Control-Plane Protocol Interactions in Cellular Networks

Guan-Hua Tu*¹, Yuanjie Li*¹, Chunyi Peng², Chi-Yu Li¹, Hongyi Wang¹, Songwu Lu¹

¹: University of California, Los Angeles;
²: The Ohio State University

* The first two authors contribute equally to this work.
Cellular Services are Ubiquitous

- Large-scale wireless infrastructure
- Offer data and voice services to *anyone, anywhere, anytime*

6.8+ billion

*Source: http://www.4gamericas.org/*
Control Plane in Cellular Network

- Connectivity Management (CM)
- Mobility Management (MM)
- Radio Resource Control (RRC)

Layered protocol stack

Diagram showing 3G and 4G gateways, Mobile Switching Center, and Mobility Management Entity (Control Node) connectivity.
Control Plane in Cellular Network

- Layered protocol stack
- Domains separated for voice (CS) and data (PS)
Control Plane in Cellular Network

- Layered protocol stack
- Domains separated for voice (CS) and data (PS)
- Hybrid 3G/4G systems
Protocol work together to offer vital 3G/4G utilities

- Rich patterns along three dimensions

- Cross-domain
- Cross-layer
- Cross-system
Problem:
Each individual protocol may be well designed. How about protocol interactions?
Rich Protocol Interactions

- Complex interactions in common scenarios
  - Inevitable interplay between radio, mobility, data/voice
  - Concurrent voice and data use
  - 3G/4G switch due to hybrid deployment, mobility, voice

- Two causes of problematic interactions
  - Design defects
  - Operation/Implementation slips
Rich Protocol Interactions

- Complex interactions in common scenarios

Diagnosis over one layer/domain/system is insufficient

- Two causes of problematic interactions

Single-type test fails to unveil both issues
Our Solution: CNetVerifier

- Cellular-specific model checking
  - Extract full-stack cellular model from 3GPP standards
  - Create a variety of usage scenarios
  - Define desirable user-perspective properties
  - Discover counterexamples for possible design defects
Our Solution: CNetVerifier

- Cellular-specific model checking
- Phone-based experimental validation
  - Instrument end devices to collect traces for verification
  - Discover operational slips in real networks
Finding Overview

I. Necessary but problematic cooperation

II. Independent but coupled operations
Finding Overview

I. Necessary cooperation

II. Independent operations

cross-layer  cross-domain  cross-system
Improper cooperation: Cross-System

Scenario: run data services during 4G → 3G → 4G

1. Setup 4G connectivity to access internet
Scenario: run data services during 4G → 3G → 4G

1. Setup 4G connectivity to access internet

2. 4G → 3G: 4G conn. context is converted to 3G for seamless switch
Scenario: run data services during 4G $\rightarrow$ 3G $\rightarrow$ 4G

3. 3G $\rightarrow$ 4G: 3G conn. context is converted back to 4G
Problematic scenario: **3G context is deleted** before returning to 4G

1. 3G conn. context is deleted.

**Causes of deletion (in 3GPP)**
- Low layer failures
- User disables data services
- No enough resources
- ....
Problematic scenario: **3G context is deleted** before returning to 4G

2. **3G->4G**: No 3G context transferred to 4G context

"Out-of-Service"
Problematic scenario: **3G context is deleted** before returning to 4G

2. **3G->4G**: No 3G context transferred to 4G context

PS conn context is **not mandatory in 3G (PS+CS)**, but **mandatory in 4G (PS only)**

*Shared context for 4G and 3G is not well protected in 3G*

“Out-of-Service”
Improper cooperation: Cross-System

- **Real-world impact**
  - Occurs 3.1% in user study
  - “out-of-service” for up to 25s

- **Lessons: a design defect**
  - Different demands of packet switching in 3G & 4G
  - *Desirable but not enforced: shared context should be consistently protected in 4G & 3G*

- **Proposed remedies**
  - Avoid unnecessary 3G PS context deactivation
  - Immediately enable 4G PS context reactivation
Scenarios: 4G users make calls via 3G CS Fallback

1. To make a call, 4G user → 3G
Improper cooperation: cross-domain+system

Scenario: 4G users make calls via 3G CS Fallback

1. To make a call, 4G user → 3G
2. When the call ends, 3G → 4G
Problematic Scenario: Call with background data

1. A call makes 4G → 3G; Data is migrated to 3G, too

Improper cooperation: cross-domain+system

How and Why?
Improper cooperation: cross-domain+system

How and Why?

Problematic Scenario: Call with background data

2. When the call ends, No 3G→4G (data is still on)

User gets stuck in 3G, losing 4G.
Improper cooperation: cross-domain+system

How and Why?

- Unexpected loop in RRC state machine

User gets stuck in 3G, losing 4G.

Voice only
Improper cooperation: cross-domain+system

How and Why?

- Unexpected loop in RRC state machine

User gets stuck in 3G, losing 4G.
Improper cooperation: cross-domain+system

How and Why?

- Unexpected loop in RRC state machine

3G CS  3G PS

RRC

4G PS

RRC

Voice + Data
(certain setting)

RRC state transition is inconsistent with dual-domain, inter-system settings

User gets stuck in 3G, losing 4G.
Improper cooperation: cross-domain+system

- **Real-world impact**
  - 62.1% 4G users being stuck in 3G after the call
  - Stuck in 3G for 39.6s in average

- **Lessons: a design defect**
  - 3G CS and 3G PS are *indirectly* coupled in RRC
  - Inconsistent state transition with all 3G→4G options

- **Proposed remedies**
  - Revise the RRC state transition for possible settings
Problem Scenario: Signaling loss for registration

Improper cooperation: Cross-Layer
How and why?

- Attach request
- Attach accept
- Attach complete

Deregistered
Registered
Deregistered
Registered
Deregistered
Registered
Improper cooperation: Cross-Layer
How and why?

“out-of-service” right after being attached

Attachment process:
- Attach request
- Attach accept
- Attach complete
- Location update
- Location update response (error)

Registered
Deregistered
Registered
Deregistered
Registered
Deregistered
Improper cooperation: Cross-Layer
How and why?

“out-of-service” right after being attached

Deregistered

Registered

Attach request

Attach accept

Deregistered

Deregistered

Upper-layer (MM) assumes underlying reliable in-sequence signal transfer, but lower-layer (RRC) cannot offer this guarantee
Scenario: voice/data request with location update

1. Location update is triggered by MM (e.g., user moves)
Scenario: voice/data request with location update

1. Location update is triggered by MM (e.g., user moves)
2. After location update, user can send/receive voice and data
Problemsatic Scenario: voice/data request during the location update

1. Location is triggered by MM (e.g., user moves)
Problematic Scenario: voice/data request during the location update

2. User dials out

“Updating the location”

Outgoing call is delayed
Unnecessary Coupling: Cross-layer
How and why?

“Without user location, the cellular network cannot route user voice/data.”

“Updating the location”

Outgoing call is delayed
“Without user location, the cellular network cannot route user voice/data.”

Outgoing voice/data requests can be routed without user location.

Unnecessary prioritization of location update over outgoing call/data.
Real-world Impact
- up to 8.3s call delay and 4.1s data delay
- 7.6% of outgoing calls occur during location update

Lessons: a design defect
- outgoing data/voice requests and location update are independent, but they are artificially correlated

Proposed remedies
- Decouple location update and outgoing data/voice requests
- E.g., two parallel MM threads for different purposes
Scenario: dial a call during data service in 3G

- Access internet at full rate
- Dials a call

Unnecessary Coupling: Cross-domain
Scenario: dial a call during data service in 3G

Data service rate declines up to 74%
Scenario: dial a call during data service in 3G

Voice: low rate, low loss (e.g., 16QAM)
Data: high rate, loss tolerant (e.g., 64QAM)

Voice and data have competing demands on the channel, but they have to share the radio channel.
Scenario: Location update in 3G and 4G

1. Update 4G location, and notify 3G MSC

Unnecessary Coupling: Cross-system
Scenario: Location update in 3G and 4G

2. 3G location update fails, so 4G deregisters the network
Scenario: Location update in 3G and 4G

3G internal failures are exposed to 4G devices
Conclusion

- Uncover problems in signaling protocol interactions in cellular networks
- Three Lessons
  - The layering rule should be fully honored (optimistic assumptions, coupled actions)
  - Inter-domain difference should be well recognized (coupling independent services)
  - Hybrid systems are not properly coordinated (context sharing, fault isolation)
- More rigorous efforts are needed