Poster: Crowdsourcing and Mapping COSPAS-SARSAT 406 MHz Distress Beacons

Ahsan Saleem, Andrei Costin
Faculty of Information Technology
University of Jyväskylä, Finland
{saleemay, ancostin}@jyu.fi

Guillermo Suarez-Tangil
IMDEA Networks Institute
Madrid, Spain
guillermo.suarez-tangil@networks.imdea.org

***Abstract*—In this work, we present the crowdsourcing and mapping of COSPAS-SARSAT 406 MHz distress signals, making distress data and information openly available to researchers and practitioners. The standard COSPAS-SARSAT 406 MHz distress system relies on centralized and officially operated satellites and ground stations, and no comparable (open-science/open-data) crowdsourcing and mapping networks exist. To complement this, we propose a decentralized and publicly available crowdsourcing and mapping system for 406 MHz distress signals, enabling the independent research community to investigate the capacity, efficiency, applications, and security of these systems using real-world distress signals. We performed experiments on a limited and small scale to evaluate the feasibility of the proposed system and provided possible applications and future extensions of our proposed approach.**

I. Introduction

COSPAS-SARSAT is a satellite-based radio-location system that aids in search-and-rescue (SAR) operations by providing reliable and real-time distress signals to search-and-rescue centers [1]. The system was established as a treaty of intergovernmental cooperation to facilitate search-and-rescue operations [2], [3]. In this work, we propose crowdsourcing and mapping of COSPAS-SARSAT 406 MHz distress beacons. The publicly available crowdsourcing and decoding networks have transformed the aviation (e.g., FlightRadar24 [4], OpenSky Network [5], [6], [7]) and maritime (e.g., VesselFinder [8]) domains. These services aggregate data from volunteers globally and provide near real-time data on flights (ADS-B) and maritime traffic (AIS) to the general public and researchers, thus aiding OSINT, alternative information gathering, and research activities.

COSPAS-SARSAT, which is essential for search-and-rescue operations, is a primarily regulated and centralized system. Similar to ADS-B and AIS [9], [10], the COSPAS-SARSAT transmissions are plain (unencrypted, unauthenticated) [11]. Globally, over 2 million COSPAS-SARSAT distress beacons are active, including 823,621 registered in the US alone as of 2024 [12]. With the growing COSPAS-SARSAT network, it is becoming increasingly relevant to have a crowdsourcing network where distress beacons can be analyzed and researched from both operational and cybersecurity aspects. Potential applications of this network include coverage analysis to identify and mitigate blind spots.

The location information of the 406 MHz distress signals relies on the Global Navigation Satellite System (GNSS), and there is no alternative method for ground-based systems to accurately verify this information, detect inherent issues, validate beacon transmission, or identify security vulnerabilities within the transmission. The community-oriented crowdsourcing COSPAS-SASRAT network, composed of low-cost hardware, can enable the availability of distress data for the research community to develop and propose methodologies to overcome the associated issues. Our work involves passive non-invasive reception of distress signals at 406 MHz, with no transmission or rebroadcasting, ensuring non-interference with operating SAR systems. The distress messages contain unique identifiers that are not publicly resolvable to individual users. Moreover, additional anonymization of identifiers (especially for personal beacons) could be enabled immediately at the sensor level before data is sent to the central aggregator node, thereby reducing any potential privacy impact in the event of a leak or breach of the central aggregator. To enable distress beacon analysis, our contributions are:

- We propose the *first* (to the best of our knowledge) crowdsourcing and mapping system and efforts targeting COSPAS-SARSAT 406 MHz distress signals.
- We identify an essential gap to the COSPAS-SARSAT Threat Model by Costin et al. [11], and extend the model.
- We outline potential future extensions and applications.

II. Method

The proposed crowdsourcing network is a volunteer- or participant-based sensor network designed to collect, analyze, store, and visualize 406 MHz distress signals. The crowdsourcing network comprises COSPAS-SARSAT sensors and receivers deployed by volunteers at their homes or workplaces. Similar to aviation data crowdsourcing, such as FlightRadar24 [4], our proposed network provides extensive live insights into COSPAS-SARSAT data, potentially from worldwide COSPAS-SARSAT distress beacons. Similarly, like the OpenSky network [5], [6], our network stores the raw 406

Workshop on Security of Space and Satellite Systems (SpaceSec) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-02-2
https://dx.doi.org/10.14722/spacesec.2026.23094
www.ndss-symposium.org

MHz distress beacon data in its database, allowing for further analysis and research, as well as enabling digital forensics and historical tracking when needed.

The system architecture of the proposed crowdsourcing for the COSPAS-SARSAT 406 MHz system is illustrated in Fig. 1. The sensors/receivers deployed by volunteers receive distress signals over 406 MHz frequency channels and forward them to the central system via the Internet in real-time. The central system manages all the registered sensors/nodes, receives, processes, and decodes the distress beacons, and subsequently makes the data available via the Web-UI dashboard and OpenAPI.

III. Preliminary Implementation

For implementation, we proposed that each SAR sensor node consists of a low-cost software-defined radio (e.g., RTL-SDR, HackRF), hosted on a low-power device (e.g., Raspberry Pi). The sensors continuously receive distress signals over the 406 MHz channel. When connected to the Internet, they forward the received distress data to the central system using Internet protocols, such as secure MQTT. Local nodes do not permanently store distress data, ensuring that data handling is managed centrally. In our minimal proof-of-concept implementation, we generated a bit stream of distress signals (EPIRB) following the protocol specification defined in [13]. We developed the GRC script to transmit the EPIRB distress signals, using HackRF, and received the distress signals using RTL-SDRs. For the experiments, we transmitted low-power local-range COSPAS-SARSAT compliant messages within a controlled environment using the 433 MHz unlicensed ISM band to minimize any potential regulatory and interference issues. To decode the received distress signals, we use *dump406* [11], [14] and then show the distress locations on a map using OpenStreetMap [15] (Fig. 2).

Regarding ethical and regulatory matters, our system works entirely passively. It receives, collects, and decodes data without interfering with critical SAR transmissions, and at no point does the proposed system/network transmit distress signals.

IV. Conclusion and Future Work

We presented the participatory crowdsourcing network for COSPAS-SARSAT 406 MHz distress beacons, where sensors deployed at volunteer locations receive and forward raw distress signals to the central system via Internet protocols. The central system collects, processes, decodes, stores, and makes the distress data available to the research community.

Future work aims to tackle several possible directions. One main direction is to extend the OpenSky Feeders to support the collection of COSPAS-SARSAT messages (i.e., from aircraft ELTs). This would require code contributions to OpenSky Feeder [16], and extensions to the setup instructions as well as to the OpenSky Raspberry Pi packages and images [17]. Another direction includes deploying real 406 MHz receiving nodes at volunteers' locations and establishing resilient communication channels to forward the received raw data from volunteers' receiving devices to the central system. This will enhance coverage mapping and the availability of raw data for further analysis and research activities. We plan to develop an API and make it available to the community and researchers, allowing them to access raw, aggregated datasets and thereby foster research activities.

Acknowledgment

Ahsan Saleem acknowledges Research Mobility Funding 2025, nominally awarded by the Faculty of Information Technology within the University of Jyväskylä. The authors thank Louis MIERMONT from IMDEA Networks Institute, Madrid, Spain for providing valuable feedback during the development of this work. The authors acknowledge the creators of the royalty-free icons used in Fig. 1 sourced from https://www.flaticon.com/ (icons by: Smashicons, Freepik, Assetwave).

References

[1] Maqsood Ahmed. Satellite-aided search and rescue (SAR) system. *IEEE Aerospace and Electronic Systems Magazine*, 22(8):3–8, 2007.

[2] D Levesque. The COSPAS-SARST system. In *IEE Colloquium on Satellite Distress and Safety Systems*, pages 3–1. IET, 1993.

[3] COSPAS-SARSAT Participants. https://www.cospas-sarsat.int/en/about-us/participants. (Access 22 Oct 2025).

[4] FlightRadar24. https://www.flightradar24.com/. (Access 24 Oct 2025).

[5] Matthias Schäfer, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, and Matthias Wilhelm. Bringing up OpenSky: A large-scale ADS-B sensor network for research. In *Proceedings of the 13th international symposium on information processing in sensor networks*. IEEE, 2014.

[6] Martin Strohmeier, Xavier Olive, Jannis Lübbe, Matthias Schäfer, and Vincent Lenders. Crowdsourced air traffic data from the OpenSky Network 2019–2020. *Earth System Science Data*, 13(2):357–366, 2021.

[7] Martin Strohmeier. Demonstration Abstract- OpenSky: A Large- scale ADS- B Sensor Network for Research. 2014.

[8] VesselFinder. https://www.vesselfinder.com/. (Access 24 Oct 2025).

[9] Andrei Costin and Aurélien Francillon. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *BlackHat USA*, 2012.

[10] Syed Khandker, Hannu Turtiainen, Andrei Costin, and Timo Hämäläinen. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. *IEEE Access*, 10:29493–29505, 2022.

[11] Andrei Costin, Syed Khandker, Hannu Turtiainen, and Timo Hämäläinen. Cybersecurity of COSPAS-SARSAT and EPIRB: threat and attacker models, exploits, future research. In *Workshop on Security of Space and Satellite Systems (SpaceSec)*, 2023.

[12] SARSAT System. https://www.sarsat.noaa.gov/wp-content/uploads/2024-SAR-WKSHOP_SARSAT-Overview.pdf. (Access 5 Nov 2025).

[13] SPECIFICATION FOR COSPAS-SARSAT 406 MHz DISTRESS BEACONS. https://www.cospas-sarsat.int/images/stories/SystemDocs/Current/T001-MAR-25-2022.pdf. (Access 24 Oct 2025).

[14] Andrei Costin Ahsan Saleem, Hannu Turtiainen, and Timo Hämäläinen. Towards message authentication and integrity for COSPAS-SARSAT 406 MHz distress beacons using lightweight ECDSA digital signatures.

[15] OpenStreetMap. https://www.openstreetmap.org/. (Access 5 Nov 2025).

[16] Feed Data to OpenSky. https://opensky-network.org/feed. (Access 5 Nov 2025).

[17] Raspberry Pi ADS-B Base Station for OpenSky Network. https://github.com/openskynetwork/raspberry-pi-adsb. (Access 5 Nov 2025).

Crowdsourcing and Mapping COSPAS-SARSAT 406 MHz Distress Beacons

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Ahsan Saleem[1] Andrei Costin[1] Guillermo Suarez-Tangil[2]

[1]University of Jyväskylä, Finland

[2]IMDEA Networks Institute Madrid, Spain

Abstract

In this work, we present the crowdsourcing and mapping of COSPAS-SARSAT 406 MHz distress signals, making distress data and information openly available to researchers and practitioners. The standard COSPAS-SARSAT 406 MHz distress system relies on centralized and officially operated satellites and ground stations, and no comparable (open-science/open-data) crowdsourcing and mapping networks exist.

To complement this, we propose a decentralized and publicly available crowdsourcing and mapping system for 406 MHz distress signals, enabling the independent research community to investigate the capacity, efficiency, applications, and security of these systems using real-world distress signals.

Contributions

- Propose the *first* (to the best of our knowledge) crowdsourcing and mapping system for COSPAS-SARSAT 406 MHz distress signals.
- Identify an essential gap to the COSPAS-SARSAT Threat Model by Costin et al. [11], and extend the model.

COSPAS-SARSAT Threat Model Extension

NEW THREAT VECTOR: Global COSPAS-SARSAT interference by jamming or spoofing CALBE and/or REFBE fixed beacons.

- COSPAS-SARSAT system relies on eight (8) fixed reference beacons (REFBE) and five (5) calibration beacons (CALBE) to monitor SAR performance and calibration.
- REFBEs assist in monitoring forward link service (FLS) and return link service (RLS).
- CALBEs provide precise, continuous time and frequency calibration for SAR/Galileo services.

Impact

- Targeted attack on CALBE and REFBE beacons can disrupt calibration, degrade performance, or accuracy of SAR operations.
- Spoof distress signals by placing devices near targeted REFBEs or CALBEs.
- Simultaneous attack on all fixed beacons would further exacerbate this issue.

Method

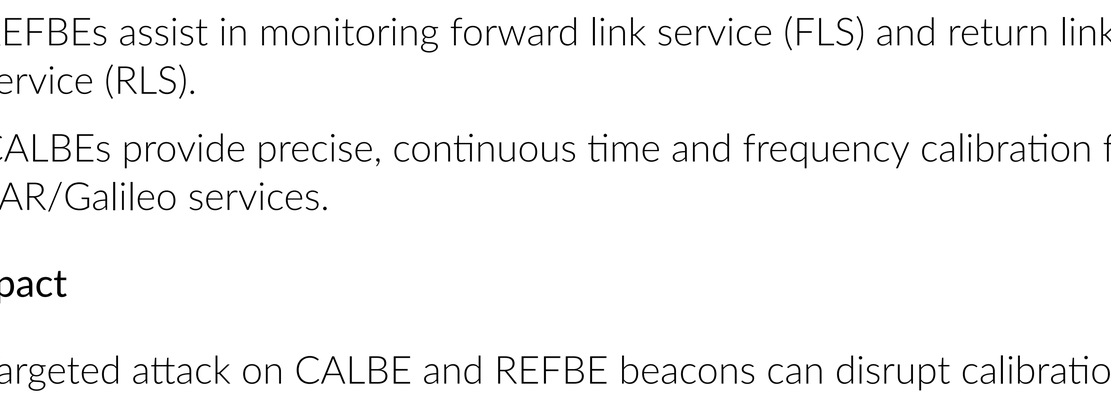

Figure 1. Proposed COSPAS-SARSAT crowdsourcing model

- Crowdsourcing network is a volunteer- or participant-based sensor network designed to collect, analyze, store, and visualize 406 MHz distress signals (Fig. 1).
- Central system manages all the registered nodes, receives, processes, and decodes the distress beacons.
- Stores the raw 406 MHz distress beacon data in its database, allowing for further research, digital forensics, and historical tracking.

Implementation, Evaluation and Results

- Each SAR sensor node uses low-cost SDR (RTL-SDR, HackRF), hosted on a low-power device (Raspberry Pi).
- Nodes passively receive COSPAS-SARSAT distress signals over the 406 MHz channel, forward data securely (e.g., via MQTT) to a central system.
- Proof-of-concept: Generated EPIRB signals, transmitted via HackRF, and received via RTL-SDRs.
- Experiments conducted at low-power local-range using 433 MHz ISM band in a controlled environment.
- Received data decoded with *dump406* and visualized on OpenStreetMap (Fig. 2).

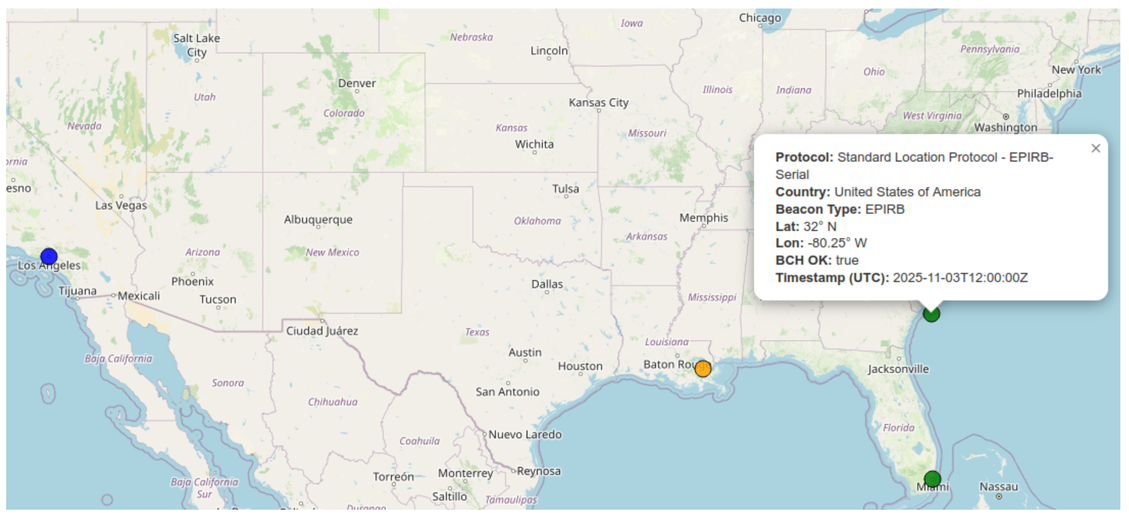

Figure 2. Demo of COSPAS-SARSAT 406MHz crowdsourcing

Ethical and regulatory matters: Fully passive system; does not transmit distress signals over 406 MHz, ensuring no interference with operational SAR services.

Applications

- **Coverage analysis.** Identify blind spots, weak beacon receptions.
- **Performance evaluation.** Analyze channel performance, message loss rate, RF interference, and bottleneck identification.
- **Error and fault diagnosis.** Detect errors, faults, or non-standard compliance of distress transmissions.
- **Security:** Detect spoofing, jamming, and interference; supporting researchers in developing backward-compatible hardening solutions.

Future Directions

- Extend OpenSky Feeders to support collection of COSPAS-SARSAT messages (i.e., from aircraft ELTs).
- Deploy real 406 MHz receiving nodes at volunteers' locations and establish resilient communication channels.

https://orcid.org/0000-0002-2704-9715

Scan for Papers