, and then it requires higher computing power and more memory to accommodate various applications. Due to such stringent requirements, the size of the implemented SoC is 3.32 × 3.51 mm, which makes it larger than other IoT chips but small enough to be accommodated into IoT devices. The developed chip can support both AP and station mode, so the size can be reduced more if implemented only for station. The power consumption of the SoC is minimized with low-power design and a power saving mechanism. The receiver consumes 30 mA at 3.3 V, and the transmitter consumes 32 mA at 3.3 V for 0 dBm transmit power. Receiver sensitivity improvement and calibration features for RF impairments are also important in market competition. Moreover, the temperature sensor and battery voltage monitor circuit provide an interface to optimize performance according to the process, voltage, and temperature variations of the chip.

Performance Evaluation and Field Tests

Receiver Sensitivity

Receiver sensitivity was measured when the signal was generated by the vector signal generator (VSG) in a shielded room using the implemented WiFi HaLow chip. The VSG and the chip receiver port were connected via a cable whose loss was considered in the measurements. For all channel bandwidths and MCS modes supported by the chip, we measured the received signal strength, which guaranteed a packet error rate (PER) of 10 percent when transmitting 10,000 packets at a packet length of 256 bytes. According to the experimental results, the receiver sensitivity was −109 dBm in the 1 MHz bandwidth MCS10 at the lowest data rate of 150 kb/s. At the 4 MHz bandwidth MCS7 with a data rate of 13.5 Mb/s (64-QAM, 5/6 code rate), the receiver sensitivity was −81 dBm.

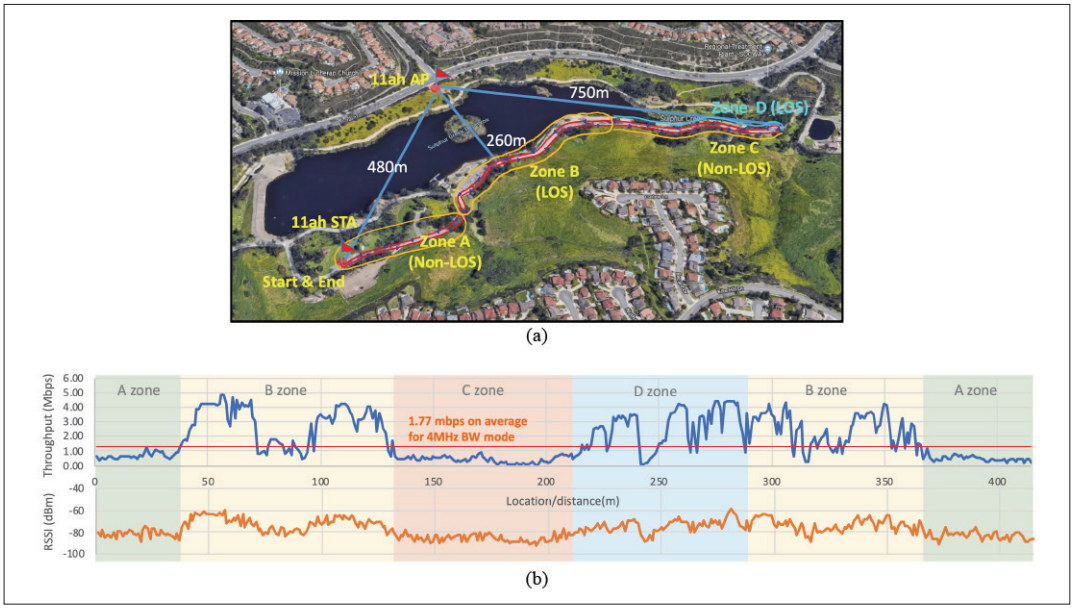

FIGURE 2. Average throughput evaluation in outdoor environments: a) experiment setup, channel condition; b) throughput and received signal strength indicator (RSSI) along the test route in a 4 MHz bandwidth mode.

Receiver sensitivity improvement and calibration features for RF impairments are also important in market competition. Moreover, the temperature sensor and battery voltage monitor circuit provide an interface to optimize performance according to the process, voltage, and temperature variations of the chip.

Outdoor Throughput

The throughputs of a single-MAC protocol data unit (MPDU) and aggregated-MPDU (A-MPDU) were measured, and they were compared in the outdoor point-to-point environment. An AP and a station were installed at a 3 m height from the ground, and packets were delivered from the AP to the station in full load condition. The transmit power measured for both devices was 16 dBm, and the antenna gain was 2 ± 1 dBi. Tests were performed by varying the distance between the two communication devices under line of sight (LoS) conditions from 0.5 to 1.5 km. As an example, the performance of the A-MPDU mode with 4 MHz bandwidth was 4.48 Mb/s at 0.5 km and 2.12 Mb/s at 1.5 km. For the single-MPDU mode with 4 MHz bandwidth, the measured throughput was 3.62 Mb/s at 0.5 km and 1.13 Mb/s at 1.5 km. These results indicate that transmission as an A-MPDU showed up to 1.87 times better throughput than that of the single MPDU.

Figure 2a shows a map with four different zones where the mobility test was performed. The four zones were classified by distance from the AP and the differences in the regional propagation environment. In this test, the AP was installed on a hill 10 m above the ground, and the station was placed on the front dashboard in a sport utility vehicle (SUV) moving along the four zones at 10 mph speed. Figure 2b shows the received signal strength indicator (RSSI) and throughput measurements in a 4 MHz bandwidth mode. Zone A represents the non-LoS condition, where the LoS was blocked by a hill between Zone A and the AP. The signal at Zone A was measured at a distance of 380–480 m from the AP. Zone B represents the LoS condition at 260–360 m from the AP. The signals at Zone C and D were measured at a distance of 360–750 m from the AP with the non-LoS and LoS conditions, respectively, depending on the movement path. When the signal was measured at Zone C, the SUV traveled away from the AP, and the SUV's body consequently blocked the LoS from the dashboard to the AP. The signal at Zone D was measured along the same path as that of Zone C, but the SUV traveled toward the AP, and therefore an LoS condition was established for Zone D. The User Datagram Protocol (UDP) throughput was measured while the station moved at 10 mph. The average throughputs over four different zones were measured as 0.9, 1.4, and 1.77 Mb/s in the 1, 2, and 4 MHz bandwidth modes, respectively. With such field tests, it can be shown that IEEE 802.11ah can be a promising solution for high-throughput IoT networks that cannot be realized with the other IoT technologies.

Indoor Throughput

The experiments for multi-station uplink performance evaluation were carried out in an indoor laboratory (21 m × 24 m) where multiple rooms were separated by partition walls, as shown in Fig. 3. In this laboratory, 10 stations were randomly placed, and an AP was installed in the room in the upper left corner. This study compared the performance of the stations at an instance when only one of 10 stations transmitted to the AP with the one when all 10 stations simultaneously transmitted. During the test, every station sent packets under its peak load condition. The peak load condition in a network throughput measurement tool was set to 5 Mb/s UDP packets, which mostly yielded a packet size of 1500 bytes. An adaptive modulation and coding function was enabled, and the channel bandwidth was set to 2 MHz. In the single-station case, the station (#8) achieved a throughput of 2.6 Mb/s. This is used as a reference for the performance of the simultaneous transmission case in the multi-station environment. When all stations transmitted their own packets simultaneously, 10 stations successfully sent throughputs of 328.6, 275.3, 274.0, 245.0, 251.3, 246.0, 240.3, 237.3, 243.3, and 301.6 kb/s, respectively, on average. The aggregated throughput of 10 stations is equal to 2.643 Mb/s, which were obtained with multiple measurements.

Mode	Wakeup interval	Pre-active		Active		Deep sleep		Power consumption	Battery lifetime
		Duration	Current	Duration	Current	Duration	Current		
TIM	1 s	4.35 ms	15 mA	2.78 ms	32.77 mA	994.11 ms	20 μA	0.577 mW	2.74 yrs
	10 s	4.35 ms	15 mA	2.78 ms	32.77 mA	9.99 s	20 μA	0.117 mW	13.51 yrs
Non-TIM	1 s	4.35 ms	15 mA	2.30 ms	40.67 mA	993.53 ms	20 μA	0.590 mW	2.68 yrs
	10 s	4.35 ms	15 mA	2.30 ms	40.67 mA	9.99 s	20 μA	0.118 mW	13.37 yrs

TABLE 2. Power consumption and battery life of the IEEE 802.11ah SoC depending on operation mode.

FIGURE 3. Layout of indoor laboratory for multi-station uplink performance evaluation.

Power Consumption

The developed IEEE 802.11ah chip supports the low-power operation modes that are specified by the IEEE 802.11ah standard, including the TIM, non-TIM, TWT, and wireless multimedia power save mode. Furthermore, the chip divides the power into six domains and controls each domain separately to reduce the power consumption by switching on only the necessary domains. When the system boots, it transitions between active, sleep, and deep sleep modes depending on the operation condition for low power consumption. In sleep mode, the clocks of all peripherals except the CPU, bus, memory, digital baseband, power management controller, and real-time clock are turned off, and only the clock oscillator is selectively turned on and off. In deep sleep mode, all circuits except the always-on block are turned off to save power, reducing power consumption to less than 20 μA. In the TIM mode, a station wakes up periodically and receives a beacon to send or receive data after identifying a channel access period. In the non-TIM mode introduced for IoT sensor applications, the listening interval is negotiated to prevent excessive uncontrolled uplink channel access and improve energy efficiency.

The estimated power consumption and battery life of the chip is shown in Table 2. The prediction was achieved by applying the total consumed current measured on the chip to the calculation under two scenarios, the TIM and non-TIM modes of operation. Power consumption varies depending on the pattern of application data traffic, for example, the size and period of application data. To avoid such dependency of power consumption on the traffic pattern, we do not consider application data for power consumption assessment. In the TIM mode, a station monitors (receives and decodes) DTIM and TIM beacons to identify a channel access period. In the TIM mode, an AP sends a 27-byte short beacon frame with MCS10 in every beacon interval (i.e., a wakeup interval in Table 2). In the non-TIM mode, a station sends a 17-byte trigger packet with MCS10 and 0 dBm transmit power to an AP to confirm the presence of buffered data with the AP and receives an Acknowledgment (ACK).

In Table 2, "pre-active" denotes the time spent on configuring the transceiver to send or receive packets. "Active" denotes the actual time for receiving a beacon frame in the TIM mode, and transmitting a trigger frame and receiving its ACK in the non-TIM mode. The wakeup interval is considered to be extendable to a period that is proportional to listening intervals. The battery voltage (VBAT) is assumed to be 3.3 V, and the battery capacity value is 4200 mAh. Table 2 shows that when the wakeup interval is 10 s, a life of approximately 13 years is estimated, and when the wakeup interval is 1 s, a life of approximately 2.7 years is estimated.

Discussion

Wireless Channel and Channel Access

The sub-1 GHz band propagates to a relatively long distance due to its propagation characteristics, and it experiences interference due to the electromagnetic waves emitted from numerous electronic devices. Consequently, the channel quality is inevitably poor. In addition, as WiFi uses unlicensed bands, it is generally considered less stable than mobile communications. Accordingly, to be used in service areas closely related to human safety, properties, and life, such as smart grids, smart factories, and smart homes using IoT, research on interference mitigation technology is required to ensure stable operations in the case of interference.

In the sub-1 GHz band, most IoT devices follow the listen-before-talk channel access protocol, which checks before transmission whether other users are using the transmission channel. It transmits information only when the channel is not in use. Thus, the transmitting side transmits only when there is no signal in the channel, and the receiving side transmits an ACK signal to the transmitting side when it receives the signal. If another user is using the same frequency, it is difficult to find a chance to transmit, and even normal transmissions are difficult due to interference. In this case, the ACK signal does

not reach the signal sender, leading it to retransmit the same signal several times, quickly depleting the battery and potentially reducing communication efficiency due to unnecessary signal transmissions.

Various Applications of WiFi HaLow

Large-Scale IoT Sensor Networks with an Extended Range: WiFi HaLow enables the construction of large-scale sensor networks of more than 8000 sensor nodes with extended service coverage. In large-scale networks, IEEE 802.11ah devices can enable WiFi services in shaded areas such as garages, backyards, and basements. The improved link budget allows home networking even when transmitting without a power amplifier. Furthermore, the long-sleep operation and packet structure optimized for small packets enables low-power operation, and network construction costs are low because of TCP/IP support. The key lies in ensuring the networking efficiency of thousands of nodes in the broadband network.

Smart City, Smart Grid, and Smart Factory: Wireless Internet services can be provided in all areas of a city, and public infrastructure such as transportation, communication, and finance can be connected for efficient and convenient living. By utilizing the greatly expanded service coverage provided by wide-area WiFi, wireless Internet services can be offered in city centers and hotspots as well as in remote areas. Broadband IoT requires network stability and security, trustworthiness, throughput, latency, and reliability to be utilized as a backbone network.

Wireless Backhaul and Traffic Offloading: Data collected from wireless sensor nodes can be aggregated and transmitted at high data rates through a long-distance backhaul between APs using wide-area WiFi. Wide-area WiFi networks can reduce the load on mobile communication networks and solve the problem of insufficient licensed bands for mobile networks. For interworking between networks, research is necessary to introduce the integration of heterogeneous communication methods into one device and discover efficient operation techniques.

Conclusion

This article presents the research and development results of a WiFi HaLow SoC for long-range and low-power IoT networks. Additionally, the field tests in various conditions are fulfilled to evaluate HaLow performance in real environments. The indoor and outdoor performance measurements of the implemented IEEE 802.11ah SoC indicate that the requirements for communication range, data rate, performance, and battery life, which are defined in the standard, are satisfied. This demonstrates the feasibility of IEEE 802.11ah as a long-range, low-power technology for IoT networks using unlicensed bands. Future research will involve the performance evaluation and improvement in dense network environments.

Acknowledgments

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R1I1A3041887), in part by the NRF grant funded by the Korea government (MSIT) (No. 2020R1F1A1061107), and in part by MSIT, Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2016-0-00313) supervised by the IITP (Institute for Information and Communications Technology Promotion).

References

[1] A. Nikoukar *et al.*, "Low-Power Wireless for the Internet of Things: Standards and Applications," *IEEE Access*, vol. 6, 2018, pp. 67,893–926.
[2] M. Chen *et al.*, "Narrow Band Internet of Things," *IEEE Access*, vol. 5, 2017, pp. 20,557–77.
[3] E. Sisinni *et al.*, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Trans. Ind. Inf.*, vol. 14, no. 11, 2018, pp. 4724–34.
[4] D. Wang *et al.*, "From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies," *IEEE Commun. Mag.*, vol. 56, no. 10, Oct. 2018, pp. 114–20.
[5] M. R. Palattella *et al.*, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE JSAC*, vol. 34, no. 3, 2016, pp. 510–27.
[6] V. K. Jones and H. Sampath, "Emerging Technologies for WLAN," *IEEE Commun. Mag.*, vol. 53, no. 3, Mar. 2015, pp. 141–49.
[7] T. Adame *et al.*, "IEEE 802.11 AH: The WiFi Approach for M2M Communications," *IEEE Wireless Commun.*, vol. 21, no. 6, Dec. 2014, pp. 144–52.
[8] S. Aust *et al.*, "Outdoor Long-Range WLANs: A Lesson for IEEE 802.11 ah," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 3, 2015, pp. 1761–75.
[9] B. Bellekens *et al.*, "Outdoor IEEE 802.11ah Range Characterization Using Validated Propagation Models," *Proc. IEEE GLOBECOM*, 2017, pp. 1–6.
[10] A. Bel *et al.*, "An Energy Consumption Model for IEEE 802.11 ah WLANs," *Ad Hoc Networks*, vol. 72, 2018, pp. 14–26.
[11] M. Park, "IEEE 802.11 ah: Sub-1-GHz License-Exempt Operation for the Internet of Things," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 145–51.
[12] E. Khorov *et al.*, "Enabling the Internet of Things with WiFi Halow — Performance Evaluation of the Restricted Access Window," *IEEE Access*, vol. 7, 2019, pp. 127,402–15.
[13] M. Nurchis and B. Bellalta, "Target Wake Time: Scheduled Access in IEEE 802.11ax WLANs," *IEEE Wireless Commun.*, vol. 26, no. 2, Apr. 2019, pp. 142–50.
[14] WiFi Alliance WiFi HaLow Marketing Task Group, Marketing Requirements Document for Interoperability Testing of Certified ERah Devices, 2015.
[15] E. Khorov *et al.*, "A Survey on IEEE 802.11ah: An Enabling Networking Technology for Smart Cities," *Comp. Commun.*, vol. 58, 2015, pp. 53–69.

Biographies

Il-Gu Lee (iglee@sungshin.ac.kr) was with Newracom Inc. as a project leader. He received his Ph.D. in computer science and engineering from KAIST, Daejeon, Korea, in 2016. Currently, he is a professor in the Department of Convergence Security Engineering, Sungshin University, Seoul, Korea.

Duk Bai Kim (db.kim@newracom.com) received his M.S. degree in information and communication engineering from KAIST in 2004. Currently, he is in charge of product development at Newracom Inc.

Jeongki Choi (jk.choi@newracom.com) received his Ph.D. in information and communication engineering from KAIST in 2015. Currently, he is in charge of the development of RF transceivers for WLAN SoCs at Newracom Inc.

Hyungu Park (hyungu.park@newracom.com) received his M.S. degree in computer science and engineering from Seoul National University in 2007. Currently, he is vice president at Newracom Inc., where he leads a department that develops WLAN MAC hardware and software.

Sok-Kyu Lee (sk.lee@newracom.com) received his Ph.D. in electrical engineering from the New Jersey Institute of Technology. Currently, he serves as the CEO and Chairman of the Board at Newracom Inc., where he is responsible for guiding the vision and direction of corporate strategy.

Juphil Cho (stefano@kunsan.ac.kr) received his Ph.D. in electronics engineering from Chonbuk National University in 2001. Currently, he is a professor in the Department of Integrated IT & Communication Engineering, Kunsan National University, Korea.

Heejung Yu (heejungyu@korea.ac.kr) received his Ph.D. in electrical engineering from KAIST in 2011. Currently, he is an associate professor in the Department of Electronics and Information Engineering, Korea University, Sejong.

As WiFi uses unlicensed bands, it is generally considered less stable than mobile communications. Accordingly, to be used in service areas closely related to human safety, properties, and life, such as smart grids, smart factories, and smart homes using IoT, research on interference mitigation technology is required to ensure stable operations in the case of interference.