Demo: Ubiquitous Battery-free Sensing AirTags

Spanddhana Sara, Dhairya Shah, Pramuka Sooriya Patabandige, Rajashekar Reddy Chinthalapani, Ambuj Varshney
National University of Singapore, Singapore
{spanddhanasara,dhairya,pramuka,rajashekar.c}@u.nus.edu,ambujv@nus.edu.sg

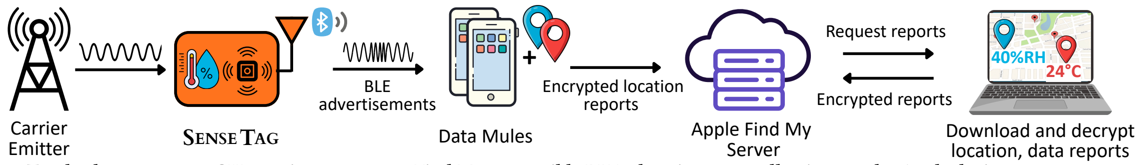


Figure 1: SenseTag backscatters a 2.4 GHz carrier to generate Find My compatible BLE advertisements, allowing nearby Apple devices to act as opportunistic data mules. Sensor readings are encoded through the Find My cryptographic key generation process, without exposing readings in public BLE fields. The backend running on a commodity computer decrypts both location and sensor data for visualization on a web-based dashboard.

Abstract

Commercial asset tracking systems such as Apple AirTags use hundreds of millions of mobile devices as opportunistic data mules, enabling global location coverage without dedicated cellular infrastructure. However, existing trackers are limited to location reporting, rely on active BLE radios and coin-cell batteries, and cannot support long-term sensing deployments. We demonstrate SenseTag, a work-in-progress tracker that extends AirTag-like functionality towards battery-free, sticker form-factor sensing. SenseTag leverages Apple's Find My network as a global backhaul for both location and sensor data, using backscatter communication to eliminate the cost of active BLE transmission. A key challenge is implementing Find My's cryptographic protocol within the tag's constrained compute and energy budget. Unlike prior systems that encode data into public BLE advertisement fields, exposing it to passive scanners, SenseTag embeds sensor readings into the private-key generation process, preserving Find My-compatible location decryption while preventing exposure to passive BLE scanners. We demonstrate an end-to-end prototype using commodity tag-side hardware and a controllable carrier emitter, backhauling environmental sensor data through Apple's Find My network and visualizing recovered location and sensor readings on a web-based dashboard.

CCS Concepts

• **Hardware → Sensor devices and platforms**; **Wireless devices**;
• **Security and privacy → Cryptography**.

Keywords

Backscatter communication, Apple Find My, Opportunistic networks, Battery-free sensing, Crowd-sourced infrastructure

ACM Reference Format:
Spanddhana Sara, Dhairya Shah, Pramuka Sooriya Patabandige, Rajashekar Reddy Chinthalapani, Ambuj Varshney. 2026. Demo: Ubiquitous Battery-free Sensing AirTags. In *The 24th Annual International Conference on Mobile Systems, Applications and Services (MobiSys Companion '26), June 21–25, 2026, Cambridge, United Kingdom.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3812835.3814966

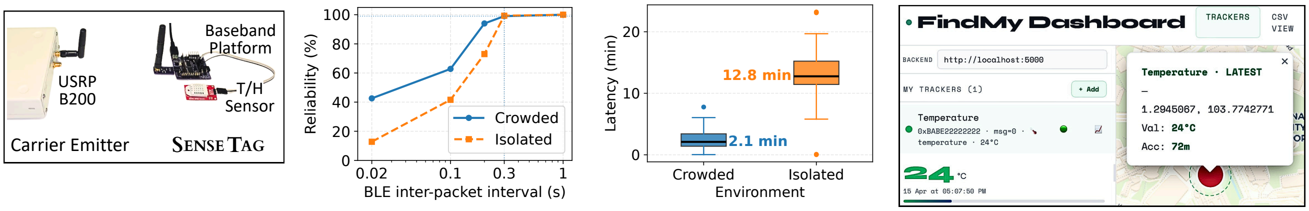
ACM ISBN 979-8-4007-2711-5/2026/08
https://doi.org/10.1145/3812835.3814966

1 Introduction

Asset tracking systems like Apple AirTags use hundreds of millions of Apple devices as opportunistic data mules, enabling global location coverage through Apple's Find My ecosystem [5]. However, AirTags were designed solely for location reporting with no support for relaying sensor data. They rely on active BLE radios and are thus powered by coin-cell batteries, requiring periodic replacement and limiting deployment in inaccessible or large-scale environments [5]. Recent efforts [2, 3, 9] have extended Find My to relay sensor data but these designs retain active radios, and also expose sensor values to nearby passive BLE scanners by embedding them in public advertisement fields. With over one billion active Apple devices worldwide, Find My represents the largest and most extensively studied opportunistic network to date. While similar crowd-sourced tracking ecosystems from Google and Samsung have begun to emerge, they remain comparatively nascent. Find My offers a uniquely dense, globally distributed receiver infrastructure that no purpose-built IoT network can match in scale or coverage, without requiring any dedicated deployment.

To tackle these challenges, we first describe how Apple's Find My network operates, as SenseTag builds directly on this protocol. Tags broadcast BLE advertisements containing a compressed P-224 elliptic-curve public key. Nearby Apple devices encrypt their GPS location using this key and upload the report to Apple's cloud server. The tag owner retrieves location by querying the cloud with the SHA-256 hash of the public key and decrypting reports with the corresponding private key [5]. Crucially, Apple cannot verify whether a broadcast key belongs to a legitimate AirTag, enabling extensibility beyond first-party devices. Prior work exploits this by embedding sensor values into the public key [2, 3, 9], but this exposes sensor data to passive BLE scanners and precludes location decryption since the private key is unavailable. SenseTag addresses both limitations by encoding sensor data into the private key rather than the public key, ensuring standard AirTag compatibility and enabling full decryption of location reports and sensor information.

The second challenge is power consumption. Active BLE radios, such as those in AirTags, consume milliwatts of power, necessitating coin-cell batteries that require frequent replacement. This power budget also precludes flexible batteries or energy harvesting with small capacitors, both essential for a sticker form factor. To



(a) Experiment setup (b) Decoding reliability (c) Latency with mule density (d) Visualization dashboard

Figure 2: (a) SENSETAG experiment setup (b) The decoding reliability increases with inter-packet BLE interval time. (c) The end-to-end latency is inversely proportional to mule density. (d) A web-based dashboard displays recovered tag location, sensor value, and timestamp.

address this, we leverage backscatter, which enables transmission at microwatts by reflecting an ambient carrier rather than generating one locally [4, 6]. However, existing backscatter systems typically require dedicated gateways for data collection [12]. SENSETAG solves this by implementing a BLE backscatter transmitter whose packets are fully compatible with Apple's Find My protocol, turning hundreds of millions of Apple devices into opportunistic data mules for backscatter data. Prior work has shown that commodity devices such as smartphones and routers can serve as carrier emitters [6, 11], and Apple's Find My network provides a global receiver infrastructure, together eliminating both the dedicated emitter and gateway that have prevented backscatter from scaling.

We demonstrate SENSETAG, a battery-free sensing tracker that implements Find My's P-224 elliptic-curve cryptography on a resource constrained microcontroller and uses backscatter communication to generate Find My-compatible BLE advertisements. Location and sensor readings can be recovered and decrypted on a commodity computer, as shown in Figure 1.

2 Design

The SENSETAG prototype comprises a carrier emitter (ED), a backscatter tag with onboard sensor, and a commodity computer for decoding, as shown in Figure 2(a). A USRP B200 software-defined radio serves as the ED, generating the 2.4 GHz carrier. A low-power MSP430FR5969 microcontroller drives a backscatter switch to produce Find My compatible BLE advertisements by modulating this carrier. We also evaluate a BeagleBone Black as an alternative baseband platform, using its Programmable Real-Time Unit (PRU) to generate packets on BLE advertising channels.

Although SENSETAG can transmit arbitrary data, we use environmental sensors to measure temperature and humidity, encoding the readings into the private scalar of a valid P-224 Find My key pair. To evaluate the performance of SENSETAG, we conduct experiments in two environments: crowded (~25 mules) and isolated (single mule). At a 0.3 s inter-packet interval, the tag achieves >99% delivery reliability across both environments, as shown in Figure 2(b).

On the backend, SENSETAG builds on FindMy.py [1] to authenticate with iCloud and retrieve encrypted location reports. For each sensing cycle, the server generates one candidate private key per possible sensor value, derives SHA-256 hashes of the corresponding public keys, and issues batch queries to the cloud. The matching hash identifies the transmitted sensor value, and its private key decrypts the report to recover GPS location, accuracy, and timestamp.

We design a web-based dashboard (Figure 2(d)) that allows users to configure tags by modem ID and sensor type, querying Apple's servers every 15–20 minutes. We define end-to-end latency as the time from first advertisement to report recovery. SENSETAG achieves median latency of 2.1 min in crowded and 12.8 min in isolated environments, confirming that latency scales inversely with mule density (Figure 2(c)). This makes SENSETAG well suited for monitoring applications reporting on minute-to-hour timescales.

SENSETAG currently requires carrier signal from an ED to backscatter. Recent works have stabilized tunnel-diode oscillators to eliminate the ED. While SharpPeak [7] and AudioCast [8] likely lack stability for commodity standards, M^2 [10] generates highly stable carriers at low power and could enable standalone Bluetooth transceivers, which we are exploring as future work.

3 Demonstration

We demonstrate SENSETAG end-to-end with two tags in a busy indoor area near the demo booth, where nearby Apple devices opportunistically serve as Find My data mules. For repeatability, a USRP B200 serves as the ED, though ambient carrier sources are also possible. The tags are placed at different locations and report different sensor readings. Each tag backscatters BLE advertisements that nearby mules relay to Apple's cloud server. The dashboard (Figure 2(d)) recovers sensor readings and tag locations, which updates as new reports arrive. The pipeline requires no dedicated receiver gateway or network subscription, demonstrating the feasibility of battery-free sensing and location tracking over Apple's Find My ecosystem using commodity Apple devices and backend hardware.

Acknowledgements. We thank the reviewers for their comments. This work is funded by a MoE Tier-1 grant (A-8001661-00-00), a startup grant from ODPRT (A-8000277-00-00), and an unrestricted gift from Google through their Research Scholar Program (A-8002307-00-00-00), all hosted at the National University of Singapore.

References

[1] M. Almeloo. 2024. FindMy.py: Everything You Need to Query Apple's FindMy Network. https://github.com/malmeloo/FindMy.py.

[2] A. Bellon et al. 2023. TagAlong: Free, Wide-Area Data-Muling and Services. In *ACM HotMobile '23*.

[3] F. Bräunlein. 2021. Send My: Arbitrary Data Transmission via Apple's Find My Network. https://positive.security/blog/send-my

[4] J. Ensworth et al. 2017. BLE-Backscatter: Ultralow-Power IoT Nodes Compatible with Bluetooth 4.0 Low Energy (BLE) Smartphones and Tablets. In *IEEE T-MTT*.

[5] A. Heinrich et al. 2021. Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System. In *Proceedings on Privacy Enhancing Technologies (PoPETS)*.

[6] V. Iyer et al. 2016. Inter-Technology Backscatter: Towards Internet Connectivity for Implanted Devices. In *ACM SIGCOMM '16*.

[7] M. Padmal. 2025. *Wireless Communication Systems for Energy-Constrained Environments*. Ph. D. Dissertation. Uppsala University, Sweden.

[8] C. Rajashekar Reddy, Dhairya J. Shah, Nobel Ang, and Ambuj Varshney. 2025. AudioCast: Enabling Ubiquitous Connectivity for Embedded Systems through Audio-broadcasting Low-power Tags. *ACM IMWUT* (2025).

[9] S. Sara et al. 2024. GateHaul: A Gateway Architecture using Backhauling Networks to Address the Connectivity Challenges of Embedded Systems. In *Proceedings of ACM MobiCom '24*.

[10] P. Sooriya Patabandige et al. 2026. Microwatt Microwave (M^2) Oscillator: Going Beyond the Delegation Architecture of Low-power Wireless Communication. In *ACM MobiSys '26*. (To appear).

[11] Ambuj Varshney et al. 2017. LoRea: A Backscatter Architecture That Achieves a Long Communication Range. In *SenSys '17*.

[12] T. Zachariah et al. 2015. The Internet of Things Has a Gateway Problem. In *ACM HotMobile '15*.