Poster: Towards Simultaneous Attacks on Multiple Cellular Networks

Alexander Ross
NC State University
ajross6@ncsu.edu

Bradley Reaves
NC State University
bgreaves@ncsu.edu

***Abstract*—Cellular network attack research has dramatically expanded its capabilities in the last decade, but threat models routinely assume an attacker who targets a single cell with a small number of moderately-priced software defined radios. In many settings, such as mass crowd surveillance, attackers seek to gain passive or active dominance over a given area that is virtually always served by multiple cells and network operators. To do so, the only method publicly available is to naïvely duplicate their hardware at extensive cost. This paper presents a preliminary analysis of the feasibility of using a single software defined radio to surveil multiple networks simultaneously. Our key insight is that an attacker is often interested in only a portion of transmissions in a cell, and by design cellular transmissions are rigidly and predictably scheduled. Our system, Intercellular, rapidly schedules a single radio to tune between cells, effectively multiplexing the downlink channels of cells together. We demonstrate that radio tuning time is quite low (around 100ms), radio clocks are sufficiently stable to skip synchronization when retuning, and that even when monitoring multiple cells a radio can quite accurately count the devices served by all cells under observation. In so doing, we open new research directions advancing the efficiency and broad applicability of cellular network attacks.**

Keywords*—*Cellular Networks, Cellular Network Attacks

I. Extended Abstract

Cellular networks are critical infrastructure for nearly every aspect of life, and researchers have analyzed these networks to find vulnerabilities, demonstrate attacks, and propose fixes. The advent of software defined radios (SDRs) and open-source air interface implementations democratized cellular attack research. SDRs in particular significantly lowered the cost barrier to entry, and they put cellular attacks within reach of academic researchers and attackers alike. Compared to the extreme costs of the custom hardware and software previously required for cellular research, SDRs are remarkably affordable.

SDRs are still costly, though, with the higher end equipment costing thousands of dollars per unit. Accordingly, labs have few such radios for attack research, and attacks that target a single cell comprise practically all published work to-date. Unfortunately, the well-funded actors who actually conduct large-scale attacks apparently have no such limitations [1]. This leaves researchers who work on attacks and defenses "out-gunned" and unable to work within state-of-the-art threat models. Simply put, researchers live in a world with overlapping network coverage but only work one-cell-at-a-time.

In this work, we present a research vision of techniques that allow researchers to work in large multi-cell attack scenarios with laboratory-scale budgets. Our overarching approach is to "multiplex" a single radio across multiple cells to duplicate capability without duplicating hardware. Such an approach is feasible because most attackers seek only a fraction of overall traffic, such as temporary or permanent identifiers, paging and other signaling, or DNS requests. For this approach to work, the downtime of the radio during retuning and resynchronization must be small enough that the radio can capture the phenomena of interest.

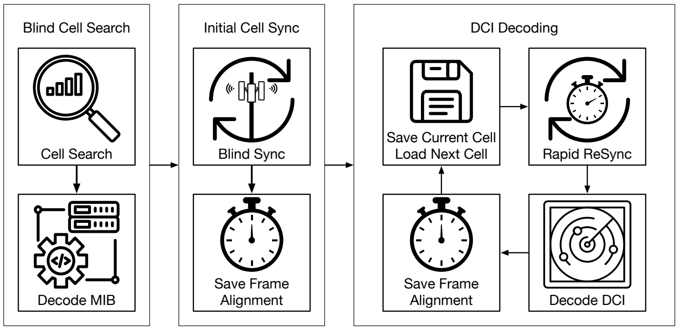


Fig. 1: Intercellular System Overview

To answer this critical question, we developed Intercellular, a proof-of-concept framework for passive device monitoring across multiple cells. In this preliminary analysis, we demonstrate the feasibility of passively achieving situational awareness of active devices on multiple cells in reception range. To implement Intercellular, we built a downlink sniffer based on a heavily modified version of srsRAN [3] that is capable of maintaining synchronization with multiple cells simultaneously. An overview of the Intercellular system architecture is shown in Figure 1

To maintain synchronization with each cell, we designed a rapid resynchronization algorithm that is used in place of traditional PSS/SSS based synchronization. This algorithm uses the time of arrival of the last observed radio frame for that cell to calculate the time of arrival for the next radio frame. Such an approach is practical because LTE radio frames have a fixed periodicity and duration. Since accurate time keeping is critically important for our synchronization algorithm, we utilized an external high accuracy clock to stabilize the radio.

To identify active devices within each cell, we monitor the cell for uplink and downlink resource grants. Specifically, we monitor the downlink control channel for downlink control information (DCI). We designed a DCI decoder based on a heavily modified version of the FALCON DCI decoder.

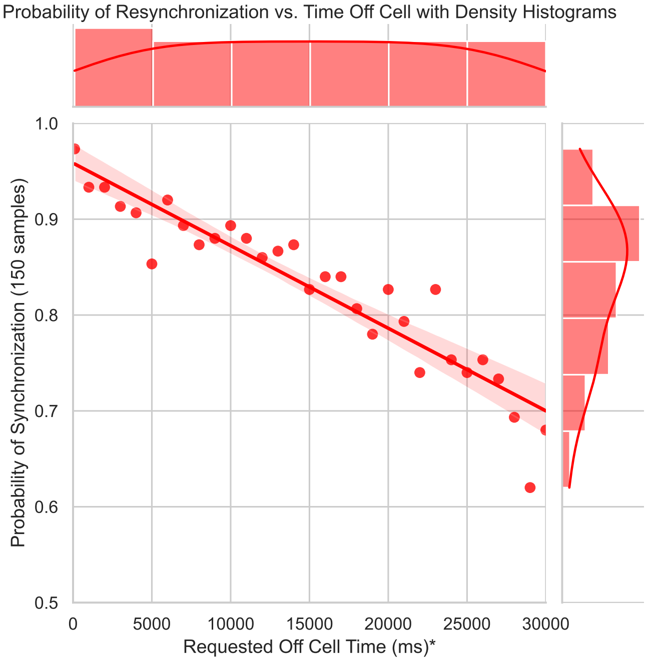


Fig. 2: Probability of successfully synchronizing decreases as time off cell increases.

[2] Intercellular monitors the DCI for unique radio network temporary identifiers (RNTIs) to identify all active UEs in each cell.

We first evaluated whether Intercellular could successfully resynchronize with the cell without resorting to blind primary and secondary synchronization signal (PSS/SSS) based synchronization. The accuracy of our scheduling algorithm was measured by first synchronizing with the cell using PSS/SSS based synchronization. Intercellular then instructed the SDR to tune away from the cell and wait for the desired off-cell time. After the off-cell time had elapsed, Intercellular issued a tune request to tune the radio back to the cell. A timed receive stream start command is then issued to the SDR and the location of the PSS is checked. Synchronization is achieved if the PSS successfully decodes. We observed that Intercellular could reliably calculate the start time of the next radio frame and achieve downlink synchronization, even when off cell for 30 seconds, as shown in figure 2

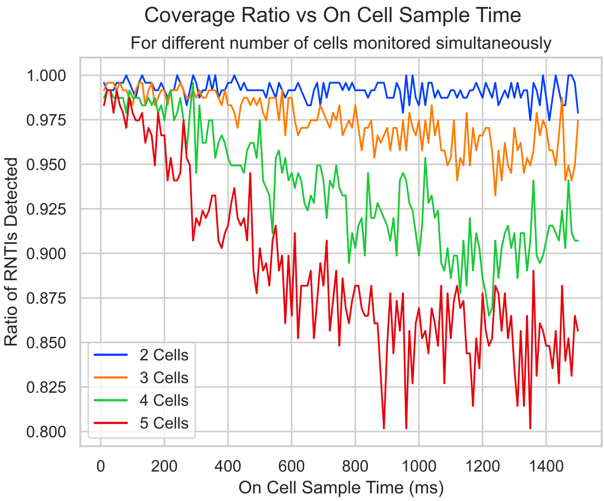


Fig. 3: Coverage decreases as on-cell sample time increases

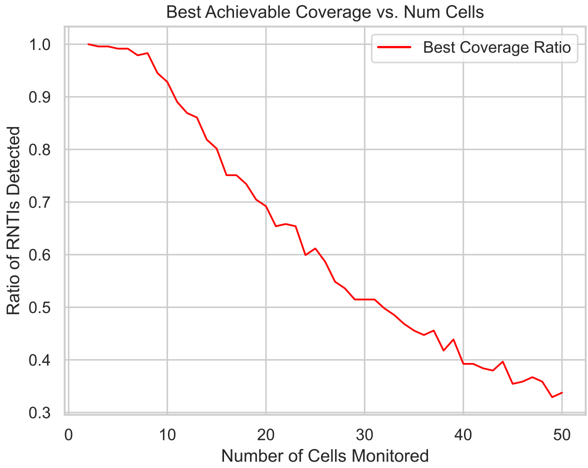


Fig. 4: Coverage decreases as the number of cells monitored simultaneously increases.

Since Intercellular cannot continuously monitor every cell simultaneously, only a fraction of the total subframes transmitted by the cell will be decoded. We quantified the coverage ratio for various cell configurations by checking if any active UEs were missed by the DCI decoder compared to a baseline trace. A test cell containing 235 randomly allocated UEs was first generated using MatLab. The samples generated by MatLab were first run through the DCI decoder running in single-cell mode to obtain a baseline DCI trace. We then simulated operation in an environment served by multiple cells by selectively skipping samples in the trace to simulate various sampling configurations. The DCI traces produced by both runs were then compared to the baseline DCI traces to determine if any allocations were missed. We observed that increasing the number of radio frames decoded in each sample decreased the probability that an active device in the cell would be detected, as shown in 3 We also observed that increasing the number of cells monitored simultaneously negatively impacted the coverage of the cell, as shown in figure 4

References

[1] Government Cellphone Surveillance Catalogue, December 2015.

[2] Robert Falkenberg and Christian Wietfeld. FALCON: An accurate real-time monitor for client-based mobile network data analytics. *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7, December 2019. arXiv: 1907.10110.

[3] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, and Douglas J. Leith. srsLTE: An Open-Source Platform for LTE Evolution and Experimentation, February 2016. arXiv:1602.04629 [cs].

We designed a system that uses a **single** SDR to efficiently monitor **all** cells in a local area **simultaneously**.

Towards Simultaneous Attacks on Multiple Cellular Networks

Alexander Ross, **Bradley Reaves**

Introduction

- Cellular Network Attack and Defense Research rely on Software Defined Radios (SDRs).
- While a single SDR is relatively affordable, most areas are served by multiple Mobile Network Operators, each with several cells.
- Well funded actors are not cost sensitive and are currently capable of mounting large scale attacks.†
- Research labs usually have few such radios for attack and defense research. Practically all prior work in cellular research has focused on either monitoring a single cell at a time or using multiple SDRs to monitor several cells simultaneously.

Methods

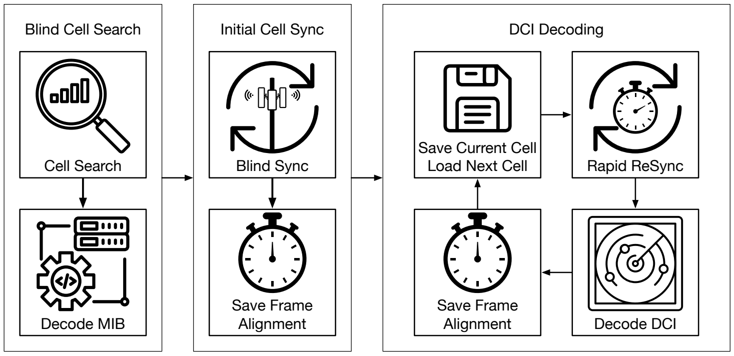
- We modified srsRAN to support maintaining synchronization with multiple commercial cells simultaneously.
- We exploit the fact that LTE radio signals are structured into radio frames broadcasted at predictable times.
- Before disconnecting from the current cell, a timestamp corresponding with the start of the last radio frame is saved to for use in calculating when the beginning of a new radio frame will occur.
- The radio is instructed to start streaming received samples at the instant the start of the next frame is being broadcasted over the air.
- The FALCON** Downlink Control Information decoder was ported to MultiCell to provide blind radio network temporary identifier (RNTI) discovery.

Results

- Intercellular can reliably calculate the start time of the next radio frame and achieve downlink synchronization, even when tuning back after 30 seconds.
- Increasing the number of radio frames decoded in each sample resulted in a decrease in the probability that an active device in the cell would be detected.
- Increasing the number of cells monitored simultaneously negatively impacted the coverage of the cell.

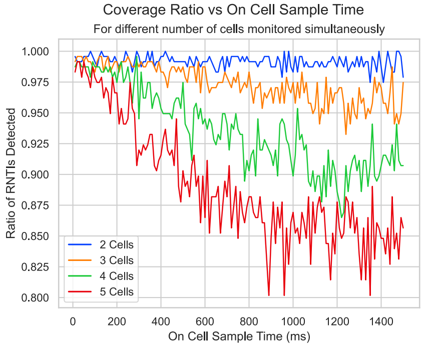
Takeaways

- We demonstrated that it is practical to monitor multiple cells simultaneously using a single radio with only minor to moderate coverage limitations.

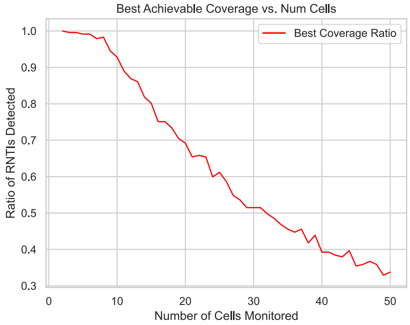


† Government Cellphone Surveillance Catalogue, December 2015.

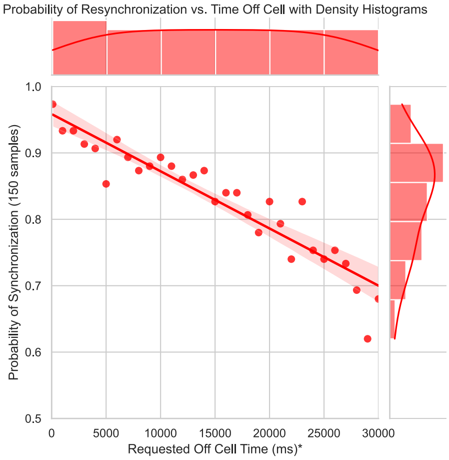
** Robert Falkenberg and Christian Wietfeld. FALCON: An accurate real time monitor for client-based mobile network data analytics. 2019 IEEE Global Communications Conference (GLOBECOM), pages 1–7, December 2019. arXiv: 1907.10110



Coverage decreases as on-cell sample time increases



Coverage decreases as the number of cells monitored simultaneously increases.



Probability of successfully synchronizing decreases as time off cell increases.

*Requested off cell time is the duration between when the radio is tuned off of the cell to when a tune request is issued to tune back to the cell. Actual time off cell is greater due to the analog front end tuning delay.

NC STATE UNIVERSITY

WSPR