A Directional Hand-Held 2.4 GHz WiFi Detector

6.2300 Class Project: Final Report

Bernard Jin
MIT EECS
bljin@mit.edu

Liong Ma
MIT EECS
liongma@mit.edu

Elwin Au
MIT EECS
eau131@mit.edu

***Abstract*—The prevalence of Wifi and Bluetooth devices in modern technology use the 2.4 GHz band, making it a convenient target for tracking wireless devices. This paper proposes an RF detector that selectively detects devices transmitting on the 2.4 GHz band via power harvesting. Radio frequency (RF) power is received by a highly directional helical antenna, then amplified using a low noise amplifier (LNA) and filtered using a hairpin microstrip filter. An impedance-isolated envelope detector is then used to output a usable signal as a low-frequency analog voltage.**

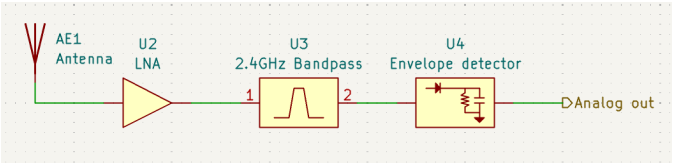

Fig. 1. Block diagram of the RF detector

I. Introduction & Motivations

The ability to detect and localize wireless-emitting devices has significant applications in both civilian and security contexts. In particular, search-and-rescue (SAR) operations often rely on locating survivors who may be carrying WiFi-enabled devices such as smartphones, laptops, or wearable electronics [1] In particular, the 2.4 GHz band is very commonly used in personal devices and is able to penetrate a fair amount through common construction materials compared to other consumer frequencies (Table I). Existing techniques used in SAR, such as thermal imaging, radar systems, or cellular triangulation, are often expensive, infrastructure-dependent, or require active cooperation from network providers. This creates a need for a low-cost, portable, and infrastructure-independent method of detection.

TABLE I
Attenuation of 2.3 GHz and 5.25 GHz waves in common construction materials [2]

Material	T (dB)	
	2.3 GHz	5.25 GHz
Glass	-0.4998	-1.6906
Drywall (9mm)	-0.5095	-0.8470
Red brick (dry)	-4.4349	-14.621
Cinder block (dry)	-6.7141	-10.326
Fir lumber	-2.7889	-6.1253

Previous work in RF detection has demonstrated the feasibility of identifying the presence of signals using directional antennas and power detection techniques [3]. These systems can detect and characterize RF sources over a wide frequency range. However, these systems are typically bulky and costly, limiting their use in field deployment. More compact solutions, such as handheld RF detectors used in electronics debugging or surveillance, often sacrifice sensitivity or selectivity, making them less effective in weak-signal environments such as disaster zones [4].

Similar RF detection techniques have also been applied in the context of electronic surveillance and counter-surveillance, particularly in the identification of hidden wireless transmitters ("bugs"). In these applications, devices are designed to detect unintended RF emissions in specific frequency bands commonly used by consumer wireless protocols. Although effective, many commercial solutions again rely on broadband detection or expensive components, which limits accuracy, accessibility, and customization [4].

In this project, we propose a low-cost RF detection device optimized for the 2.4 GHz ISM band, which is heavily utilized by WiFi-enabled devices [5] . By combining a directional helical antenna, a low-noise amplification stage, a narrowband filter, and an envelope detector, the system is designed to detect the presence and relative strength of nearby wireless signals without requiring demodulation or protocol-specific decoding. This approach enables a simple yet effective method for locating RF-emitting devices through directional scanning.

The primary motivation of this work is to demonstrate that a compact and inexpensive system can provide meaningful functionality for both search-and-rescue scenarios and RF surveillance applications. By focusing on simplicity, cost-efficiency, and ease of construction, this project aims to bridge the gap between high-performance RF instrumentation and practical, deployable detection tools.

II. Approach (aka Materials & Methods)

The device consists of four major parts (Fig. 1): the antenna, a low-noise amplifier (LNA), a 2.4 GHz bandpass filter, and an envelope detector. Waves received by the antenna will be amplified into a usable range by the LNA. The bandpass filter then only allows frequencies of interest (around 2.4 GHz) to pass to the envelope detector. The envelope detector

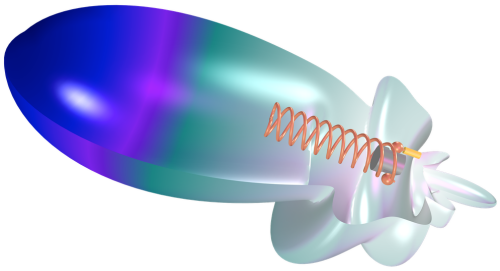

Fig. 2. Helical antenna and radiation pattern [9]

then converts the signal into a low-frequency voltage that corresponds to the power of the received wave.

The antenna used is a helical antenna (Fig. 2) operating in axial mode, chosen for its directivity [6] and ease of construction. This directivity is achieved by having the path length around one revolution of the antenna be close to the wavelength of our wave, resulting in constructive interference out the end of the helix while destructive interference reduces sidelobes. This condition is often approximated to $\frac{3\lambda}{4} \leq 2\pi r \leq \frac{4\lambda}{3}$ [7], where r is the radius of the antenna. Our design will use a helical antenna with $r = 2\,\mathrm{cm}$, resulting in a circumference of $\approx 12.6\,\mathrm{cm}$, which is close to the wavelength of a $2.4\,\mathrm{GHz}$ wave ($\approx 12.5\,\mathrm{cm}$) The antenna for our device was constructed out of copper wire and a 3D printed support.

The impedance for a helical antenna can be approximated as $Z_0 = 140\frac{2\pi r}{\lambda}$ [7]. For our antenna, this results in an impedance of $140.82\,\Omega$. Impedance matching to the antenna will be achieved with tapered triangular copper strip, which will be manually tuned.

Due to the low transmission power of cell phones and other wireless devices, an LNA is used to amplify the signal received by the helical antenna to a usable level. The typical output power of most devices is around $1\,\mathrm{W}$. [8] The Friis transmission equation can be used to estimate the received power in ideal conditions. This is then used to size the gain of the LNA and analog-to-digital converter (ADC).

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$$

The received voltage is then simply a function of the received power, $V_r = \sqrt{P_r Z_0}$. Estimating around a 50% efficiency for the receiving helical antenna, this produces around $5\,\mathrm{mV}$ at the input of the LNA. Thus a $30\,\mathrm{dB}$ LNA can be used to amplify the signal to $150\,\mathrm{mV}$ to be fed into the Envelope detector. The chosen LNA is the PSA-8A+ $50\,\Omega$ $31dB$ monolithic amplifier.

The band pass filter is a 3rd order hairpin microstrip Chebyshev filter, chosen for its small size, low loss, and steep rolloff. The bandwidth of this filter was chosen to be $150\,\mathrm{MHz}$ to be able to filter out other frequencies while covering a fair portion of the $2.4\,\mathrm{GHz}$ band. The passband ripple was chosen to be $0.1\,\mathrm{dB}$ to minimize the effect of the filter on the passband while retaining a steep rolloff. A stub was placed on either side of the filter to attenuate $4.8\,\mathrm{GHz}$ signals, which would also pass through the filter. A prototype was designed with the coefficients for a Chebyshev filter [10], and then fine-tuned using HFSS simulations. The lowest insertion loss we were able to achieve with our bandwidth was $-5.4\,\mathrm{dB}$ due to the loss of the FR4 substrate.

The final stage is an envelope-follower, which is effectively a rectified half-wave rectifier. Due to the high input impedance, a common-collector amplifier circuit is used to create an impedance isolated voltage follower to feed into the RC output. Since it must continuously modulate at 2.4 GHz, the gain-bandwidth product is chosen to be at least 350 GHz for a gain of 15 dB. The diode creates a voltage drop which may be larger than the output of the LNA, so a DC bias is added through a voltage divider to the input of the RF diode. [11] The diode must have an exceptionally low junction capacitance to reduce reverse-recovery time, as well as low lead inductance which would introduce parasitic oscillations to the output. The chosen diode is BAR63-03W which has pF junction capacitance at 2.4 GHz. A resistor capacitor (RC) filter is utilized to filter out the high frequency signal. The chosen frequency is 10kHz which provides 40dB of attenuation to the 2.4GHz modulation frequency.

To validate individual parts of our design, we will build the electronics for the detector on two separate printed circuit boards (PCB): one for the antenna and amplifier, and one for the filter and envelope detector. All lines will be tuned to function with a 50-Ohm impedance matched microstrips to reduce reflections and other undesired behavior.

III. Legality, Safety and Ethics

The FCC generally does not regulate the reception of electromagnetic waves with the exception of emergency [12] and cellular [13] frequencies. This device is unable to receive signals at the aforementioned frequencies, as the filter attenuates all signals under $1\,\mathrm{GHz}$ by more than $-50\,\mathrm{dB}$.

The FCC also limits emissions within the $2.4\,\mathrm{GHz}$ band to less than $36\,\mathrm{dBm}$ ($4\,\mathrm{W}$) [13]. Since the detector only receives power and does not radiate it, as well as the fact that the P1dB point of our amplifier is at $2\,\mathrm{GHz}$ is $9.6\,\mathrm{dBm}$, this device will not be able to radiate more than $4\,\mathrm{W}$.

The main ethical concern with this device is with regards to its ability to eavesdrop and stalk people. While information could theoretically be skimmed through the ripple of the envelope detector, this is very unlikely to happen in reality due to the very large time constant and small signal amplitude. With regards to stalking, though this device could be used in such a manner, the prevalence of $2.4\,\mathrm{GHz}$ devices in most settings would make stalking difficult. Furthermore, as a passive detection device, this device cannot actively track down an individual, enabling stalking no more than an ordinary microphone.

With regards to safety, the highest voltage on the entire system of the supply of $6\,\mathrm{V}$, with only a maximum of $300\,\mathrm{mA}$ through the system, and is unlikely to hurt anybody electrically. The antenna will have its end sanded down and be

wrapped around a plastic support, making it unlikely to come loose and cause damage.

IV. Results

The device was tested using the hotspot feature on a Google Pixel 6 smartphone. Tests were done for the effect of range and material attenuation.

Measurements of the antenna performance showed a highly-directed central lobe with smaller sidelobes (Fig. 3), as would be expected from an antenna operating in the axial mode.

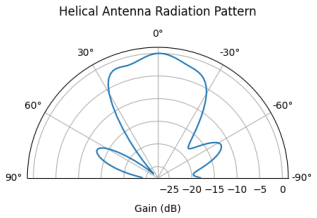

Fig. 3. Measured Antenna Gain

Basic functionality was demonstrated by placing the phone a distance of $1\,\mathrm{m}$ in front of the antenna. When the hotspot was enabled, a regular pattern of beats timed approximately $100\,\mathrm{ms}$ were observed from the device (Fig. 4), which were not present otherwise.

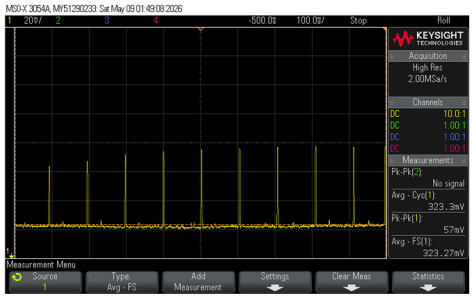

Fig. 4. WiFi beacon frames observed from the device

To measure the amplitude, the maximum voltage is subtracted from the minimum voltage to derive the signal voltage. The noise level was calibrated with the antenna pointed away from all sources of noise and then electromagnetically shielded, measuring to 2 mV. The amplitude of the WiFi beats are normalized to 1 ft away with an amplitude of 150 mV.

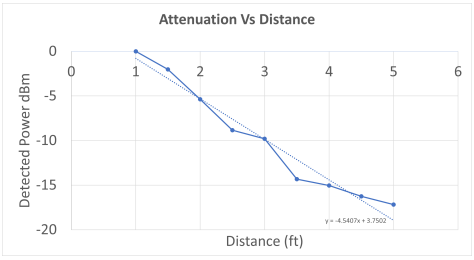

Fig. 5. Received power from hotspot phone over distance

The rate of attenuation is measured with large distances, which experimentally follows a decay of $\frac{1}{r^2}$. The effective distance is found with $D_{\text{eff}} = D\sqrt{\frac{V_D}{V_{min}}}$ meaning the effective distance for the WiFi detector on a phone with hotspot is $15\mathrm{m}$ before reaching the noise floor.

TABLE II
Device Performance

Center Frequency	2.4	GHz
Device Impedance	50	Ω
Noise Floor	2	mV
Device Gain	30	dB
Range	15	m

Testing interfering materials demonstrated little to no signal degradation through less dense, non-conductive materials, which are common in construction or outdoors. There was significant attenuation through denser, thicker, or conductive materials, limiting the usage to devices which are relatively close to the user.

TABLE III
Output Voltage With Attenuating Materials

Material	mVpp	Attenuation (dB)
Air	150	0
Tile	150	0
MDF	150	0
2x4	146	-0.2347680654
Notebook (paper)	120	-1.93820026
Copper Clad Board 1oz	35	-12.64046429
Steel Sheet	18	-18.41637508
Flesh	17	-18.91284675
Steel Pan	14	-20.59926447

V. Discussion

The timing and presence of the beats only when the hotspot is on suggests that these are WiFi beacon frames, which are transmitted once every $102.4\,\mathrm{ms}$ [14], confirming the functionality of the device.

The exceptionally low noise floor, and thus range, can largely be attributed to electromagnetic shielding applied around the device amplifier which prevents parasitic noise coupling. Additionally, each stage of the device was tuned separately leading to accurate impedance matching.

Though the device is able to detect $2.4\,\mathrm{GHz}$ devices at a distance, materials between the source and the device may attenuate signals and limit its effective range (Table III). In particular, conductive materials such as steel and human flesh attenuate the signal significantly due to impedance mismatch with air $2.4\,\mathrm{GHz}$ causing reflection of radiated waves.

Future iterations may address this with a larger amplification ratio and a more directional antenna which would improve the device gain, allowing significantly smaller signals to be detected, for the tradeoff of higher cost and complexity.

VI. Conclusions

The device is able to effectively detect the presence of a mobile device, generating a peak-to-peak voltage of $18\,\mathrm{mV}$ at a distance of $1.524\,\mathrm{m}$.

References

[1] Y. Zhang, X. Wang, J. Wen, and X. Zhu, "WiFi-based non-contact human presence detection technology," *Scientific Reports*, vol. 14, no. 1, p. 3605, Feb. 13, 2024, ISSN: 2045-2322. DOI: 10.1038/s41598-024-54077-x. Accessed: Apr. 21, 2026. [Online]. Available: https://www.nature.com/articles/s41598-024-54077-x.

[2] R. Wilson, "RF propagation losses: 2.4 GHz vs 5 GHz building materials," Magis Networks, Inc., 2002. Accessed: Apr. 22, 2026. [Online]. Available: https://www.am1.us/wp-content/uploads/Documents/E10589_Propagation_Losses_2_and_5GHz.pdf.

[3] S. Denis, R. Berkvens, and M. Weyn, "A survey on detection, tracking and identification in radio frequency-based device-free localization," *Sensors*, vol. 19, no. 23, p. 5329, Jan. 2019, ISSN: 1424-8220. DOI: 10.3390/s19235329. Accessed: Apr. 21, 2026. [Online]. Available: https://www.mdpi.com/1424-8220/19/23/5329.

[4] H. Shahid, "Radio frequency detection, spectrum analysis, and direction finding equipment,"

[5] C. Wang, S. Chen, Y. Yang, F. Hu, F. Liu, and J. Wu, "Literature review on wireless sensing-wi-fi signal-based recognition of human activities," *Tsinghua Science and Technology*, vol. 23, pp. 203–222, Apr. 1, 2018. DOI: 10.26599/TST.2018.9010080.

[6] J. Kraus, "The helical antenna," *Proceedings of the IRE*, vol. 37, no. 3, pp. 263–272, Mar. 1949, ISSN: 2162-6634. DOI: 10.1109/JRPROC.1949.231279. Accessed: Apr. 21, 2026. [Online]. Available: https://ieeexplore.ieee.org/document/1697976/.

[7] "Helical antenna (helix antenna)," Accessed: Apr. 21, 2026. [Online]. Available: https://www.antenna-theory.com/antennas/travelling/helix.php.

[8] "Power of a cell phone transmitter - the physics factbook," Accessed: Apr. 21, 2026. [Online]. Available: https://hypertextbook.com/facts/2006/EbruBek.shtml.

[9] "Analyzing operating mode options for helical antennas," COMSOL, Accessed: Apr. 21, 2026. [Online]. Available: https://www.comsol.com/blogs/analyzing-operating-mode-options-for-helical-antennas.

[10] J. S. Wong, "Microstrip tapped-line filter design," *IEEE Transactions on Microwave Theory and Techniques*, vol. 27, pp. 44–50, Jan. 1, 1979, ADS Bibcode: 1979ITMTT..27...44W, ISSN: 0018-9480. DOI: 10.1109/TMTT.1979.1129556. Accessed: Apr. 21, 2026. [Online]. Available: https://ui.adsabs.harvard.edu/abs/1979ITMTT..27...44W.

[11] *Envelope detector*, in Analog Devices Wiki, Jan. 3, 2021. [Online]. Available: https://wiki.analog.com/university/courses/alm1k/circuits1/alm-cir-envelope-detector.

[12] "47 CFR § 18.303 - prohibited frequency bands.," LII / Legal Information Institute, Accessed: Apr. 21, 2026. [Online]. Available: https://www.law.cornell.edu/cfr/text/47/18.303.

[13] "47 u.s. code § 302a - devices which interfere with radio reception," LII / Legal Information Institute, Accessed: Apr. 21, 2026. [Online]. Available: https://www.law.cornell.edu/uscode/text/47/302a.

[14] nayarasi. "802.11 mgmt : Beacon frame," mrn-cciew, Accessed: May 9, 2026. [Online]. Available: https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/.