Wi-Fi HaLow Internet of Things System on Chip (SoC) in Sub-1 GHz

Surendra Raju M, Aman Shrestha, Andrew Terry, Eyal Mendel, Jaric Thorning, Julius Baxter, Mohammed Mohammed, Neil Weste, Rama Kishore Chikkam, Yingbo Zhu

Morse Micro Pty. Ltd., 10-14, Waterloo Street, Surry Hills, Sydney, NSW 2010, Australia

2023 22nd International Symposium on Communications and Information Technologies (ISCIT) | 978-1-6654-5731-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISCIT57293.2023.10376041

***Abstract*—A state-of-the-art IEEE 802.11ah (Sub-1GHz, Wi-Fi HaLow) compliant system on chip (SoC) realized in the CMOS process is presented. The SoC is the industry's smallest, fastest and lowest power Wi-Fi HaLow SoC, providing up to ~10x the range of traditional Wi-Fi solutions. The device is the first 802.11ah system that supports 32.5 Mbps (using 8 MHz bandwidth). An architecture overview, key performance metrics, and various range comparisons are presented.**

Keywords—*Transceivers, Wi-fi IoT, low power, long range*

I. Introduction

The IEEE 802.11ah was standardized by the IEEE Task Group ah (TGah) to provide a low-power, high-throughput, long-range Internet of Things (IoT) communication technology. The Wi-Fi Alliance (WFA) marketed it under Wi-Fi HaLow and introduced a certification program whose first compliant products appeared in the market in 2021 [1]. Current low-power IoT communication technologies fall into Wireless Personal Area Networks (WPAN) and Low-Power Wide Area Networks (LPWAN). In the former group, Bluetooth Low Energy (BLE) and ZigBee fall short in range and throughput. In the latter group, proprietary solutions like LoRa and Sigfox focused on extreme long-range co-exist with cellular communication standards such as NB-IoT and LTE-M operating in licensed frequency bands. Wi-Fi HaLow aims to fill the gap by offering data rates varying from hundreds of kbits/s to tens of Mbits/s and across distances of tens of meters to over a kilometer [2].

The traditional 2.4-GHz Wi-Fi technologies provide high throughput in indoor scenarios with a moderate number of stations. However, Wi-Fi HaLow operates in the unlicensed sub-1 Gigahertz (S1G) frequency bands and supports up to 8191 addressable stations from a single access point. The lower radio frequencies (750 - 950 MHz) provide an 8-10 dB lower path loss due to a larger effective antenna aperture. In addition, the physical layer design resembles a 10x downclocked version of the IEEE 802.11ac, including an extra 1-MHz bandwidth mode that translates into a 13 dB improvement of the link budget [3]. This 1-MHz mode adds a range-optimized Modulation and Coding Scheme (MCS10), which provides an additional 3 dB by repeating symbols twice. In total, it provides 24.5 dB gain advantage compared to 20 MHz 2.4 GHz link budget, which greatly enhances the range for IoT applications especially when the utility meters and automation sensors are mounted in places which are far away from the AP. These attributes make Wi-Fi HaLow appealing to a myriad of scalable, smart systems, including smart sensors and meters, backhaul aggregation, camera networks, hotspot range extension or cellular offloading.

Detailed review on state of the art IoT technologies and their application in industrial automation are covered in [4] where the IoT architectures and components which constitute the "things" – such as sensors, actuators and the "Internet" which provide the connectivity are given. Moreover, security and privacy of IoT applications is important for ensuring data integrity and protection against data theft [5]. In this context, an IoT device with the latest security features such as WPA3 and native support for TLS or IPV6 would be a preferred choice. In the emerging applications such as Smart homes, Smart cities and Smart grid the need for low latency, ubiquitous IoT sensors and massive machine to machine type communication is a necessity [6]. Hence, we need one protocol which can cater to a variety of range, rate, latency and power save options to enable the ubiquitous coverage, dense deployment of sensors and long battery life. In light of the above requirements for IoT devices, which span orders of magnitude in terms of key parameters such as range, rate, duty cycling for power saving, as well as state of the art security features, the device addressed in this paper is relevant. Moreover, it operates in a license free ISM band available world-wide with different channel bandwidths and transmit power levels [7].

The contributions of this article are as follows:

- A state-of-the-art IEEE 802.11ah compliant system on chip (SoC) is presented, featuring the lowest power consumption in the market to the best of our knowledge and the first device to support 8 MHz bandwidth (allowing 32.5 Mbps in single spatial stream) modes of operation up to MCS7. This is double the maximum rate of previously reported devices [1].
- Extensive field tests, outdoor and indoor, prove the feasibility of Wi-Fi Halow at higher ranges

and in typical office environments such as multi-storey buildings compared to the well-established IEEE 802.11n/ac.

II. System-On-Chip Architecture

The SoC, as shown in the block diagram of Fig. 1 and chip photo of Fig. 2, is a single-chip solution, including radio, digital physical layer (PHY), and medium access controller (MAC) sections, designed in compliance with the IEEE 802.11ah standard, and supporting data rates up to 32.5 Mbps. Some key performance metrics are summarized in Table 1. The device is commercially available in complete FCC certified modules as small as 13 x 13 mm whilst the IC is encapsulated in a 6 x 6 mm QFN48 package.

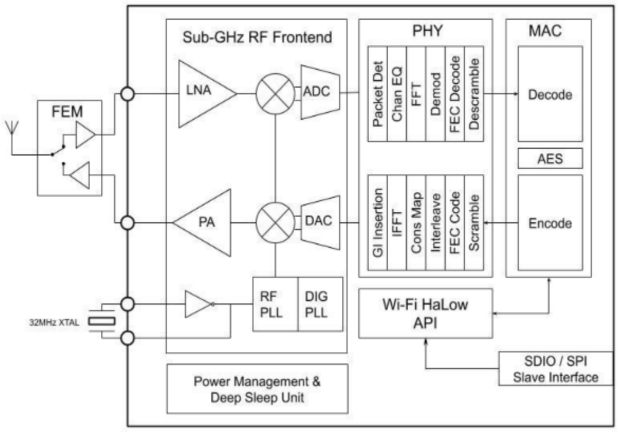


Fig. 1. SoC - Functional block diagram.

Table 1. Key Performance Metrics.

Parameter	Value
Supply Voltage	1.8 V to 3.6 V
Frequency Range	750 - 950 MHz
Max Transmit Power (without Front-end module (FEM))	8 dBm
Receiver Sensitivity at 10% PER (lowest rate, MCS 10, 1MHz)	-109 dBm
Receiver Sensitivity at 10% PER (highest rate, MCS 7, 8MHz)	-78 dBm
Rates	167 kbps to 32.5 Mbps
Baseband operating bandwidths	1, 2, 4, 8 MHz

The transmitter (Tx) architecture supports the use of an on-chip PA for low-power, low-cost devices, or the use of an external FEM for ultra-long reach applications. The receiver (Rx) architecture, as shown in Fig. 3, uses direct conversion with a 16 bit high resolution, low current consumption sigma-delta analog to digital converter (ADC). The local oscillator is generated using an all digital PLL (ADPLL) capable of transmitting and receiving signals over a relatively wide range from f_{RF} = 750 to 950 MHz.

For high frequency clocking simplicity, the ADC is clocked at a programmable rate that is directly derived via simple dividers from the local oscillator. Specifically, the ADC clock varies from $f_{ADC} = f_{RF}/2$ (8-MHz baseband mode) to $f_{RF}/16$ (1-MHz baseband mode) and subsequently the decimation chain reduces this sample rate (by a multiple of 2^n where n is programmable from 3 to 5) whilst removing quantization noise. In order to save power and area, the final sample rate of the complex I and Q at baseband is very low, being programmably adjusted to correspond to the channel BW. This necessitates a flexible non-integer resample rate conversion block which feeds into an FIR channel filter.

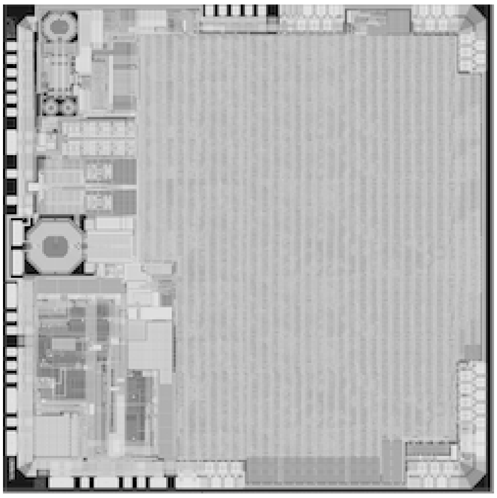


Fig. 2. Chip layout.

The baseband processing consists of 4 subsystems each with a dedicated RISC-V processor as shown in Fig. 3. The subsystems are time-domain physical (PHY), frequency domain PHY, medium access control (MAC), and host/interface processor. The RISC-V processor offers the benefits of open-source IP and configurability without extra licensing costs.

A notable feature of the baseband device architecture is the partitioning between software and hardware with the device essentially a software defined radio supported by a reconfigurable hardware accelerator. The 11ah PHY (Physical Layer) processing uses a RISC-V processor with a custom hardware accelerator called the Coproc (for coprocessor). The Coproc has a set of hardware resources such as (multipliers, memories, CORDIC processors, forward error correction en/de/coder, FFT (32-256 point) engine, de/puncturing, de/scrambling, de/interleaving, equalization, de/modulation) required by 11ah PHY path. The Coproc reconfigures these

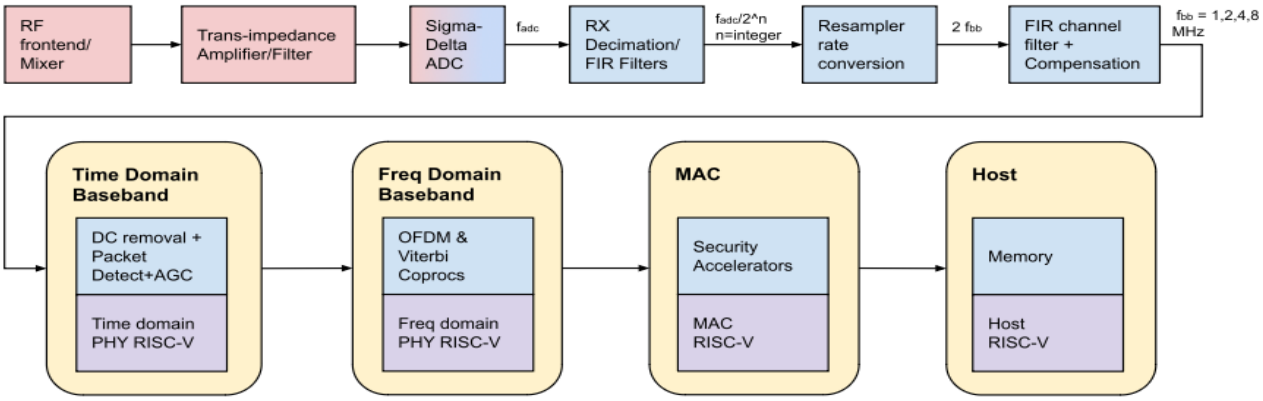


Fig. 3. Receiver Block Diagram showing the 4 RISC-V processors with accelerators.

hardware resources to achieve a single operation (say FFT) or a cascade of PHY operations.

Normally, the instructions are internally cascaded to achieve a classically pipelined design. However, should modifications be required post fabrication, the pipeline can be broken by the controlling RISC-V processor and error mitigation inserted in the form of C code patches. The pipelined processor is fast enough to provide margin for the much slower RISC-V. This partitioning facilitates flexible advancement of functionality such as the introduction of algorithms for handling interference. The system may be classified as a Targeted Software Defined Radio. (TSDR).

Time domain processing for packet detection and frequency offset estimation is especially challenging in 802.11ah due to the large number of potential operating bandwidths combined with modes such as sub-bands (e.g. transmission of 1, 2, 4 or 8 MHz within an 8-MHz operating band), and duplicate modes (transmission of 1 or 2 MHz duplicated across the operating bandwidth). A configurable DSP block is used for correlation and classification of this complex set of potential signals.

An integrated DC-DC buck converter supports a wide supply voltage range from 1.8 V to 3.6 V. The buck output is connected to 3 internal voltage regulators for receiver, transmitter and digital subsystems.Current consumption for key operating modes is low, as summarized in Table 2. Of particular note is the receiver - periodic STA listen current which can dominate many low power applications. Careful control of protocol timing and sub-system power up was used to reduce current consumption.

The MAC layer supports a wide range of functions in the 802.11ah specification including:

- Station (STA) and access point (AP) roles
- Listen-Before-Talk (LBT) access with energy detect
- 802.11ah power save modes such as Target Wake Time (TWT) support for long battery life
- 802.11ah fragmentation and defragmentation
- Automatic and manual modulation coding scheme MCS rate selection
- Security features such as AES and hardware hash functions

Table 2. Measured Current Consumption.

Mode	Conditions	Value
Transmit Current	1 MHz channel, MCS0, 0 dBm power,	56 mA
	8 MHz channel, MCS7, 0 dBm power	71 mA
Receiver - Active	1 MHz bandwidth, Vbat = 3.3V	25 mA
	8 MHz bandwidth, Vbat = 3.3V	52 mA
Receiver - periodic STA listen	DTIM = 10, 8 MHz, beacon interval = 100 ms, Note 1	95 µA
Deep Sleep	RTC On, configurable wake up timer	0.8 µA
Hibernate	Power off, wait for external interrupt	0.1 µA

Note 1: DTIM (Delivery Traffic Indication Message) is a feature that allows the access point (AP) to inform connected clients when their buffered multicast or broadcast data is ready to be retrieved. With DTIM = 10 and a beacon interval of 100 ms, the station will be listening every 1 sec. This is a common periodic listen state for a station (STA) device.

The device also includes an array of interface and peripheral options including

- SDIO 2.0 and SPI Host interface
- GPIO/UART/I2C/PWM

III. Range Testing - Outdoor Environment Results

In this section, we evaluate the performance of the HaLow-based chip in an outdoor environment, where the goal is to demonstrate the long-range capability whilst maintaining high data rates supported by the Wi-Fi ah standard. Further, we compare the performance against the ubiquitous standard IEEE 802.11n.

During the outdoor ranging test, the receiver (Rx) device is static, at a height of 2m as shown in Fig 4, whereas the transmitter (Tx) is continuously moving further away from the receiver, with starting and ending points as described in Fig. 5. As the Tx moves, the distance from the receiver and the corresponding throughput are recorded. For each location, dozens of seconds worth of data are captured at the receiver, which calculates the average throughput in kbps.

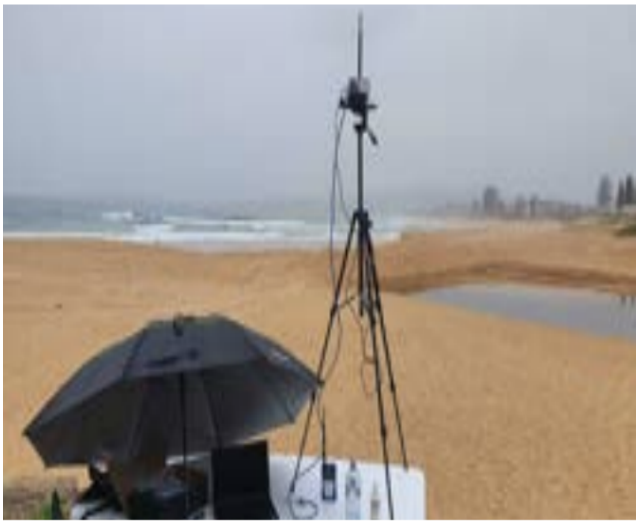


Fig. 4. Receiver device configuration used in the outdoor range testing.

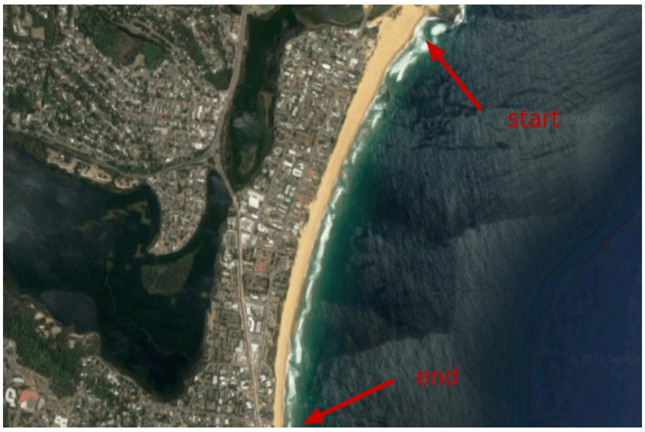
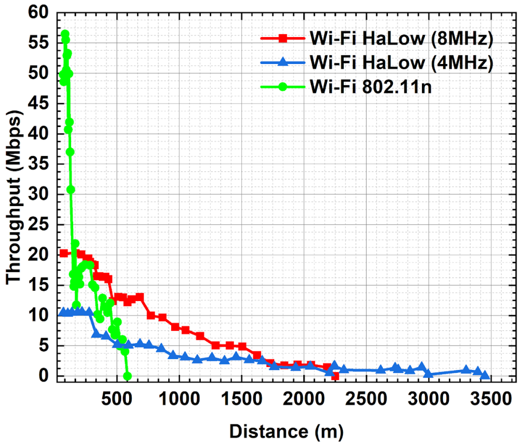


Fig. 5. Starting and ending points of the range testing.

B. Throughput results

Fig. 6 displays the throughput recorded across several distances between Tx and Rx for the Wi-Fi HaLow chip and the one using 802.11n. Considering the former, two different bandwidth values were employed, 4 and 8 MHz. It can be seen that when 802.11n is used, the throughput rapidly decreases with distance until no data is received for distances greater than 565 meters, whereas the HaLow chip enables data transmission for distances up to 2250 and 3500 meters (4 and 8 MHz respectively), providing a coverage range around 6 times greater than its 802.11n counterpart. In addition, even for lower distances around 300 m, the HaLow-based chip presents higher throughput, outperforming the chip based on the 802.11n standard, and demonstrating that this technology yields excellent coverage with high data rates.



￼Fig. 6. Throughput vs. distance recorded during outdoor range testing.

IV. Range Testing - Indoor Environment Results

In this section, we evaluate the performance of the HaLow-based chip when compared to 802.11n in an indoor environment.

A. Experimental setup

The APs (for both 802.11ah and 802.11n) were collocated at a fixed, relatively central, location on the 4th floor of an 8 level building. The corresponding STA devices were positioned successively at 10 locations over distances from 2 to 25 m where the number of walls in the path varied from 0 to 5 and the number of floors varied from 0 to 4.

The 802.11n system was set-up to use a 20-MHz, 2.45-GHz channel in order to provide the longest possible range. The 802.11ah system was set-up with rate-control enabled such that it will adapt the channel bandwidth and MCS to provide the highest possible rate whilst still preserving range. Measurements of rate, distance, number of floors (concrete thickness = 24 cm, height = 3.3 m), and number of walls were recorded and shown in Table 3.

B. Throughput results

A comparison of throughput rate for each location is shown in Fig. 7 with the distance. Clearly 802.11ah demonstrates higher rates compared to 802.11n especially when the RF path consists of multiple floors and walls in complex environments. The throughput for 802.11n is dramatically affected by the concrete floors such that data rates are quite low (<3.5 Mbps) for a single floor and no connection is observed for greater than 1 floor. Conversely 802.11ah can maintain a link even over 4 floors. Similar results on a single level with multiple walls is also observed.

As an example, examining the NIST database of signal attenuation in construction materials [8], for a 178-mm brick wall, the wall loss at 2.4 GHz is 11 dB whilst at 920 MHz this loss is 5.5 dB. Herein lies one of the major advantages of 802.11ah-HaLow - it is relatively unaffected by internal walls and floors (building material in general).

Table 3. Indoor range comparison data - 802.11ah vs 802.11n.

Position	**L4 posA**	**L4 posC**	**L4 posD**	**L5 posA**	**L5 posB**	**L5 posC**	**L5 posE**	**L8 posA**	**L8 posB**	**L8 posC**
distance(m)	0.5	19.8	24.2	9.7	4.4	20.1	12.1	14.7	14.2	25.4
floors	0	0	0	1	1	1	1	4	4	4
walls	0	2	5	0	1	1	3	0	1	1
802.11ah(Mbps)	17.2	18.8	2.8	18.8	16.7	10.4	12.9	0.994	4.88	2.56
802.11n(Mbps)	23.5	0.6	0	3.49	2.2	0	0.275	0	0	0

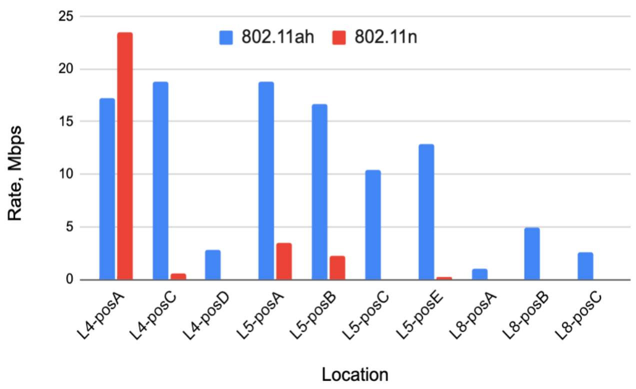


Fig. 7. Throughput vs. location during indoor range testing.

V. Conclusions

A high performance 802.11ah SoC is presented featuring the first implementation of a 32-Mbps, 8-MHz bandwidth device. The device supports a wide range of sub-GHz channels from 750-950 MHz and includes a highly configurable targeted software defined baseband utilizing 4 RISC-V processors with accelerators. Indoor range testing highlighted one of the major advantages of 802.11ah - enhanced propagation through building materials and robustness in complex environments. Similarly, in an outdoor environment, HaLow can extend the range of ~8 Mbps data rates from less than 250 m for 802.11n to over a kilometer and can maintain a link of >167 kbps up to 3.5 km. With a modest omni gain antenna (5-9dBi) on the AP, ranges can easily be extended to 8 km.

VI. Acknowledgements

The authors would like to thank Peter Bradley, Cristo Suarez-Rodriguez, Joy Baitin, Gelyn Manzanares, Maria Valenzuela, Winston Ong, Michael De Nil, David Goodall, Bassem Dawood, Simon Wadsworth, and Anthony Burch for technical discussions and helpful comments.

VII. References

[1]. I-G. Lee et al., "WiFi HaLow for Long-Range and Low-Power Internet of Things: System on Chip Development and Performance Evaluation," in IEEE Communications Magazine, vol. 59, no. 7, pp. 101-107, July 2021.

[2]. Tian, Le, et al. "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11 ah research." in Journal of Network and Computer Applications, vol. 182, May-2021.

[3]. Khorov et al., "A Survey on IEEE 802.11ah: An Enabling Networking Technology for Smart Cities," Comp. Commun., vol. 58, 2015, pp. 53–69..

[4]. K. Shafique, et al, "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," in *IEEE Access*, vol. 8, pp. 23022-23040, 2020.

[5]. F. Meneghello, et al. "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices." *IEEE Internet of Things Journal* 6.5 (2019): 8182-8201.

[6]. T. Singh, et al. "A Decade Review on Smart Cities: Paradigms, Challenges and Opportunities." *IEEE Access* (2022).

[7]. 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 - Annex E, IEEE Standards Association, 2020.

[8]. W. C. Stone, "Electromagnetic Signal Attenuation in Construction Materials," , NISTIR 6055, NIST Construction Automation Program, Report No. 3, October 1997, Building and Fire Research Laboratory, NIST, Gaithersburg, Maryland 2089, Section 4.1, pp 63-67.