Privacy-Preserving Mobile Phone Localization with Cryptographic Authorization in 5G Networks Mid-Term Status

Rishabh Kumar (cs25resch04002)

CS5553: Wireless Networks and Security

November 11, 2025

Project Overview (Review)

Problem Statement

- Current 5G positioning systems process location data in plaintext through centralized Location Management Functions (LMF), enabling potential mass surveillance without authorization controls or privacy protections

Key Objectives

- Design cryptographic multi-party authorization framework for 5G positioning
- Implement privacy-preserving localization using homomorphic encryption
- Develop secure network slicing for authorized positioning services
- Integrate judicial oversight mechanisms with threshold cryptography

Success Metrics

- Positioning Accuracy: Maintain $\leq$ 3m with security controls
- Authorization Latency: $<$ 5 minutes for judicial approval

Methodology & Threat Model (Review)

Proposed Technical Approach

- **5G Simulation:** OpenAirInterface core (AMF, SMF, UPF) with custom secure LMF
- **Radio Access:** RF Simulator-based gNB with multiple base stations for positioning
- **Positioning Methods:** Cell-ID, E-CID, OTDOA, Multi-RTT techniques
- **Privacy Enhancement:** Multi-party authorization + encrypted processing

Threat Model

- **Adversary:** Rogue government agencies or compromised network operators
- **Attack:** Unauthorized mass surveillance using 5G sub-meter positioning
- **Method:** Compromised AMF credentials, bulk location requests, movement profiling

Mid-Term Deliverables (Status)

Promised Mid-Term Deliverables (from Proposal)

Deliverable	**Status**
5G Simulation Environment Setup	Completed
OpenAirInterface 5G Core (AMF, SMF, UPF)	✓
gNB and UE simulation infrastructure	✓
Standard Localization Implementation	Completed
Cell-ID and E-CID positioning methods	✓
UE location extraction from AMF logs	✓
Vulnerability Demonstration	Completed
Unauthorized location access PoC	✓
Extract UE location without authorization	✓
Cryptographic Security Framework	In Progress
TLS infrastructure foundation	✓
Threshold signature scheme	Planned
Multi-party authorization protocol	Planned

Work Completed & Implementation Details

Hardware Setup (Simulation-Based)

- Windows 11 with WSL2 Ubuntu 24.04 (16GB RAM)
- Docker Engine 28.2.2 for 5G component orchestration
- 7 containers: MySQL, AMF, AMF-2, SMF, UPF, gNB, UE
- No physical hardware required - pure software simulation

Software & Tools

- **5G Core:** OpenAirInterface v2.1.10 (AMF, SMF, UPF)
- **RAN:** OAI RF Simulator (gNB + NR-UE develop branch)
- **Localization:** Python 3.13.9 for positioning calculations
- **Security:** Rsyslog with rsyslog-gnutls (RFC 5425), OpenSSL for x509 certificates

Implementation

- `ue_location_service.py` - Extract Cell ID, IMSI, gNB, TAC from AMF
- `rsyslog-server.conf` - Secure log collection with TLS
- `amf2_entrypoint.sh` - Custom AMF with secure logging

Experimental Setup

5G Network Configuration

- Control Plane Network: 192.168.71.128/26
- User Plane Network: 192.168.72.128/26
- PLMN: MCC=208, MNC=99, TAC=0x0001
- Test UE IMSI: 208990100001100
- Multiple gNB simulation for positioning triangulation

Metrics Used for Analysis

- **Positioning Accuracy:** Cell-ID and E-CID precision (target $\leq$ 3m)
- **Authorization Latency:** Time for multi-party approval (target $<$ 5 min)
- **Privacy Overhead:** Performance impact of encryption/authorization
- **Attack Prevention:** Effectiveness against unauthorized requests

Baseline for Comparison

- Standard 3GPP 5G positioning (TS 38.305) without security enhancements

Preliminary Results

5G Simulation Environment (Completed)

- All 7 containers operational: MySQL, AMF, AMF-2, SMF, UPF, gNB, UE
- gNB connected to AMF (ID: 0x0E00, Status: Connected)
- UE registered successfully (State: 5GMM-REGISTERED)
- End-to-end connectivity verified: 0% packet loss

Standard Localization Implementation (Completed)

- **Cell-ID Method:** Successfully extracts Cell ID (0000e014e)
- **E-CID Data:** TAC (00 00 01), PLMN (208/99), gNB (gnb-rfsim)
- **Location Extraction:** Python service parses AMF logs for UE location
- **Data Format:** JSON export for integration with authorization framework

Vulnerability Demonstration (Completed)

- **Attack Vector:** Direct access to AMF container logs without

Live Demo

VIDEO DEMONSTRATION

Click to play video:

WNS_20251112_03_01.mp4

(Video file: WNS_20251112_03_01.mp4)

Demonstration includes:

1. **5G Network Simulation:** All containers running (docker ps)
2. **UE Registration:** Device connecting to 5G network
3. **Standard Localization:** Extracting UE position from AMF logs (Cell-ID, E-CID)

Challenges & Risks Encountered

Original Risks (from proposal)

- Simulation complexity for realistic 5G positioning
- Cryptographic performance overhead
- Integration of multi-party authorization with 3GPP standards

Technical Challenges Faced

- **Infrastructure & 5G Simulation:** WSL resource limitations, container orchestration complexity, AMF/gNB integration issues
- **Security:** TLS certificate management, authentication configuration
- **Positioning:** Limited to Cell-ID/E-CID (OTDOA, Multi-RTT require multiple gNBs)

Design Challenges & Solutions

Design Choices & Architectural Challenges

- **Authorization Service Integration:** How to integrate multi-party authorization framework?
  - Option 1: Modify AMF directly (3GPP non-compliant, breaks standards)
  - Option 2: Proxy/middleware layer between LMF and AMF (adds latency)
  - Option 3: Separate authorization service with hooks into LMF (chosen approach)

Solutions Implemented

- Leveraged existing RFC 5425 for secure syslog implementation
- Implemented triangulation with multiple gNBs for improved positioning accuracy

Shamir's Secret Sharing for Multi-Party Authorization

Problem with Current System

- Single entity (AMF operator/admin) can authorize location requests
- No checks and balances $\rightarrow$ Potential for abuse
- Demonstrated vulnerability: Anyone with AMF access can track UEs

Proposed Solution: Threshold Cryptography

- Require multiple independent parties to approve location requests
- Use **(t, n)-Threshold Scheme:** t out of n parties must agree
- Proposed: **(3, 5) scheme** - 3 out of 5 parties must approve

5 Authorization Parties:

1. **Judicial Authority** - Court order validation
2. **Law Enforcement Agency** - Investigation justification
3. **Network Operator Security Officer** - Technical feasibility
4. **Privacy Oversight Officer** - Privacy impact assessment
5. **Independent Auditor** - Compliance verification

Shamir's Secret Sharing - Mathematical Foundation

How It Works (Shamir 1979):

1. Secret Generation & Sharing

- Authorization secret S (e.g., LMF access key)
- Encode as polynomial of degree $t-1$:

$$f(x) = S + a_1x + a_2x^2 + \ldots + a_{t-1}x^{t-1} \pmod{p}$$

  where p is large prime, a_i are random coefficients
- Each party i receives share: $(i, f(i))$

2. Secret Reconstruction

- Collect t shares: $(x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t)$
- Use Lagrange interpolation to reconstruct polynomial:

$$S = f(0) = \sum_{j=1}^{t} y_j \prod_{k=1, k\neq j}^{t} \frac{x_k}{x_k - x_j}$$

- Recovered S authorizes location request to LMF

Updated Timelines & Next Steps

Completed Work (Mid-Term)

- 5G Simulation Environment (OAI + gNB + UE) → **Done**
- Standard Localization (Cell-ID, E-CID) → **Done**
- Vulnerability Demonstration (unauthorized access) → **Done**
- Security Infrastructure Foundation (TLS, RFC 5425) → **Done**

Work Remaining for Final Deliverable (Nov 24)

- **Week 1 (Nov 11-17):**
  - Implement threshold signature scheme (Shamir's Secret Sharing)
  - Develop multi-party authorization protocol (3-of-5 approval)
  - Begin homomorphic encryption integration for privacy-preserving positioning
- **Week 2 (Nov 18-24):**
  - Complete secure LMF with encrypted positioning calculations
  - Performance benchmarking: Standard vs. Privacy-Preserving
  - Final attack/defense demonstration comparing both approaches
  - Documentation, final report, GitHub repository push

References

GitHub Repository

- https://github.com/Rishabh0712/WNSTermProject

References

1. 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN" https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3501
2. Shamir, A.: "How to share a secret." *Communications of the ACM* 22.11 (1979): 612-613
3. Gentry, C.: "Fully homomorphic encryption using ideal lattices." *STOC* 2009
4. OpenAirInterface 5G Core: https://gitlab.eurecom.fr/oai/cn5g/oai-cn5g-fed
5. OAI 5G RAN: https://gitlab.eurecom.fr/oai/openairinterface5g
6. Microsoft SEAL Library: https://github.com/Microsoft/SEAL