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

Rishabh Kumar (cs25resch04002)

Wireless Network Security Course

Jul-Nov 2025

Problem Statement

- **Motivation**: 5G networks enable sub-meter localization accuracy, creating unprecedented surveillance capabilities that lack constitutional safeguards and judicial oversight mechanisms.
- **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.

Objectives & Success Metrics

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

Metrics

- **Positioning Accuracy**: Maintain $\leq 3m$ accuracy with security controls
- **Authorization Latency**: < 5 minutes for judicial approval workflow
- **Baseline**: Standard 3GPP 5G positioning (TS 38.305) without security enhancements

Threat Model

- **Threat Model**: Rogue government agencies or compromised network operators attempting unauthorized mass surveillance using 5G's sub-meter positioning capabilities to track citizens without judicial oversight.
- **Assumptions**:
  - 5G network infrastructure is operational and follows 3GPP standards
  - Cryptographic primitives (threshold signatures, homomorphic encryption) are secure
  - Judicial authorities maintain secure key management systems

Attack Scenario Illustration:

Compromised AMF credentials $\rightarrow$ Bulk location requests $\rightarrow$ Precise coordinates $\rightarrow$ Movement profile construction

Methodology & Technical Approach

Simulation-Based Approach: Deploy complete 5G network simulation to demonstrate privacy-preserving localization

- **5G Simulation Environment**:
  - **Core Network**: Open5GS with AMF, SMF, UPF, and custom secure LMF implementation
  - **Radio Access**: srsRAN-based gNB simulation with multiple base stations for positioning
  - **User Equipment**: Simulated mobile devices with realistic mobility patterns
  - **Positioning Methods**: Implementation of Cell-ID, E-CID, OTDOA, and Multi-RTT techniques
- **Privacy Enhancement**: Demonstrate attack scenarios on standard 5G localization and show how multi-party authorization and encrypted processing prevent unauthorized surveillance

Hardware and Software Requirements

Hardware Requirements

- **Development Machine**: Ubuntu 22.04 LTS with 16GB RAM, multi-core CPU
- **Docker Environment**: Container orchestration for 5G core components
- **Network Virtualization**: Virtual interfaces and network namespaces for isolation
- **Storage**: 50GB+ for simulation data, logs, and container images

Simulation Software Stack

- **5G Simulation**: Open5GS (core network), srsRAN (RAN simulation)
- **Cryptography**: Python libraries (cryptography, pycryptodome), OpenSSL
- **Network Simulation**: Docker Compose, Linux network namespaces
- **Mobility & Testing**: Python scripts for UE movement simulation, performance measurement tools

Key Advantage: Pure software simulation eliminates hardware dependencies while enabling comprehensive 5G privacy-preserving localization testing

Timeline & Milestones

- **Week 1**: Deploy 5G simulation environment (Open5GS + srsRAN), implement basic localization methods (Cell-ID, E-CID), demonstrate standard positioning workflow
- **Week 2**: Develop attack simulation scenarios, implement unauthorized surveillance demonstrations, design and integrate cryptographic authorization framework
- **Week 3**: Implement privacy-preserving localization with encrypted processing, integrate multi-party authorization, develop secure LMF with threshold signatures
- **Week 4**: Complete simulation testing with multiple attack/defense scenarios, performance benchmarking (accuracy vs. security), documentation and demonstration preparation

Deliverables

- **Mid-term deliverables (for 11 Nov)**:
  - **5G Simulation Environment Setup**: Basic 5G core network (Open5GS) with gNB and UE simulation infrastructure
  - **Standard Localization Implementation**: Working 5G positioning using Cell-ID, E-CID, and OTDOA methods in simulated environment
  - **Vulnerability Demonstration**: Proof-of-concept showing how unauthorized localization requests can be executed in standard 5G
  - **Cryptographic Security Framework**: Initial implementation of threshold signature scheme and multi-party authorization protocol
- **Final deliverables (for 24 Nov)**:
  - **Complete 5G Network Deployment Simulation**: Software-based 5G core (Open5GS) with multiple gNBs and UE mobility simulation
  - **Privacy-Preserving Localization Demo**: Live demonstration showing standard vs. secure localization with multi-party authorization
  - **Attack Simulation & Defense**: Mass surveillance attack simulation and privacy protection effectiveness demonstration
  - **Performance Analysis**: Quantitative evaluation of positioning accuracy, authorization latency, and security overhead in simulated environment
  - **Deployment Package**: Complete simulation setup with documentation for reproducible 5G privacy-preserving localization testing

Privacy-Preserving Workflow Demonstration

Standard 5G Localization (Vulnerable)

1. **Client Request**: Law enforcement sends location request to AMF
2. **Direct Processing**: AMF forwards request to LMF without authorization checks
3. **Position Calculation**: LMF collects measurements from gNBs in plaintext
4. **Result Delivery**: Precise coordinates returned immediately to client
5. **Privacy Risk**: No audit trail, no judicial oversight, potential for mass surveillance

Privacy-Preserving 5G Localization (Secure)

1. **Authorization Request**: Client submits court order with digital signatures
2. **Multi-Party Validation**: Threshold signature verification (3-of-5: judicial, law enforcement, operator, privacy officer, oversight)
3. **Encrypted Processing**: LMF performs positioning calculations on encrypted measurement data using homomorphic encryption
4. **Secure Communication**: All data exchanges use secure network slice with end-to-end encryption

References

- 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
- Shamir, A.: "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.
- Gentry, C.: "Fully homomorphic encryption using ideal lattices." STOC 2009.
- Open5GS Project: https://open5gs.org/
- srsRAN Project: https://www.srslte.com/
- Microsoft SEAL Library: https://github.com/Microsoft/SEAL
- RELIC Cryptographic Toolkit: https://github.com/relic-toolkit/relic