How Voice Calls Affect Data in Operational LTE Networks

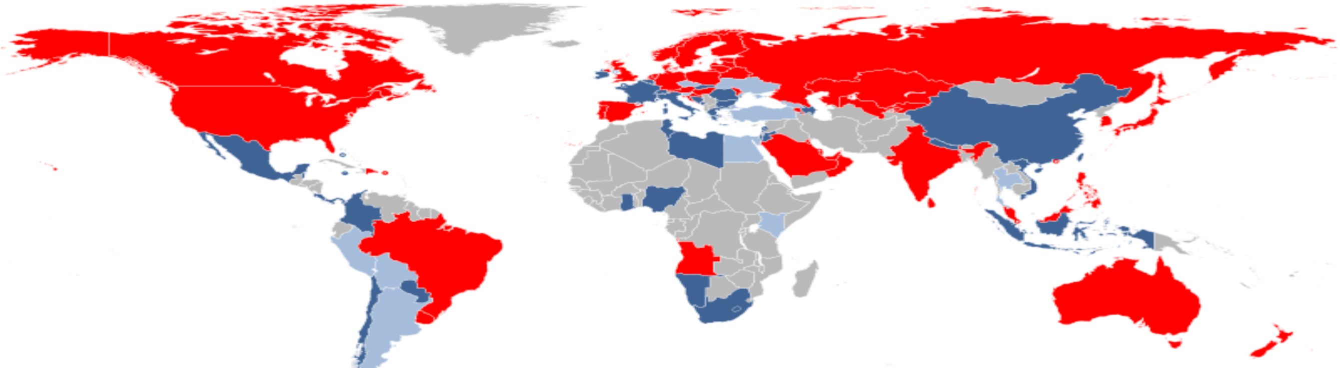
Guan-Hua Tu*, Chunyi Peng+, Hongyi Wang*,
Chi-Yu Li* , Songwu Lu*

*University of California, Los Angeles, US
+Ohio State University, Columbus, US

ACM MobiCom 2013
Miami, US

Data Access in 4G LTE

- In recent years, 4G LTE becomes very popular due to its high-speed transmission rate and has been launched in 46 countries



- However, it only supports packet-switched (PS) services; the traditional circuit-switched (CS) services, e.g., voice call, is not supported.

How does 4G LTE user make voice call?
By VoIP?

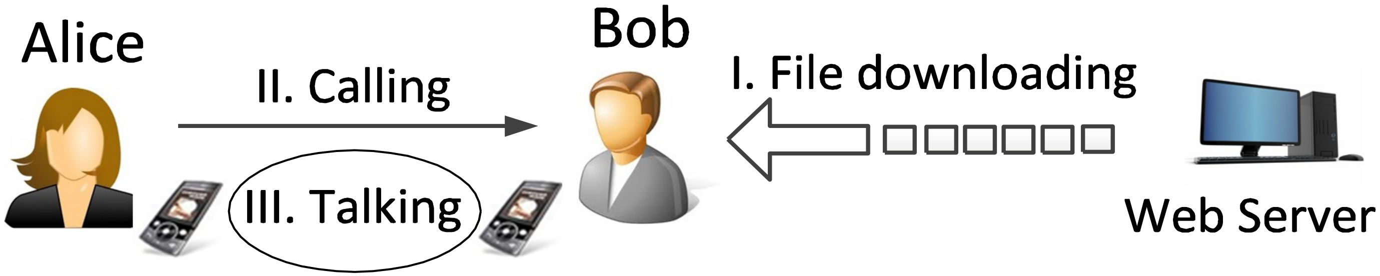
Two Solutions

- □ Voice over LTE (VoLTE)
  - It is similar to deploy SIP call services (VoIP) in LTE
  - However. operators have to deploy extra call control servers and media gateways.
- □ Circuit-Switched Fallback (CSFB)
  - Move 4G users to the legacy 2G/3G networks to access voice services.
  - So far, it has been broadly launched in many LTE networks.

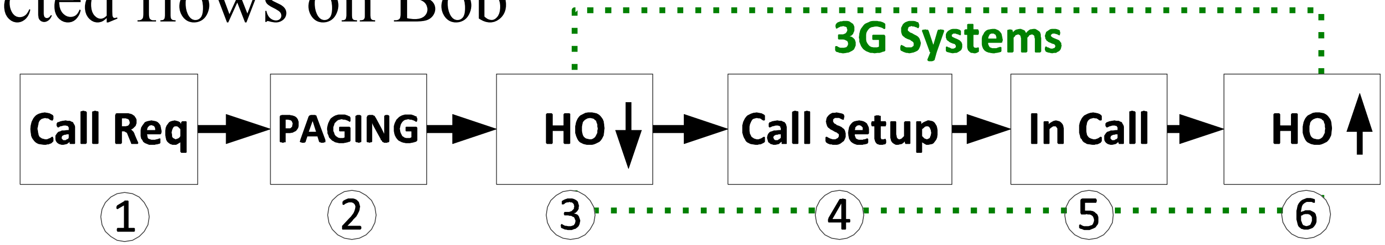
at&t Your world. Restri · T · ·Mobile· · Telefonica · SingTel ···

How CSFB Voice Calls Affect Data Access in 4G LTE?

An Example: Incoming Call Comes During Downloading



□ Expected flows on Bob



□ Our previous work# shows that data transmission suspends and user traffic is over-accounted when inter-system handover, e.g., 4G <->3G (step 3 and 6), occurs.

Anything else ?

#: Accounting for Roaming Users on Mobile Data Access: Issues and Root Causes, MobiSys'13

The Rest of Talk

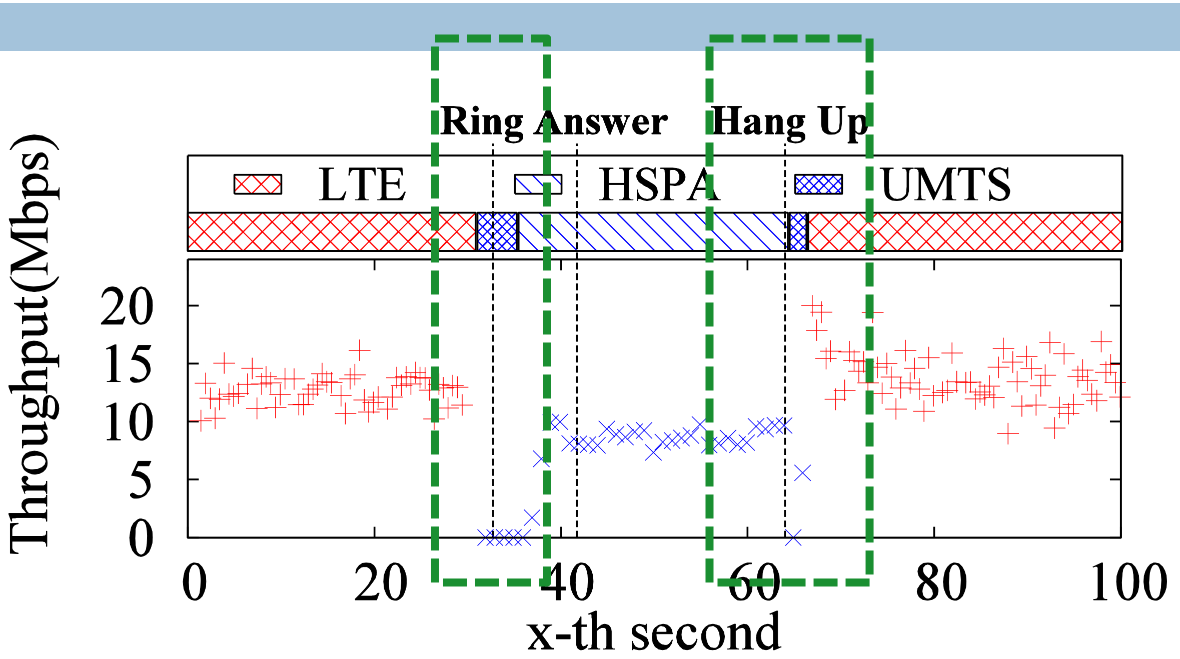
- Experimental Methodology
- Findings/Issues
- Insights
- Solutions
- Summary

Experimental Methodology

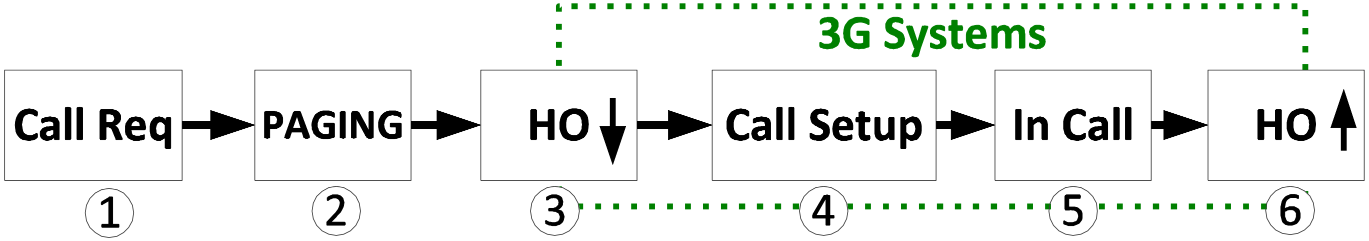
- We mainly conduct the experiments on two major US 4G LTE operators, which together cover almost 50% market share.
  - Called as OP-I and OP-II in this work
- The experiments are conducted on
  - Apple iPhone5
  - Samsung Galaxy S3/S4
  - HTC One
  - LG Optimus G.

Unexpected Throughput Slump

Throughput Slump



Logs of data throughput (4G:+, 3G:x) on Bob in OP-I


3G Systems

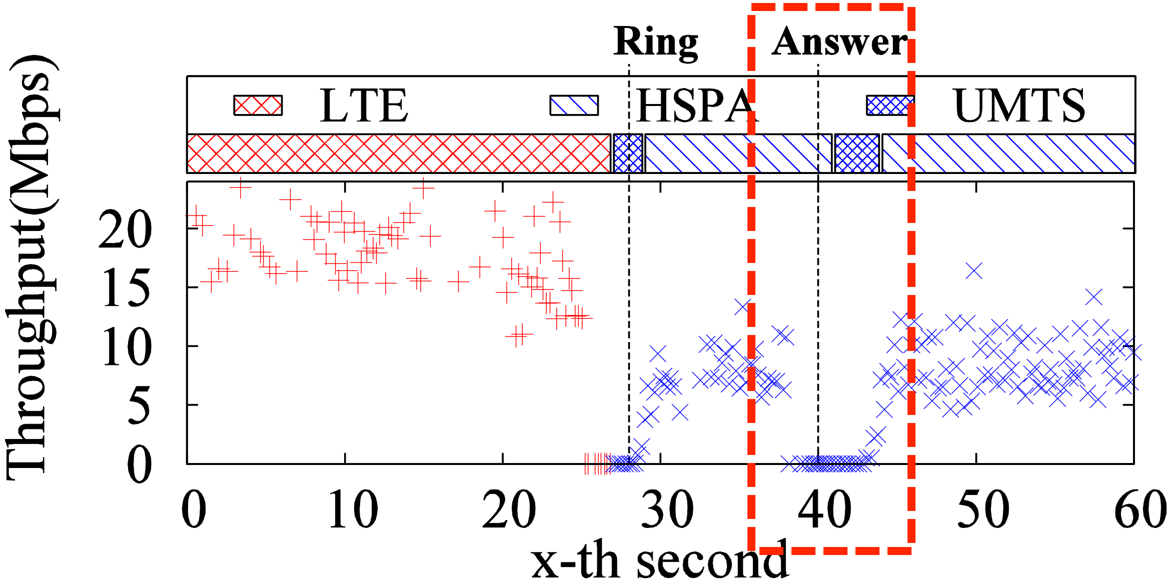
Call Req → PAGING → HO ↓ → Call Setup → In Call → HO ↑

① ② ③ ④ ⑤ ⑥

Anything else ?

One More Slump

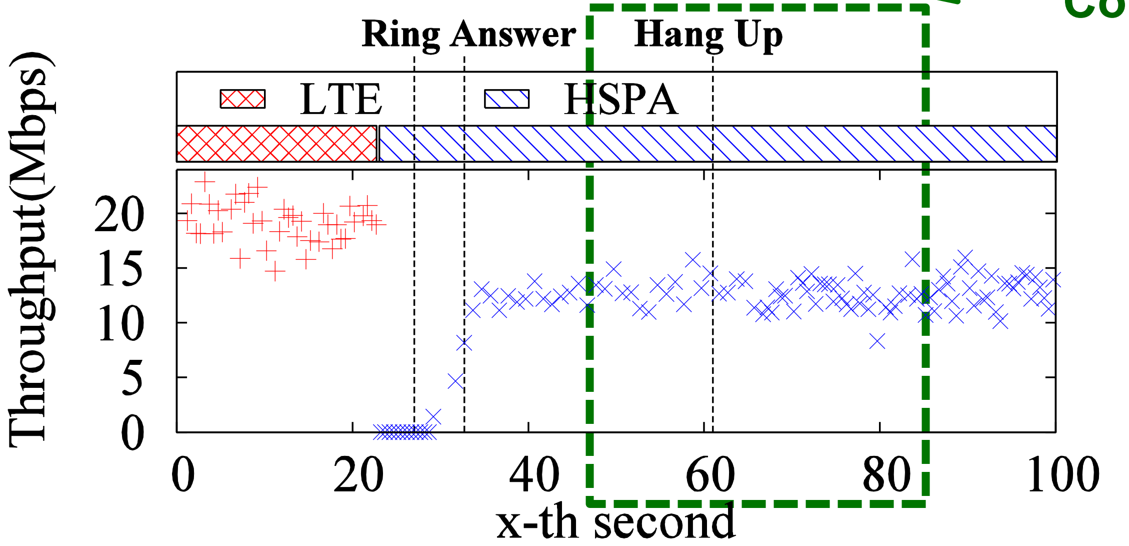
- In addition to two handovers, we observe one extra handover in the ***40.6%*** of experiment runs (149/367) in OP-I.



Logs of data throughput (**4G:+**, **3G:x**) in OP-I

Even Worse

- In OP-II, we observe that Bob cannot go back to 4G LTE after call ends.



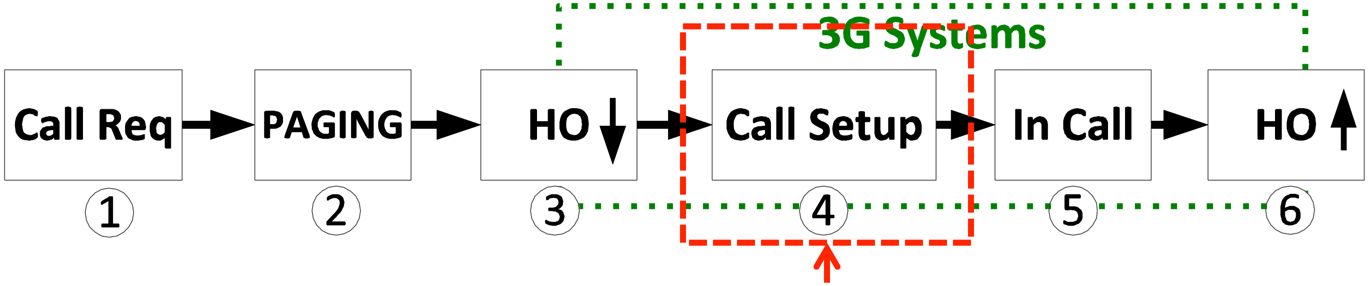
Lose 4G Connectivity

Logs of data throughput (**4G:+**, **3G:x**) in OP-II

Is it OP-II specific issue?
How long it lasts for?

Lose 4G Connectivity

- In OP-I, Bob cannot go back to 4G LTE if Alice cancels the outgoing call before call is fully established (i.e., Bob doesn’t hear ringtone yet).



Alice hangs out the outgoing call before call setup is finished

- We find that Bob will stay in 3G longer than **10** hours under certain conditions.

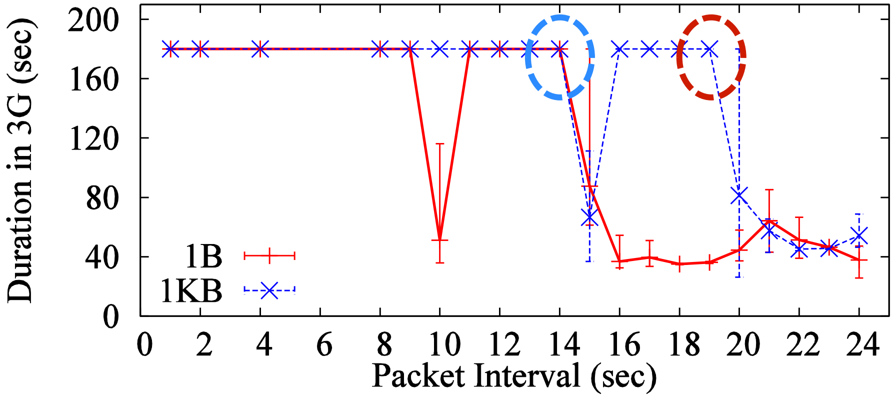
What factor influences the duration?

Data Services

- We find that it depends on whether *data service is running* on Bob’s phone.
- Specifically, the duration Bob stuck in 3G is dependent on packet size and packet interval of data service running.
- We conduct an experiment to track the duration Bob stays in 3G for 3 mins after Bob’s call conversation finishes.
  - Packet Size: 1B or 1KB
  - Packet Interval: 1~24 seconds

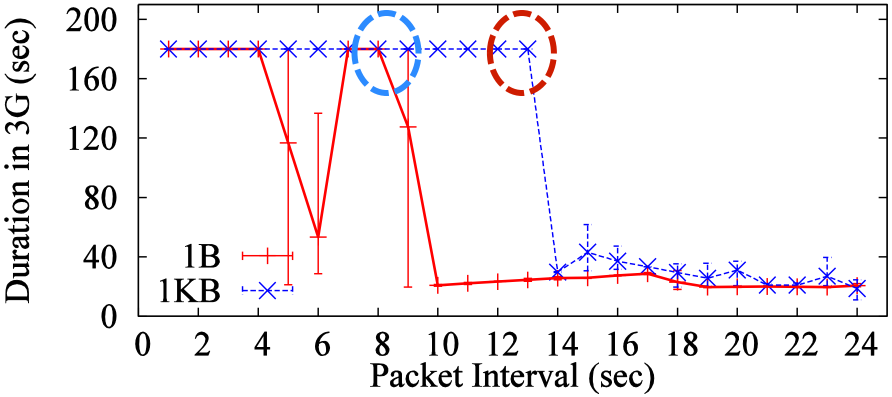
Experiment Results

14s-1B 19s-1KB



OP-I

7s-1B 13s-1KB

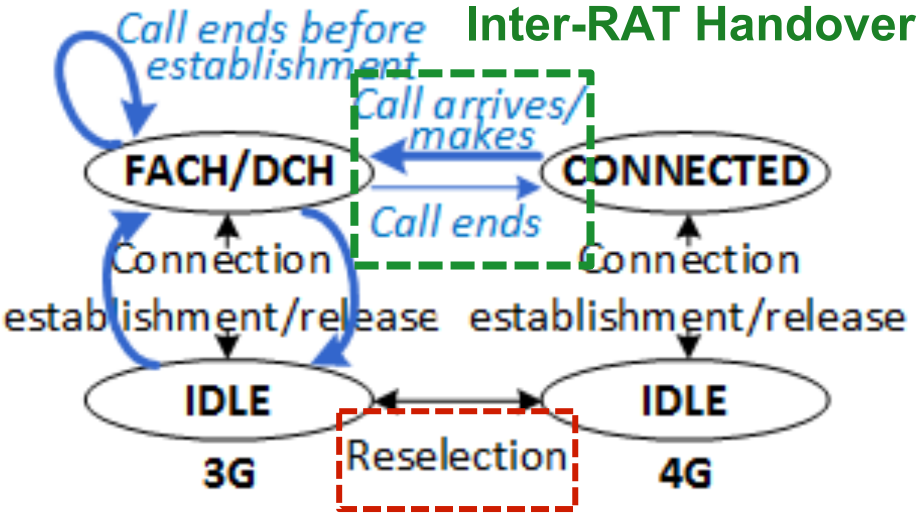


OP-II

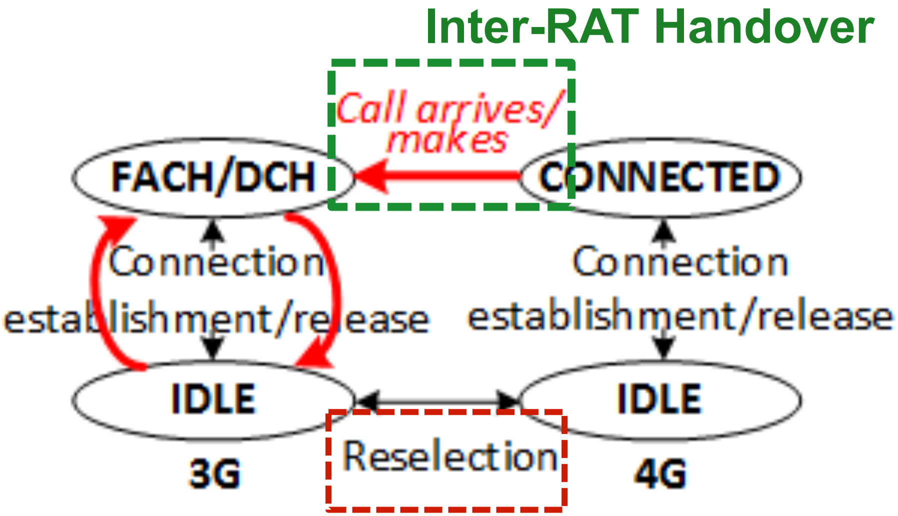
Why does it depend on traffic pattern ?

RRC State Transition

- Bob can go back to 4G LTE via *Inter-RAT Handover* or *Cell reselection*.
- RRC State Transitions observed in OP-I and OP-II


Call ends before establishment
Inter-RAT Handover
Call arrives/makes
Call ends
FACH/DCH
CONNECTED
Connection establishment/release
Connection establishment/release
IDLE
IDLE
Reselection
3G
4G

Simplified RRC State for OP-I



Simplified RRC State for OP-II

CSFB standards allow operators to decide how to move users back to 4G LTE

Applications Abort

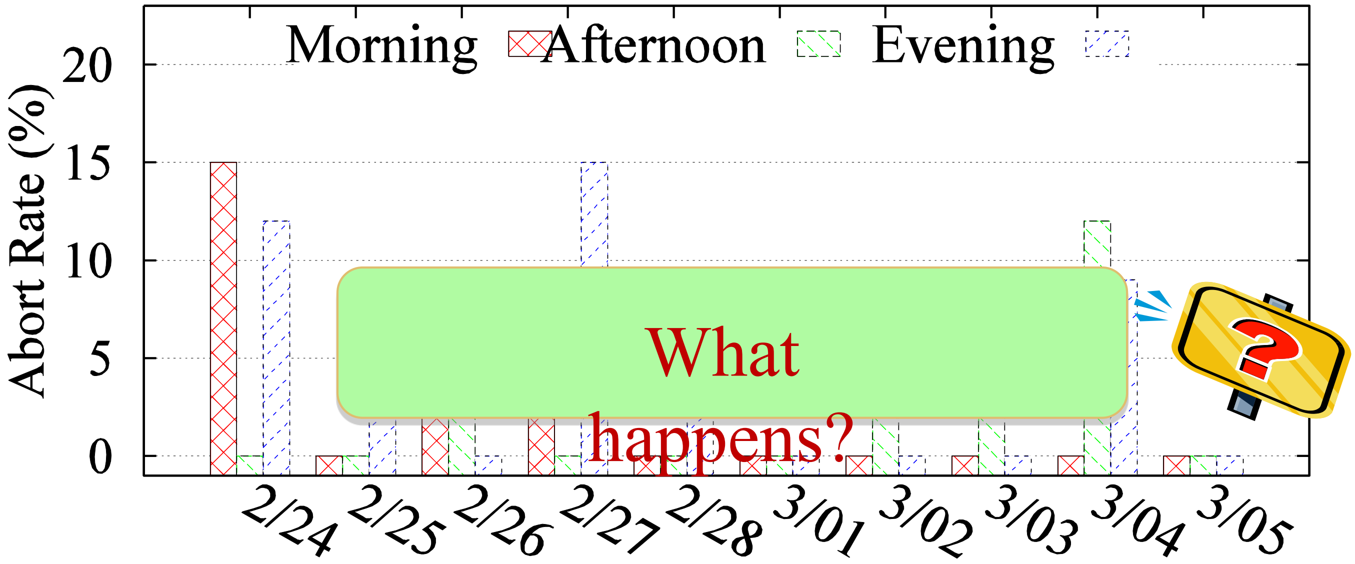
Data Applications Abort Due to Voice Call

- We are running eight popular data applications
  - Browser, Gmail, Ftp, Youtube, Skype, PPS (Streaming), Pandora (internet radio), Facebook

- We find that Browsing, Gmail, FTP, Skype and Facebook may abort due to CSFB calls.
  - Browsing/Facebook: content is not displayed
  - FTP/Gmail: downloading is terminated
  - Skype: voice call is aborted

How Often Application Aborts

- We run the experiment that user makes a call and hangs up later while data applications are running.
- We observe the average abort ratio around 3-5%.

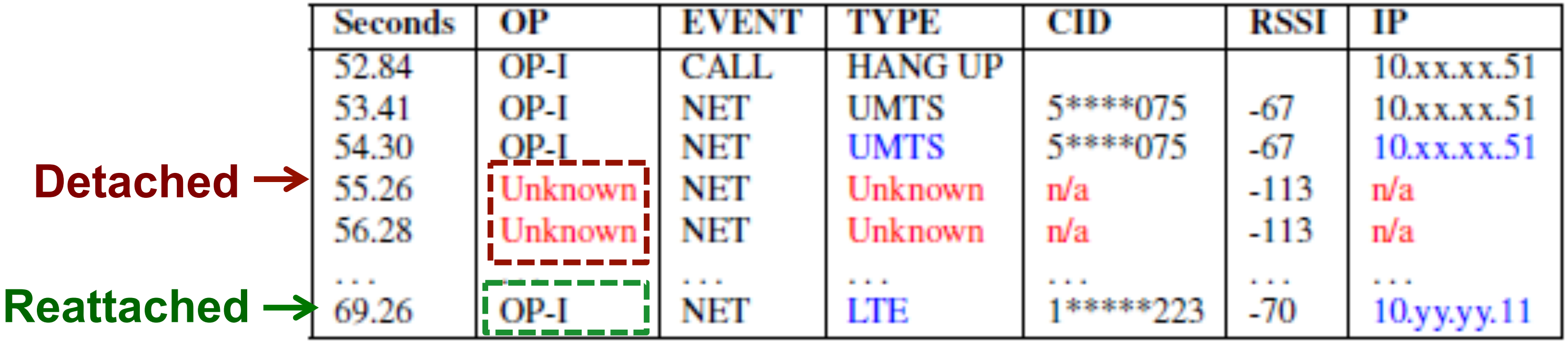


What happens?

10-day FTP downloading abort ratio (OP-I).

Detached

- The users are detached by carriers and lose both of 3G and 4G LTE connectivity for a while when this issue occurs.



Seconds	OP	EVENT	TYPE	CID	RSSI	IP
52.84	OP-I	CALL	HANG UP			10.xx.xx.51
53.41	OP-I	NET	UMTS	5****075	-67	10.xx.xx.51
54.30	OP-I	NET	UMTS	5****075	-67	10.xx.xx.51
55.26	Unknown	NET	Unknown	n/a	-113	n/a
56.28	Unknown	NET	Unknown	n/a	-113	n/a
. . .		. . .	. . .	. . .	. . .	. . .
69.26	OP-I	NET	LTE	1*****223	-70	10.yy.yy.11

Detached →

Reattached →

Logs of network status at mobile phone (OP-I).

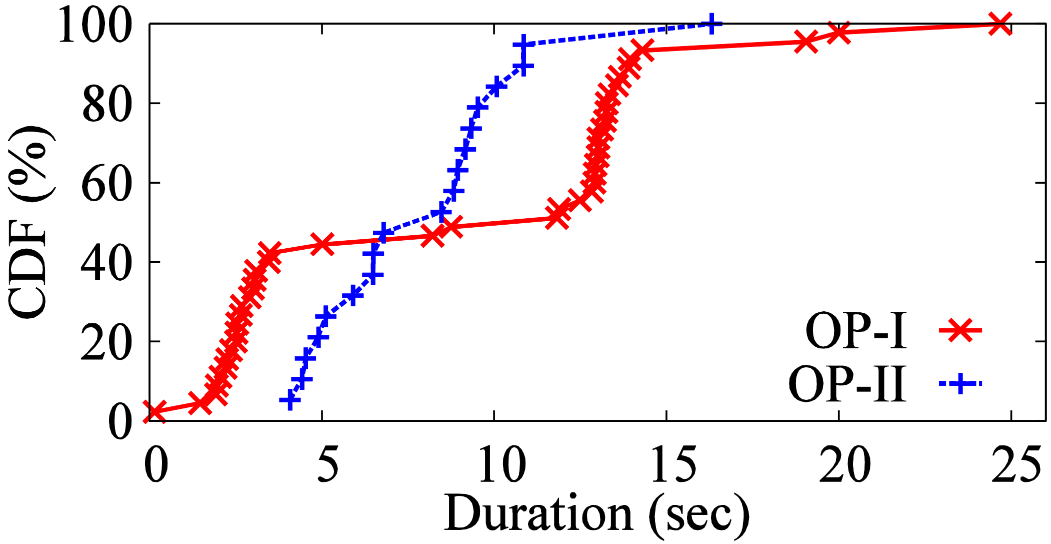
How long does it recover the connectivity?

Sign into network

Operator-II

Resign into network (OP-II).

Reattach Duration

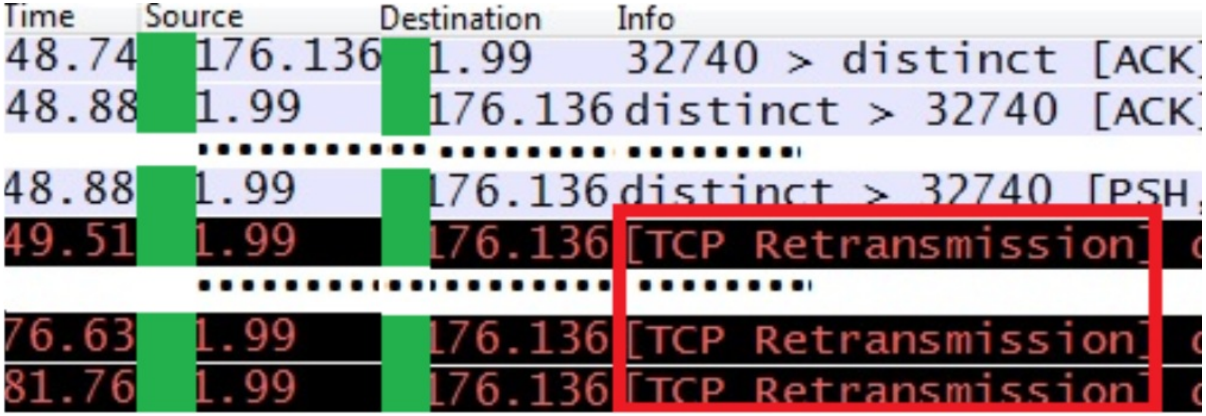


- For OP-I, **95%** of re-attaches finish within **11** seconds.
- For OP-II, **90%** of re-attaches finish within **15** seconds.

Q: Is it big issue to lose connectivity for 11-15 seconds?
It should be easily recovered by TCP retransmission.

Invalid TCP retransmission

- FTP server retransmits packets to mobile devices, however it doesn’t receive any acks.



```
Time     Source    Destination  Info
48.74    176.136   1.99         32740 > distinct [ACK
48.88    1.99      176.136      distinct > 32740 [ACK
         ..........................................
48.88    1.99      176.136      distinct > 32740 [PSH
49.51    1.99      176.136      [TCP Retransmission] c
         ..........................................
76.63    1.99      176.136      [TCP Retransmission] c
81.76    1.99      176.136      [TCP Retransmission] c
```

Wireshark traces at the FTP server

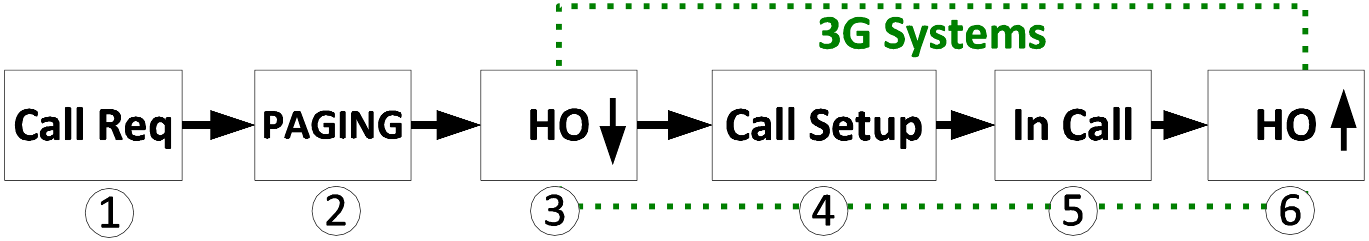
  - OP-I assigns *different IP address* to the mobile devices after reattaches.
  - OP-II assigns same IP address, however *NAT mapping* is gone after reattaches, i.e., retransmitted packets are dropped without valid mapping.

Missed Call Due To Data Service

Miss Call

- Under certain scenario, users may miss incoming calls without notifications.
- Alice is calling Bob and Bob is enabling PS network in the meantime.
  - Bob may **miss** Alice’s call without notification (e.g., ringtone).
  - However, Alice still hears alerting tone.
    - She may think Bob intentionally doesn’t answer the call.

Alerting Tone Comes Early



CSFB Incoming Call flows on Bob

- In the *paging phase* (Step 2), to avoid long period of silence at Alice, the Bob's MSC# sends indication of user alerting to Alice
- Then Alice can hear alerting tone.
- However, if Bob fails to *handover to 3G networks* (Step 3) then he will not hear ringtone.

#: On receipt of service request from MME.

Insights & Solutions

Insights

- For throughput slump
  - Temporary rate slumps to 0 Mbps is caused by handovers which are requested by CSFB standards and inevitable.
  - However, there is still something we can do.
- For loss of 4G connectivity
  - It is because that CSFB standards doesn’t *stipulate* how to move users back to 4G after call ends.
    - OP-I uses handover (for established calls) mechanism or cell reselection (for un-established calls) procedure
    - OP-II uses cell reselection procedure

Q: Can 3GPP stipulate to always handover the callee to 4G LTE after call ends? Is it completely addressed?

Security Loophole

- The scenario “Caller hangs up the outgoing call before callee’s phone is ringing.”
  - The callee will be *silently* handovered to 3G networks and *immediately* moved back to 4G LTE.
- Malicious attackers are able to launch tons of handovers which trigger *data suspension* and *overcharging* issues to the victims at their wish.
  - Introduce significant signaling overhead to operator

Solutions

- For throughput slump
  - Middle-box approach
    - When CSFB event, e.g., dialing, is detected, UE requests the middle box to cache all packets from peers.
    - After handover induced by CSFB is finished, UE informs middle box to immediately retransmit cached data.
- For losing 4G connectivity
  - Move users back to 4G LTE when they stay in 3G network longer than certain threshold, e.g., 60s, no matter data service is running or not.

Solutions

- For applications abort
  - Assign the same IP addresses to users within period, e.g., 2 hours.
  - Still keep NAT mapping after users are detached for short time, e.g., 15s
    - (90% reattach finish within 15 s).
- For miss call due to PS service
  - Defer the notification of user alerting sent to caller until the callee has been successfully handovered to 2G/3G networks.

Summary

- Throughput slumps when voice call starts and ends.
  - In OP-II, the throughput isn’t recovered even after call ends.
- Users may lose 4G connectivity for 10 hours (no signs to see limits) and may be utilized by malicious attackers.
- Users may be implicit detached by operators after CSFB call ends
  - Some applications abort due to unsuccessful receipt of packets from their applications server after re-attach finishes.
- Users may miss voice call without indications because alerting tone early comes to caller.

Questions?