SyncScan: A Spectrum Monitor for Understanding Cellular Radio Access Network Deployments

Yingjing Wu
Kahlert School of Computing
University of Utah
Salt Lake City, Utah
wyj1993@cs.utah.edu

Dustin Maas
Kahlert School of Computing
University of Utah
Salt Lake City, Utah
dmaas@cs.utah.edu

Jacobus Van der Merwe
Kahlert School of Computing
University of Utah
Salt Lake City, Utah
kobus@cs.utah.edu

***Abstract*—Understanding spectrum use in cellular networks is important for efficient frequency allocation, base station deployment planning, and improving network performance through spectrum optimization and interference reduction. Gaining these insights requires systematic monitoring and analysis across multiple transmitters and carriers. Existing commercial spectrum monitoring tools have limitations, including high costs, delayed support for new technologies, closed architectures, and complex coordination requirements with equipment vendors for customized data collection. We present SyncScan, a spectrum monitoring system based on software-defined radios that provides a detailed view of cellular network deployments. SyncScan identifies active cells across frequency bands, decodes cell broadcast channels to extract configuration details correlates propagation measurements for transmitter localization, and tracks cells' spectrum usage patterns. Evaluation of SyncScan demonstrates its ability to generate comprehensive datasets about cellular network deployments. To facilitate research and innovation in spectrum monitoring, we have released SyncScan as open-source, enabling researchers and developers to extend and improve system functionality freely.**

***Index Terms*—Cellular, Spectrum monitoring**

I. Introduction

With the growth in mobile communication demands, the interference landscape in wireless networks becomes increasingly complex as operators deploy dense small cells to increase capacity [16], [38], new private networks are deployed, and research institutions try to use shared spectrum to develop and test new technologies [15], [26]. When interference-related performance degradation occurs, spectrum users face the challenge of accurately identifying interference sources and developing mitigation strategies, regardless of whether the interference originates from neighboring cells in adjacent channels or cells sharing the same frequency (co-channel interference). Addressing this challenge is necessary to realize the full potential of network densification and spectrum-sharing initiatives. Understanding interference sources and their configurations is crucial for effective spectrum management and reliable network performance. This requires spectrum monitoring tools capable of analyzing mobile network deployments and providing a comprehensive understanding of their configurations in terms of the spectrum usage patterns, locations, transmit powers, etc.

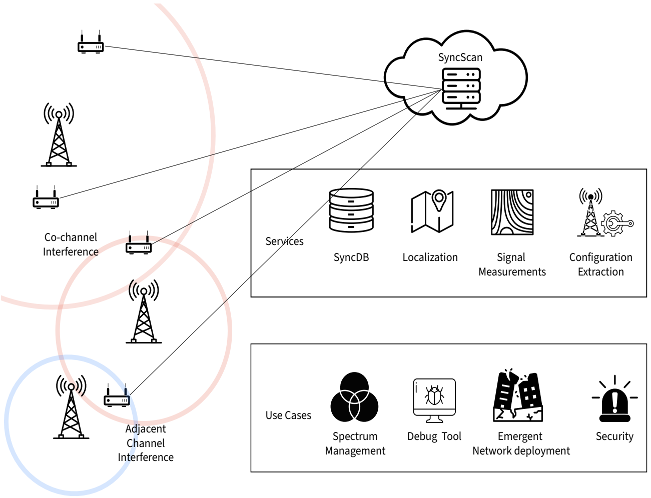


Fig. 1. SyncScan Applications and Use Cases in Spectrum Monitoring

Existing mobile network analysis tools have limitations that make each tool less than ideal for use in many situations. We list the capabilities of many such tools in Table I. Most solutions are restricted to accessing network information and signal measurements from specific mobile network operators (MNOs), and monitoring 5G networks is challenging due to device and platform compatibility. Furthermore, advanced spectrum analyzers capable of scanning large frequency ranges (multiple LTE/5G channels) do not provide transmitter localization information, making interference troubleshooting and network planning validation more complicated. The collected data are often incomplete, lacking transmitter configurations and usage patterns, limiting network operators' ability to verify deployment configurations and optimize spectrum use across carriers. In addition, commercial solutions typically have high costs and proprietary closed-source designs, which prevent users from tailoring data collection to their specific monitoring needs. More details on existing tools are explained in Section V-A. Consequently, with the growing adoption of spectrum sharing, there is a gap between current monitoring capabilities and the network insights needed for modern

This work was supported by the NSF through the following grants: #2232463 and #2346555.

spectrum management. This indicates a need for monitoring solutions that can identify signal sources, decode network configurations, and analyze temporal usage patterns.

In this paper, we present SyncScan, an open-source [1] spectrum monitoring and analysis system that provides comprehensive visibility into cellular network deployments. SyncScan operates as a passive sniffer using readily available software-defined radios (SDRs), enabling mobile network analysis without requiring MNO-specific SIM cards, or any other prior knowledge of the networks to be monitored. SyncScan listens for and identifies active cells in the frequency range it is asked to monitor, decodes broadcast channel messages that include useful network configuration parameters, and captures other useful radio signal metrics. In addition, SyncScan uses GPS-synchronized measurements collected from multiple locations to determine base station positions through signal propagation delay analysis. Finally, SyncScan is capable of extracting cell activity over long time durations, a capability motivated by the fact that MNOs often put "capacity" cells to sleep at periods of low demand in order to save energy and stand up temporary cells (so-called "cells on wheels") when required to meet short-term localized demands.

It is possible to deploy SyncScan on fixed infrastructure (e.g., in a large-scale wireless testbed like POWDER [4]) or as a portable solution that can be installed on laptops connected to small SDRs, allowing researchers and engineers to conduct real-time analysis and field measurements in a variety of scenarios. The system serves several important use cases. First, SyncScan enables network optimization by offering detailed spectrum usage data to MNOs. For example, when operators modify power levels, antenna configurations, and spectrum use [8], [10], [28], [32], SyncScan can provide real-time measurements for evaluating the impact of these changes on coverage and inter-cell interference. Second, SyncScan enhances monitoring capabilities in shared spectrum environments, e.g., within the Citizens Broadband Radio Service (CBRS) framework. For CBRS General Authorized Access (GAA) users operating without interference protection [34], SyncScan can provide network measurements that help operators and spectrum managers better understand the network landscape and identify/mitigate interference, leading to more reliable service. Third, SyncScan strengthens network security by providing detailed signal analysis capabilities. The system's measurements enable operators to detect and locate suspicious transmissions that could indicate security threats, allowing for rapid response when unauthorized signals are detected within the monitored area. Finally, SyncScan supports emergency response operations by providing critical spectrum awareness. During emergencies, first responders who may need to deploy their networks or rely on third-party networks can benefit from more complete information about the network landscape. SyncScan delivers detailed measurements of active cell locations, coverage patterns, and spectrum usage, enabling informed decisions about emergency communication service deployment.

TABLE I
CELLULAR NETWORK MONITORING TOOLS COMPARISON

Tool	No SIM Required	Band Scan	System configuration	Loc.	Open Source
SigCap	✗	✗	✓	✗	✗
QualiPoc	✗	✗	✓✓	✗	✗
Nemo	✗	✓	✓✓	✗	✗
PRiSM	✓	✓	✓✓	✗	✗
CellMapper	✗	✗	✓	✓	✗
KSMS	✓	✓	✓	✓	✗
SyncScan	✓	✓	✓✓✓	✓	✓

The key contributions of SyncScaninclude:

- Development of a mobile network monitoring system that integrates multiple useful capabilities into a unified platform, enabling cell identification, configuration decoding, and usage pattern analysis without requiring SIM cards or carrier support.
- Validation of precise base station localization through extensive drive test experiments. Our controlled evaluations demonstrate high accuracy, achieving an average localization error of 28 m for omnidirectional transmitters and 65 m for commercial base stations.
- Creation of an extensible open-source platform enabling community-driven development for commercial and academic applications.

The rest of this paper is organized as follows. Section II covers background on cellular networks and signal propagation. Section III details SyncScan's architecture, implementation, and replication summary. Section IV evaluates its performance and demonstrates the spectrum insights obtained. Section V reviews related work, and Section VI gives a conclusion and potential future work.

II. BACKGROUND

Each cellular radio access network (RAN) includes one or more base stations, each continuously broadcasting information about the network on specific parts of the radio spectrum. Since these broadcast messages must be transmitted in clear text to enable network discovery and access, passive monitoring systems like SyncScan can collect and analyze these messages to provide network intelligence. This section introduces the key technical concepts of cellular broadcast messages and signal propagation that enable such monitoring capabilities.

A. 5G Frame Structure and System Information

To organize radio transmissions efficiently, 5G networks employ a hierarchical frame structure. Each 10ms radio frame is divided into ten 1ms subframes, which are further subdivided into slots based on the subcarrier spacing (15, 30, 60, or 120 kHz). In Time Division Duplex (TDD) deployments, these slots are divided up for uplink and downlink transmissions, the ratio of which depends on the network configuration.

5G base stations transmit several broadcast messages in the downlink, three of which are illustrated in the spectrogram in

[1] SyncScan Code available at: https://gitlab.flux.utah.edu/wyj/syncscan

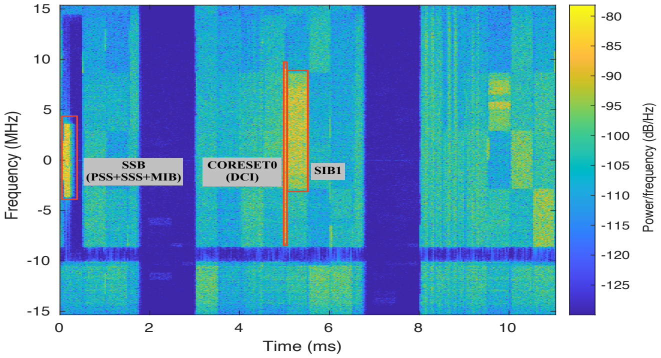


Fig. 2. 5G NR Signal Spectrogram with Key System Broadcast Components

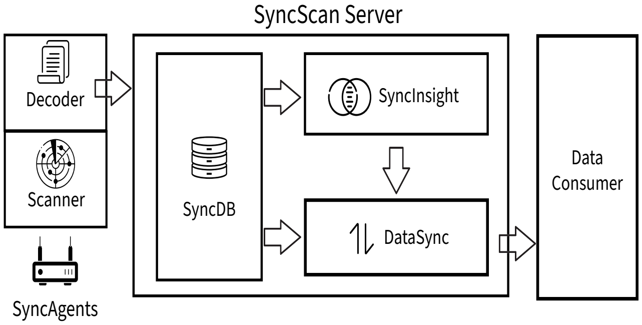


Fig. 3. SyncScan Components and Data Flow

Figure 2. The primary broadcast component is the Synchronization Signal Block (SSB), which contains three essential elements: the Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS), and Physical Broadcast Channel (PBCH) carrying the Master Information Block (MIB). These SSBs follow a periodic burst pattern in the time domain, repeating every 5, 10, 20, 40, 80, or 160 ms, depending on the cell's configuration. Within each SSB burst, up to 8 SSBs (for Frequency Range 1) or 64 SSBs (for Frequency Range 2) are transmitted with different SSB indices, where each index corresponds to a specific time position within the burst. In the frequency domain, these SSBs are centered at specific frequencies, called the synchronization raster, which are spaced at 1.44 MHz intervals for FR1 bands. Endpoints known as User Equipments (UEs) scan this raster, use the PSS/SSS to achieve time and frequency synchronization and then decode the MIB. The MIB parameters enable the device to locate the Control Resource Set Zero (CORESET0), which carries Downlink Control Information (DCI) indicating the time-frequency resources of System Information Block 1 (SIB1), which provides essential network configuration parameters, including cell identity, transmission power, and TDD uplink-downlink configuration pattern.

B. Signal Propagation

Among other radio channel effects, signals from base stations experience time delay and propagation power loss on their way to the UE. Several approaches have been developed to determine transmitter locations when designing RF-based localization systems. Traditional methods for single transmitter scenarios include Received Signal Strength (RSS) [21], Time of Arrival (ToA) [3], [36], Time Difference of Arrival (TDoA) [7], and Angle of Arrival (AoA) [23], [29], [35]. RSS methods estimate distance based on signal attenuation but are sensitive to environmental factors. ToA and TDoA achieve higher accuracy by measuring signal propagation time but require precise synchronization. AoA methods determine transmitter direction using antenna arrays but need line-of-sight conditions for best performance.

SyncScan uses a TDoA-based localization approach. The fundamental principle is that signal propagation delay is directly proportional to the distance traveled when signals propagate through space at the speed of light. We can measure the relative time delays between different signal sources by capturing signals with synchronized receivers at multiple locations. Through these time-difference measurements, we can establish a set of distance estimates and, in turn, estimate the transmitter's location using trilateration while accounting for practical challenges like multipath propagation and hardware-induced delays.

III. SyncScan Design

A. System Overview

SyncScan is designed as a distributed spectrum monitoring system consisting of two main components: SyncAgent and SyncScan Server, as illustrated in Figure 3. This architecture enables flexible deployment scenarios while maintaining centralized data processing and analysis capabilities for base station localization and understanding (in)activity patterns.

1) SyncAgent: The SyncAgent is installed on compute nodes that connect to SDRs and serves as the data collection unit. Each agent comprises three main modules working in concert to gather and process cellular network signals.

The signal acquisition module communicates with connected USRP devices (tested on X310 [13] and B210 [11]) through the UHD library [12] to capture base-band IQ samples. To ensure precise timing measurements, critical for transmitter localization, it employs synchronization mechanisms that align with the GPS clock and uses the PSS rising edge for accurate propagation delay measurements.

After signal acquisition, the Scanner processes the captured signals to identify active cells. The PSS Gold sequences are generated by OpenAirInterface (OAI) [30], and SyncScan populates these sequences across different frequencies and converts them to time-domain sequences. The Scanner then performs cross-correlation. The Scanner systematically searches all SSB raster frequencies within the frequency range of interest, accounting for different SSB intervals to identify potential cell candidates. For fixed monitoring deployments, SyncAgent operates with pre-configured location information, while in portable debug scenarios, it records GPS coordinates for each scan. The Scanner ranks cell candidates based on their correlation scores.

The Decoder is the final stage of agent-side processing, implementing the cellular signal decoding pipeline. Built on a modified version of parts of the OAI source code with enhanced CORESET0 search capabilities, the Decoder processes the captured IQ samples for each detected cell candidate. It outputs the decoded MIB and SIB1 messages from the Medium Access Control (MAC) layer. Together with the agent's coordinates, measured propagation delay, the cell's SSB frequency, and other data, these decoded messages form a comprehensive measurement record sent to the server for further processing.

2) SyncScan Server: The SyncScan Server functions as the system's central processing and analysis hub. At its core, the server comprises two main components: SyncScanDB for data storage and SyncInsight for data processing and analysis.

SyncScanDB implements a dual-structure design for efficient data organization. The agent-based records maintain raw measurement data, including agent locations, timestamps, and cell detection results from each monitoring point. The cell-based records provide a consolidated view of the network, where each unique cell entry contains its estimated location, configuration parameters, and aggregated measurements from all observing agents. This dual-structure design enables both detailed measurement tracking and efficient network-wide analysis.

SyncInsight serves as the system's analytical engine. Its primary functions include cell change detection, transmitter localization, and measurement aggregation. The change detection component monitors the cellular landscape for network modifications such as new cell deployments or deactivations. The localization component combines propagation delay measurements from multiple agents to estimate transmitter locations. The measurement aggregation component consolidates all agents' signal metrics and configuration data to maintain comprehensive cell status records. The server provides processed results to various external applications via the DataSync interface. These interfaces support queries based on time ranges, geographical areas, and cell identifiers, enabling different applications to access specific data based on their requirements.

3) Data Flow and Integration: SyncScan implements a periodic data processing pipeline between distributed agents and the central server, transmitting only the essential processed cell data and their associated SIB and MIB files. On the agent side, the system employs a systematic scanning approach that sequentially captures IQ samples at different center frequencies to cover the target frequency bands efficiently. If the SSB frequency differs from the capture center frequency for each captured band, the system performs frequency shifting on the IQ samples to decode the signal properly. Multiple processing pipelines (scanner, detector) share access to the SDR through a locking mechanism. While a pipeline needs to wait for its turn to acquire IQ samples from its target frequency band, once it obtains the samples, it can proceed with data processing independently while other pipelines continue waiting for their turn to access the SDR. This design enables pipelined processing where later stages of one capture can be executed in parallel with the acquisition of another IQ sample.

Operating at configurable intervals, agents send their processed measurement records to the server for analysis. Upon receiving new data, SyncInsight processes it through several sequential stages. The pipeline begins with change detection, comparing newly reported cells with existing records to identify network changes. For new cells, the system initiates localization calculations and creates database entries. The data fusion stage then consolidates measurements from multiple agents into a comprehensive cell-centric view, while maintaining historical records of network evolution.

Through the DataSync interface, external applications can query this processed data based on time ranges, geographical areas, and cell identifiers. This flexible access enables various use cases from network optimization to coverage analysis, while the historical records provide insights into network evolution over time.

B. System Implementation

1) Band Scanning and Cell Detection: The cell search process involves scanning for SSBs transmitted at standardized frequency positions known as SSB rasters - predefined intervals where synchronization signals can be located in 5G NR networks. Rather than capturing IQ samples at each individual SSB raster frequency, the process captures a broad bandwidth segment at once, with the segment width determined by the SDR's maximum reliable sample rate (i.e., the rate at which the SDR can operate without adding RF impairments, and at which the host running the SyncAgent can reliably consume the IQ samples). Since this maximum sample rate limits the bandwidth that can be captured in a single scan, multiple overlapping captures are necessary. Each new capture overlaps partially with the previous one to ensure no potential SSBs at raster points are missed at the segment boundaries. For each captured bandwidth segment, PSS detection involves placing pre-generated PSS sequences at all possible SSB raster frequencies within this captured bandwidth. These sequences are transformed into time domain sequences through FFT, followed by cross-correlation between these time sequences and the IQ samples from two subframes. The time sequences associated with high correlation score lags reveal both the temporal and frequency domain positions of potential active cells' PSS. Potential active cells with their PSS correlation peak positions are then ranked in a max heap based on their PSS correlation scores, prioritizing verification of the highest-scoring candidates. Verification involves decoding the SSS followed by the MIB message. Since IQ samples are collected from a wide bandwidth rather than centered at each cell's SSB frequency, frequency shift compensation is necessary during this verification process. This approach represents a more efficient method than tuning the SDR to every possible SSB raster frequency and decreases the number of IQ sample collection operations.

2) Transmitter Localization: Base stations in cellular networks typically employ a multi-sector architecture, where each base station operates multiple cells facing different directions. Within an operator's network, these sectors may share the same SSB index, creating signal overlays in boundary areas or use different SSB indices. Accurate base station localization requires first identifying and grouping all cells belonging to the same base station. SyncScan accomplishes this by extracting cell identity information (gNodeB ID and sector ID) from decoded SIB1 messages, allowing cells with the same gNodeB ID to be recognized as sectors of the same base station.

For localization through signal propagation delay measurements, all SyncScan agents must share a standard time reference through GPS synchronization at measurement locations. During signal processing, SyncScan measures the PSS peak offset, which includes both propagation delay and non-propagation delay (primarily processing delay from hardware and software). For ToA localization, when the transmitter's clock is synchronized with GPS time, SyncScan must carefully calibrate and exclude all non-propagation delays to obtain an accurate signal travel time. Alternatively, SyncScan can use TDoA techniques, which inherently cancel out common delays. However, when using TDoA with measurements from different devices, accuracy may be affected since different devices can have varying processing delays, while measurements from a single SyncAgent (in portable debug scenarios) ensure consistent processing delay across samples.

C. Replication Summary

SyncScan operates in two distinct modes: as a portable debug tool (SyncScanMenu) for field testing on individual nodes and as a distributed monitoring system (SyncScan-Monitor) across multiple nodes. The portable configuration utilizes B210 or X310 SDR with GPSDO and GPS antennas for accurate positioning and time synchronization, enabling real-time spectrum analysis in field settings. In contrast, the distributed system leverages the POWDER infrastructure with rooftop nodes comprising d430/d740 servers paired with B210 or X310 and WhiteRabbit clocks for synchronization across different locations. To replicate the portable mode, users must connect an SDR to a computer with SyncScan installed from the source, attach a GPS antenna with clear sky visibility, wait for GPSDO lock, and launch SyncScanMenu with proper frequency settings. For the distributed system, users need to reserve POWDER resources using the provided profile[2], SSH into allocated nodes, follow profile instructions to build the required OAI library and SyncScan code, deploy SyncScan Server on one compute node and SyncAgents across all SDR nodes, configure monitoring parameters, and collect synchronized spectrum data, with successful implementation showing nano-second time synchronization accuracy, signal measurements, spectrum utilization and detected cells' locations.

IV. Evaluation

We evaluate the performance of SyncScan across several key dimensions, including localization accuracy, dynamic cell activity detection, deployment considerations, and computational performance. Our evaluation validates the system's technical capabilities and its practical value for spectrum monitoring.

A. Cell Detection and Localization

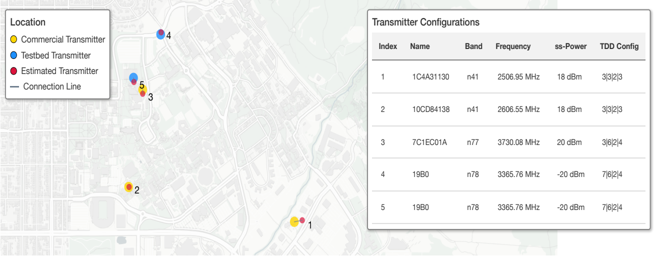
This section evaluates SyncScan's capability to identify and locate active cells across a university campus environment, including commercial and experimental base stations deployed using the POWDER testbed.

Experiment Setup: To evaluate SyncScan's detection and localization capabilities, we conducted field tests using a portable USRP B210 as our measurement device. Our test environment consisted of three commercial 5G cells, which use GPS-synchronized timing per standard specifications, and two testbed gNodeBs on campus that we also configured with GPS synchronization. Measurements were collected at various distances (28-311 meters) under Line-of-Sight conditions. Since our measurement device also uses a GPS clock, this shared GPS synchronization between transmitters and receivers enables accurate localization by measuring time offsets between expected and actual arrival times of broadcast messages. For transmitters not synchronized to GPS time, localization requires multiple synchronized SyncAgents deployed simultaneously to measure propagation delays. Using a single device to collect measurements at different locations and times is not feasible for such transmitters due to clock drift. While SyncScan maintains its capability to decode and extract system information regardless of synchronization status, these timing requirements are essential for accurate propagation delay-based positioning.

Ground Truth: For our evaluation, we established reliable ground truth through multiple verification methods. For our testbed nodes, locations were precisely known as they were under our direct control. We employed a comprehensive verification process for commercial cells: First, we obtained initial location data from the antenna search database [2]. We then confirmed these locations through visual inspection, including physical site visits and Google Street View verification to identify cellular equipment such as cylindrical antenna enclosures. Finally, using the Nemo tool, we validated each location through signal analysis, walking circular patterns around suspected locations while monitoring sector changes and signal strength variations. We also validated the accuracy of our system information decoding. We directly verified the decoded information with testbed nodes against the known gNodeBs' configurations, as we had complete control over these parameters. We cross-referenced our results for commercial cells with the industry-standard Nemo tool, which provides reliable MIB and SIB message decoding.

Results: We extracted and verified several key parameters for each cell from the decoded system information. These include the cell ID, operating frequency bands, SSB frequency, synchronization signal transmission power (SS-Power), and

[2] SyncScan POWDER profile avaliable at https://gitlab.flux.utah.edu/wyj/syncscan_powder



Transmitter Configurations

Index	Name	Band	Frequency	ss-Power	TDD Config
1	1C4A31130	n41	2506.95 MHz	18 dBm	3|3|2|3
2	10CD84138	n41	2606.55 MHz	18 dBm	3|3|2|3
3	7C1EC01A	n77	3730.08 MHz	20 dBm	3|6|2|4
4	19B0	n78	3365.76 MHz	-20 dBm	7|6|2|4
5	19B0	n78	3365.76 MHz	-20 dBm	7|6|2|4

Fig. 4. Transmitter Mapping and Configuration Summary from SyncScan Deployment

TABLE II
LOCALIZATION ERROR SUMMARY

Site ID	Samples Distance Range (m)	Min Error (m)	Max Error (m)	Average Error (m)
Site 1	48-311	66.28	154.77	107.88
Site 2	46-173	15.61	34.68	28.55
Site 3	73-230	28.91	162.34	57.71
Site 4	36-107	3.82	48.78	25.77
Site 5	28-87	8.87	114.75	30.08

TDD configuration. The TDD configuration details the temporal resource allocation through the number of uplink slots, uplink symbols, downlink slots, and downlink symbols. Our verification process confirmed that SyncScan accurately decoded all these parameters, demonstrating its reliability in extracting critical system information from commercial and testbed deployments.

Our localization accuracy evaluation encompassed five cell sites: three commercial base stations (Sites 1-3) and two testbed installations (Sites 4-5). Each commercial site comprised multiple sectors deployed on building rooftops to provide directional coverage. The testbed installations achieved high accuracy with average errors of 25.77 m and 30.08 m, respectively, benefiting from our ability to collect Line-of-Sight (LOS) measurements with the entire angular span. Site 2 achieved comparable precision among commercial sites with an average error of 28.55 m. Site 3 showed a higher variance with an average error of 57.71 m, while Site 1 recorded the most significant average error of 107.88 m. The notably higher error for Site 1 stemmed from limited measurement coverage, as environmental constraints restricted measurements to approximately 240 degrees around the site.

Considerations and Limitations: Our localization is based on the TDoA approach, requiring at least four geographically distributed measurement points for triangulation. The accuracy of this method strongly depends on the geometric distribution of these measurements. When measurements are limited to a narrow angular sector, location estimates become less reliable and must be excluded from our calculations. This limitation was particularly evident for Site 1, where restricted angular coverage led to more rejected estimates and reduced overall accuracy. While we demonstrated localization accuracy as good as 25-30 m under optimal conditions, several factors can affect performance, including multipath propagation and shadowing effect. Additionally, potential timing offsets between sectors within the same base station need to be considered, as they may affect measurement consistency.

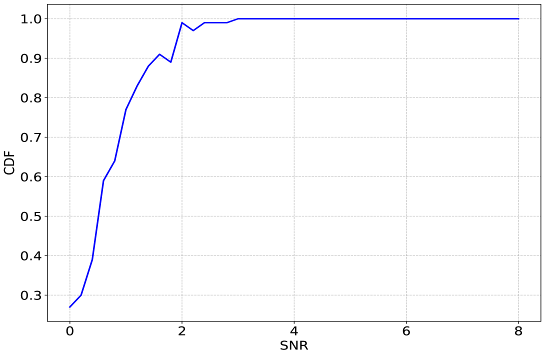


Fig. 5. SIB1 decoding success rate versus SNR. The CDF shows SyncScan achieves more than 99% successful decoding at SNR levels above 3 dB.

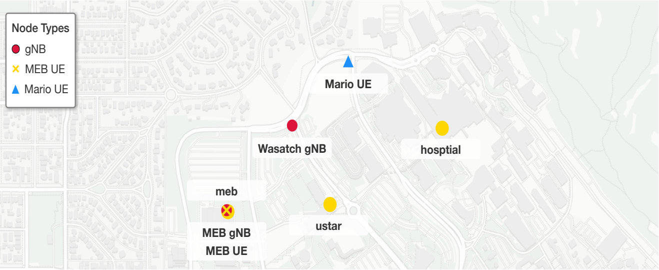


Fig. 6. Deployment for cellular activity observation and pattern analysis on POWDER testbed.

B. Deployment consideration

Successful SIB1 decoding is crucial for cell configuration tracking and base station localization. SIB1 contains essential cell configuration parameters and the gNodeB ID, which is necessary for grouping related sectors since PCIs from sectors of the same station may not be contiguous. The decoding process requires sequential success in multiple steps - PBCH, Coreset0, and SIB1 decoding - where failure at any stage prevents successful SIB1 recovery. To guide monitor deployment strategy that ensures reliable SIB1 decoding, we evaluated decoding performance across varying signal-to-noise ratio (SNR) conditions to determine the effective detection range. Our results show that successful SIB1 decoding achieves 99% success at SNR levels above 3 dB, where SNR is measured as the average power over the entire band across a time interval rather than channel-specific SNR measurements. We can estimate the spacing between monitoring locations using this SNR threshold, together with the transmission power obtained from system information and appropriate propagation models. This spacing requirement, combined with the need for geometric diversity in localization measurements, guides optimal monitor placement strategies, which can be further refined by considering specific propagation characteristics of the deployment area.

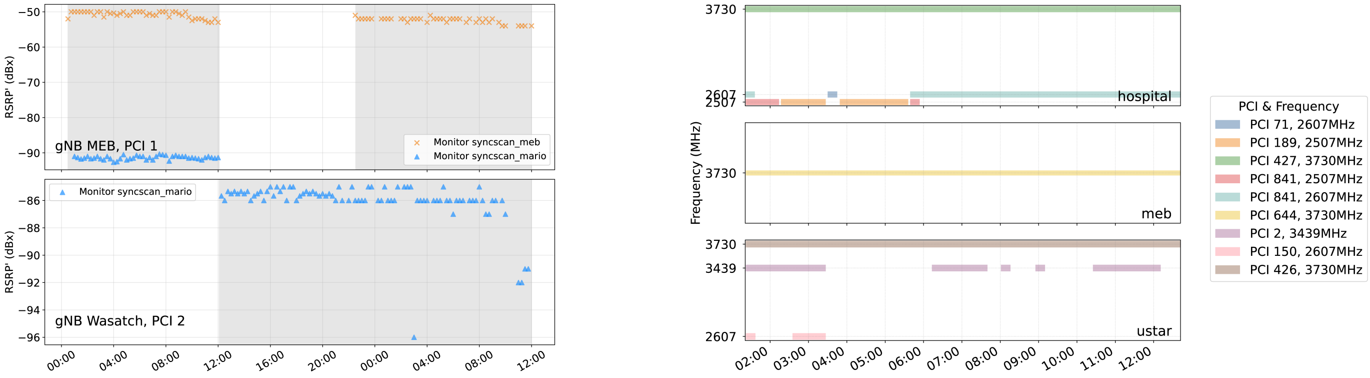


Fig. 7. The left side illustrates a controlled experiment designed to verify the functionality of SyncScan by monitoring transmissions in a known setup. The right side shows real spectrum observations, where SyncScan monitors ongoing activity from different PCIs over time.

C. *Cell's Activity Pattern Extraction*

We conducted controlled experiments on the POWDER testbed to validate SyncScan's ability to detect cell activity patterns accurately. We deployed two monitors on Mario UE and MEB UE and two gNodeBs (gNBs) on MEB gNB and Wasatch gNB as shown in Figure 6, both operating on the same frequency but with different PCIs. The cell activity was tracked through relative Synchronization Signal Reference Signal Received Power (RSRP) measurements (not calibrated). In our sequential activation test, we first activated the MEB gNB, which both monitors successfully detected. When we switched operations from MEB to Wasatch gNB, only the Mario UE detected the signal, probably due to distance or NLOS conditions on the MEB UE. Finally, with both gNBs active, the MEB UE detected only the MEB gNB, while on the Mario UE, the strong signal from the nearby Wasatch gNB dominated and prevented detection of the weaker MEB gNB signal, demonstrating the capture effect. By tracking the presence or absence of RSRP measurements, SyncScan successfully determined each cell's active/inactive state. The delay in detecting state changes depends on our configured monitoring periodicity, which can be adjusted based on the monitoring requirements.

In a real-world deployment scenario, we installed our spectrum monitoring system at three different campus locations to monitor active commercial 5G networks over 12 hours across frequencies from 2490-3825 MHz. The monitor on the hospital node detected multiple interesting patterns. At 2506 MHz, we observed signals from two different PCIs. Through field test localization, we confirmed that these signals originated from two physically separated cells operating in the same area, where signal strength competition led to our monitor alternately detecting one cell or the other based on their relative signal strengths. This capability to track multiple cells could help detect security anomalies, such as fake base station attacks or unexpected cell outages. Additionally, on the same node, we observed an interesting pattern where a 2606 MHz cell was no longer detected after 1:00 AM, coinciding with the detection of a 2506 MHz cell until approximately 6:00 AM. These cells shared the same PCI and exhibited identical PSS peak offsets. Since these cells operated on different frequencies and no other cells were detected during the transition periods, signal interference can be ruled out. Furthermore, these observations, combined with the consistent pattern across several nights, strongly suggest they originated from the same transmitter switching between frequencies during low-traffic hours, possibly as part of the operator's dynamic spectrum management strategy.

D. *Computational Performance*

Our evaluation used two different hardware setups, each with a software-defined radio. We deployed our system on a platform with an Intel Xeon E5-2630 v3 processor connected to a USRP X310 SDR with a WhiteRabbit clock for fixed-location continuous monitoring. The portable setup, serving as a mobile debug tool for field testing, combines an Intel i7-1355U processor laptop with a USRP B210 SDR and GPS clock. Both setups use identical SDR configurations, collecting IQ samples at a 30.72 MSps sampling rate and scanning a 30 MHz bandwidth for each scan.

The system performance was evaluated using five key metrics. Sample Collection measures the time required to collect IQ samples over a 2-second. Band Scan measures the time needed to read 1ms of samples from a file, generate PSS sequences, and apply PSS correlation to detect potential active cells in the captured band. System Info Decoding Time captures the processing duration required to decode system information from one subframe, including PBCH decoding, DCI decoding, SIB1 decoding, SIB1 message parsing, and saving. For continuous monitoring deployments, End-to-End SyncAgent Latency measures the total processing time from initiating a band scan to obtaining the final output, which includes scanning a 90 MHz band, detecting one active cell, and searching 20 subframes to decode one SIB1 subframe (considering SIB1's periodicity of 16 subframes). Note that end-to-end timing for the debug tool setup is not measured as it includes interactive features such as spectrogram display and manual cell selection from detected candidates. Finally,

TABLE III
SYSTEM PERFORMANCE METRICS ON DIFFERENT COMPUTING PLATFORMS

Specific Metric	**Description**	**i7-1355U**	**Xeon E5-2630 v3**
Sample Collection	Time required to collect IQ samples (30.72 MSps × 2s)	2.46 s	3.24 s
Band Scan	Time to scan 30 MHz bandwidth for cell detection	0.423 s	0.525 s
System Info Decoding Time	Processing time to decode system information in one subframe	1.32 s	3.59 s
End-to-End SyncAgent Latency	Total time from scanning three 30 MHz band to output	/	181.61 s
Localization Time	Time from initial detection to location estimate	6.86 ms	15.2 ms

Localization Time represents the duration from initial cell detection to generating a location estimate based on the decoded information. Table III breaks down the computational overhead of SyncScan's core components and presents the end-to-end execution time when the monitor scans three 30 MHz frequency bands. Our current implementation focuses on functionality rather than performance, leaving room for future optimization.

V. RELATED WORK

A. Cellular Network Monitoring Tools

Understanding spectrum usage in cellular networks can be approached from different perspectives, leading to various monitoring tools. Current tools can be broadly categorized based on data collection methods and capabilities.

The first category relies on network APIs to collect information. Commercial solutions like SigCap [33], QualiPoc [31], and Nemo [18] require SIM cards and utilize either provider APIs or Telephony API [1] for data collection. QualiPoc and Nemo leverage commercial APIs to access detailed system configurations but can only monitor their associated carriers' networks. SigCap, operating through basic Telephony API, provides even more limited configuration information. The key limitation of API-based approaches is their dependency on carrier authentication and restricted access to network information. Moreover, none of these tools offer localization capabilities.

The second category performs spectrum scanning to monitor cellular signals directly. PRiSM [9] represents this approach, operating without SIM card requirements and capable of scanning frequency bands to detect active signals. However, it provides limited system configuration information and cannot also correlate signals with their sources. Additionally, as a proprietary solution, it cannot be customized for specific monitoring needs.

Crowdsourced platforms like CellMapper [6] attempt to combine multiple data sources by aggregating network measurements from user devices. While this enables broader coverage mapping and cell tower localization, these platforms still face fundamental limitations. They rely on API-accessible information, require SIM cards, and struggle with data completeness and currency, particularly for 5G networks where API support varies across device platforms.

These limitations in existing tools highlight the need for a more comprehensive approach to spectrum monitoring - one that can independently discover and analyze cellular signals without relying on carrier access or API restrictions. This motivates the development of more sophisticated monitoring systems that can directly decode cellular signals and extract detailed configuration information from the air interface.

B. Cellular Network Sniffers

Like spectrum monitoring tools, cellular network sniffers also decode signals from cellular networks, but they serve a fundamentally different purpose. While spectrum monitoring tools focus on understanding the overall spectrum usage patterns and transmitter characteristics, sniffers aim to analyze the efficiency of radio resource allocation for individual cells.

In the 4G domain, LTEye [20] pioneered passive monitoring by developing techniques to decode LTE downlink control channels, enabling analysis of resource block allocation patterns and scheduling decisions. OWL [5] and FALCON [14] further enhanced these capabilities by improving decoding reliability and adding support for more detailed resource utilization analysis. A significant advancement came with LTESniffer [17], which provides passive decoding capabilities for both uplink and downlink traffic, offering comprehensive insights into how individual cells manage their radio resources.

The transition to 5G introduced new challenges for network sniffing due to more complex frame structures and enhanced security measures. 5GSniffer [22] successfully addresses these challenges by decoding the Physical Downlink Control Channel (PDCCH) in real-time through innovative techniques, including encoding redundancy analysis and side-channel information utilization. However, unlike spectrum monitoring tools that scan frequency bands to discover active cells, 5GSniffer requires knowledge of cell frequencies and configurations to function effectively.

In contrast, spectrum monitoring tools like SyncScan prioritize cell discovery and basic configuration decoding across wide frequency ranges. SyncScan actively scans frequency bands to locate cells and decode their basic configurations, making it more suitable for understanding overall spectrum usage patterns. Additionally, SyncScan provides a localization function that enables the determination of transmitter locations, further enhancing its spectrum monitoring and network planning capabilities.

C. Cell Tower Localization

For scenarios involving multiple transmitters, RSS-based approaches have gained particular attention due to their practical advantages. However, these methods require to first associate measurements with their corresponding transmitters. In known transmitter scenarios, where each RSS measurement can be mapped to a specific transmitter (e.g., through cell IDs), the coverage regions are naturally partitioned based on the identified signals. In [37], authors leveraged this advantage in cell tower localization using wardriving data, where measurements were already associated with specific cell IDs. For unknown transmitter scenarios where signal sources cannot be identified, the problem becomes more complex. Approaches like [27] and SPLOT [19] must rely on RSS thresholds to artificially partition coverage regions and associate measurements with different transmitters. This threshold-based separation introduces potential errors, as signal strength can be affected by various environmental factors. There are also many ML-based approaches for RSS-based localization [24], [39]. However, temporal differences between training and testing data collection can significantly impact localization accuracy, as environmental changes over time can cause fluctuations in RSS measurements, leading to a mismatch between training and testing data. In [25], authors demonstratesd how incorporating context through model confidence enables hybrid localization, thereby improving localization accuracy.

SyncScan taking the advantage of cellular network synchronization characteristic, uses TDoA-based localization approach. By decoding SSB messages, it directly obtains transmitter identities without relying on either predefined coverage regions or RSS thresholds. This identity information solves the signal association problem that plagues RSS-based methods. With guaranteed signal association through decoded identifiers, SyncScan can then apply TDoA techniques to the synchronized SSB transmissions, combining the accuracy advantages of time-based methods with reliable transmitter identification.

VI. Conclusion and Future work

SyncScan is an open-source software-defined radio solution for mobile network spectrum monitoring. It addresses the limitations of current commercial tools and the lack of open-source network intelligence tools, providing researchers with a feature-rich and flexible alternative. SyncScan enables systematic monitoring of multiple transmitters and carriers, offering key capabilities such as cell identification, parameter extraction, transmitter localization, and spectrum usage analysis. The data obtained through SyncScan can be used to optimize network deployments, enhance user experiences, reduce operational costs, and inform spectrum allocation decisions.

In future work, we will validate our approach in diverse network environments and expand monitoring capabilities to include diverse wireless signals such as LTE and WiFi, further demonstrating its generalizability. We intend to optimize performance to minimize processing overhead on monitoring devices. We will establish clearer connections between cell activity patterns and end-user experience by integrating QoS metrics. In addition, we plan to compare our system with existing monitoring tools to identify its comparative advantages and limitations better. These enhancements will strengthen our approach's scientific contribution and practical applications.

References

[1] Android Developers. Telephony provider. https://developer.android.com/reference/android/provider/Telephony. Accessed: 2024-10-28.

[2] AntennaSearch. Search for cell towers and antenna locations.

[3] Amir Beck, Petre Stoica, and Jian Li. Exact and approximate solutions of source localization problems. *IEEE Transactions on signal processing*, 56(5):1770–1778, 2008.

[4] Joe Breen, Andrew Buffmire, Jonathon Duerig, Kevin Dutt, Eric Eide, Mike Hibler, David Johnson, Sneha Kumar Kasera, Earl Lewis, Dustin Maas, et al. Powder: Platform for open wireless data-driven experimental research. In *Proceedings of the 14th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, pages 17–24, 2020.

[5] Nicola Bui and Joerg Widmer. Owl: A reliable online watcher for lte control channel measurements. In *Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges*, pages 25–30, 2016.

[6] CellMapper. Cellmapper. https://www.cellmapper.net/map. Accessed: 2024-10-28.

[7] Yiu Tong Chan and Kenneth C Ho. A simple and efficient estimator for hyperbolic location. *IEEE transactions on signal processing*, 42(8):1905–1915, 1994.

[8] Cisco Systems. *Cisco Spectrum Expert User Guide*, 2024. Version 4.1.

[9] Epiq Solutions. Prism integrated system. https://epiqsolutions.com/products/integrated-systems/prism. Accessed: 2024-10-28.

[10] Ericsson. Optus to further improve 5g customer experience with the introduction of ericsson's 5g advanced interference sensing feature, 2024. Accessed: 2024-10-31.

[11] Ettus Research. Usrp b210 usb software defined radio. https://www.ettus.com/all-products/ub210-kit/. Accessed: 2024-02-01.

[12] Ettus Research. Usrp hardware driver (uhd). https://github.com/EttusResearch/uhd. Accessed: 2024-02-01.

[13] Ettus Research. Usrp x310 software defined radio. https://www.ettus.com/all-products/x310-kit/. Accessed: 2024-02-01.

[14] Robert Falkenberg and Christian Wietfeld. Falcon: An accurate real-time monitor for client-based mobile network data analytics. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2019.

[15] Federal Communications Commission. Notice of Proposed Rulemaking and Order. https://docs.fcc.gov/public/attachments/DOC-354370A1.pdf, 2018. Accessed: 2024-10-31.

[16] GSMA. Small cells: Big opportunity for efficient networks in the 5g era, 2022. Accessed: October 30, 2024.

[17] Tuan Dinh Hoang, CheolJun Park, Mincheol Son, Taekkyung Oh, Sangwook Bae, Junho Ahn, Beomseok Oh, and Yongdae Kim. Ltesniffer: An open-source lte downlink/uplink eavesdropper. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 43–48, 2023.

[18] Keysight Technologies. Nemo outdoor 5g nr drive test solution. https://www.keysight.com/us/en/product/NTA50000B/nemo-outdoor-5g-nr-drive-test-solution.html. Accessed: 2024-10-28.

[19] Mojgan Khaledi, Mehrdad Khaledi, Shamik Sarkar, Sneha Kasera, Neal Patwari, Kurt Derr, and Samuel Ramirez. Simultaneous power-based localization of transmitters for crowdsourced spectrum monitoring. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 235–247, 2017.

[20] Swarun Kumar, Ezzeldin Hamed, Dina Katabi, and Li Erran Li. Lte radio analytics made easy and accessible. *ACM SIGCOMM Computer Communication Review*, 44(4):211–222, 2014.

[21] Xinrong Li. Rss-based location estimation with unknown pathloss model. *IEEE Transactions on Wireless Communications*, 5(12):3626–3633, 2006.

[22] Norbert Ludant, Pieter Robyns, and Guevara Noubir. From 5g sniffing to harvesting leakages of privacy-preserving messengers. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3146–3161. IEEE, 2023.

[23] Estifanos Yohannes Menta, Nicolas Malm, Riku Jäntti, Kalle Ruttik, Mário Costa, and Kari Leppänen. On the performance of aoa–based localization in 5g ultra–dense networks. *Ieee Access*, 7:33870–33880, 2019.

[24] Frost Mitchell, Aniqua Baset, Neal Patwari, Sneha Kumar Kasera, and Aditya Bhaskara. Deep learning-based localization in limited data regimes. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning*, pages 15–20, 2022.

[25] Frost Mitchell, Jie Wang, Aditya Bhaskara, and Sneha Kumar Kasera. Utilizing confidence in localization predictions for improved spectrum management. In *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 483–492. IEEE, 2024.

[26] National Telecommunications and Information Administration. Spectrum Sharing Innovation Test-Bed Pilot Program Final Report. Technical report, National Telecommunications and Information Administration, 2023. Accessed: 2024-10-31.

[27] Jill K Nelson, Maya R Gupta, Jaime E Almodovar, and William H Mortensen. A quasi em method for estimating multiple transmitter locations. *IEEE Signal Processing Letters*, 16(5):354–357, 2009.

[28] NETSCOUT. NETSCOUT and Vodafone Extend Relationship Through Multi-Year Network Monitoring Agreement, 2024. Accessed: 2024-10-31.

[29] Dragos Niculescu and Badri Nath. Ad hoc positioning system (aps) using aoa. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, volume 3, pages 1734–1743. Ieee, 2003.

[30] OpenAirInterface Software Alliance. Openairinterface: 5g software stack for 3gpp nr ran. https://gitlab.eurecom.fr/oai/openairinterface5g/, 2024. Accessed: 2024-02-01.

[31] Rohde & Schwarz. Qualipoc. https://www.rohde-schwarz.com/us/products/test-and-measurement/network-data-collection/qualipoc-android_63493-55430.html. Accessed: 2024-10-28.

[32] Rohde & Schwarz. China's Mobile Network Operators Select Test Scanners from Rohde & Schwarz for 5G Network Optimization, 202. Accessed: 2024-10-31.

[33] Vanlin Sathya, Muhammad Iqbal Rochman, and Monisha Ghosh. Measurement-based coexistence studies of laa & wi-fi deployments in chicago. *IEEE Wireless Communications*, 28(1):136–143, 2020.

[34] Armed Tusha, Seda Dogan-Tusha, Hossein Nasiri, Muhammad Iqbal Rochman, Patrick McGuire, and Monisha Ghosh. A comprehensive analysis of secondary coexistence in a real-world cbrs deployment. In *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 79–87. IEEE, 2024.

[35] Carl Wong, Richard Klukas, and Geoffrey G Messier. Using wlan infrastructure for angle-of-arrival indoor user location. In *2008 IEEE 68th Vehicular Technology Conference*, pages 1–5. IEEE, 2008.

[36] Enyang Xu, Zhi Ding, and Soura Dasgupta. Source localization in wireless sensor networks from signal time-of-arrival measurements. *IEEE Transactions on Signal Processing*, 59(6):2887–2897, 2011.

[37] Jie Yang, Alexander Varshavsky, Hongbo Liu, Yingying Chen, and Marco Gruteser. Accuracy characterization of cell tower localization. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, pages 223–226, 2010.

[38] Seung Min Yu and Seong-Lyun Kim. Downlink capacity and base station density in cellular networks. In *2013 11th international symposium and workshops on modeling and optimization in mobile, ad hoc and wireless networks (WiOpt)*, pages 119–124. IEEE, 2013.

[39] Anatolij Zubow, Suzan Bayhan, Piotr Gawłowicz, and Falko Dressler. Deeptxfinder: Multiple transmitter localization by deep learning in crowdsourced spectrum sensing. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–8. IEEE, 2020.