

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

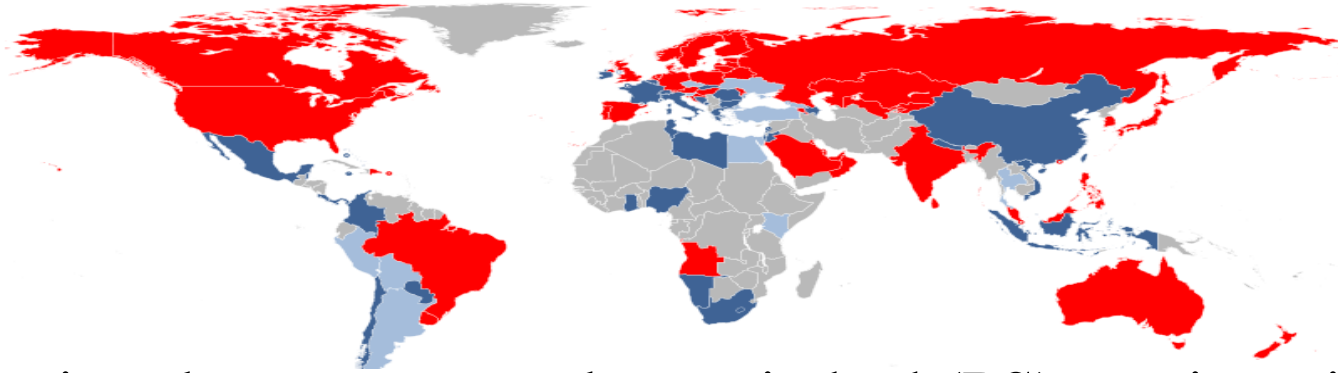
ACM MobiCom 2013

Miami, US

Data Access in 4G LTE

2

- In recent years, 4G LTE becomes very popular due to its high-speed transmission rate, i.e., 100Mbps, and has been launched in 46 countries



- However, it only supports packet-switched (PS) services, i.e., internet access; the traditional circuit-switched (CS) services, e.g., voice call or short message service, is not supported.

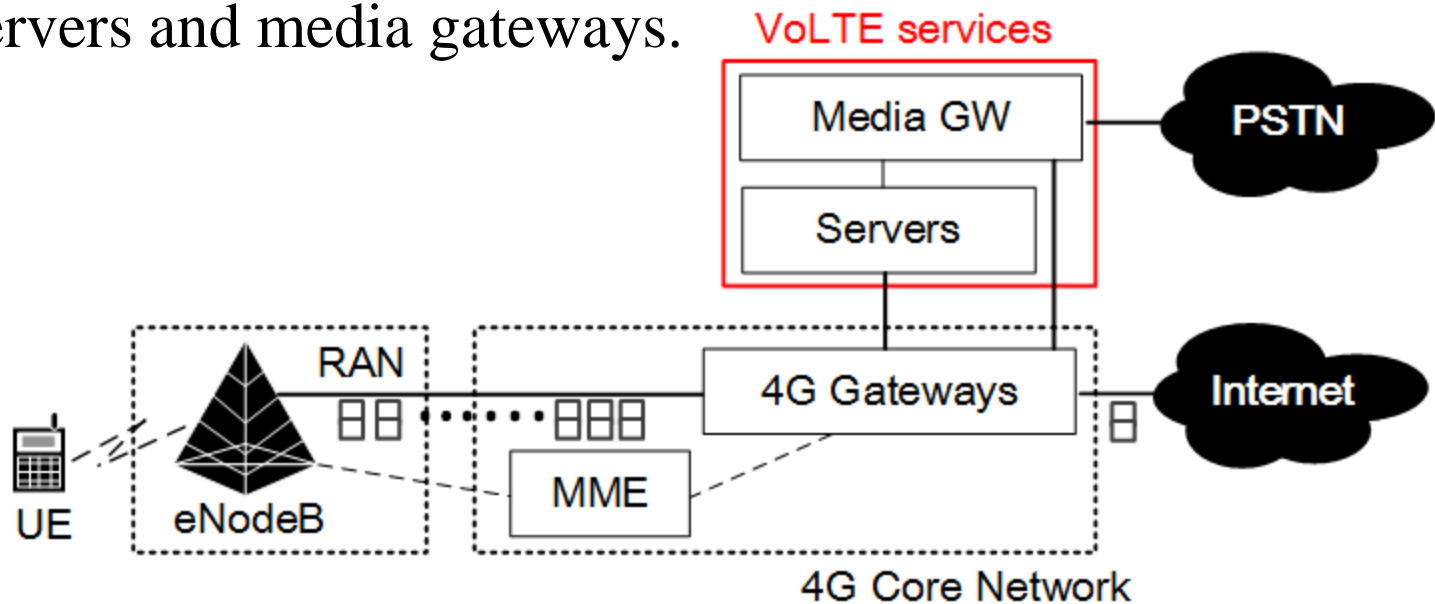
How does 4G LTE user make voice call?
By VoIP?



Solution 1: VoLTE

3

- 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.



MediaGW: Translate VoIP packets to/from PSTN voice traffic

Servers: Provide VoLTE services, e.g., registration or call control.

PSTN: Public Switched Telephone Network (traditional telephony networks)

Solution 2: CSFB

□ Circuit-Switched Fallback (CSFB)

- Handover 4G users to the legacy 2G/3G networks to access voice services.
- Packet-switched (PS) services can be also handed over to 2G/3G networks if operators support PS handover.
 - 2G: EDGE (Enhanced Data Rates for GSM Evolution)
 - max transmission rate: 236 Kbps
 - 3G: UMTS (Universal Mobile Telecommunications System)
 - max transmission rate: 384 Kbps
 - 3.75G: HSPA (High Speed Packet Access),
 - max transmission rate: 42.2 Mbps

Solution 2: CSFB

5

□ Circuit-Switched Fallback (CSFB)

- So far, it has been broadly deployed or chosen by many LTE operators including four of top 5 largest global operators, due to the following reasons.
 - Low deployment cost. There is no extra VoIP servers required.
 - Reuse the resources of legacy 2G/3G networks
 - Fully reserve the resources of 4G LTE networks to PS services

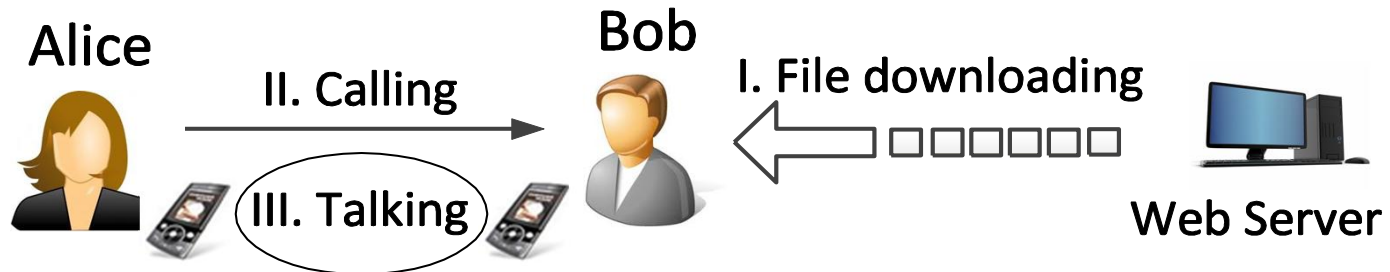


Since CSFB is the major voice solution for 4G LTE users, we are interested in how CSFB voice calls affect data access in 4G LTE?

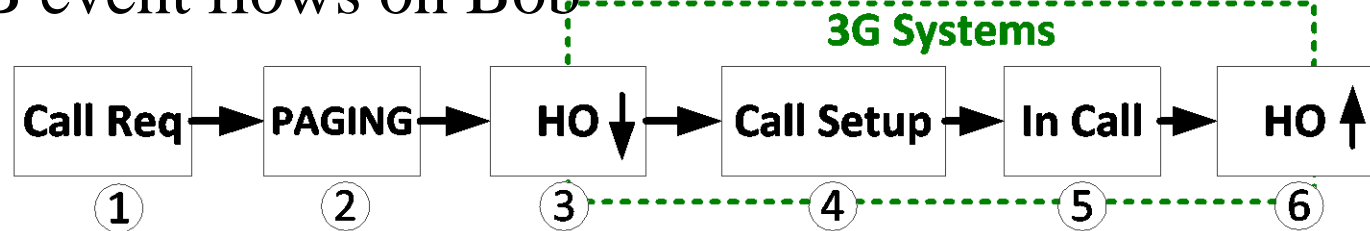


An Example: Incoming Call Comes During Downloading

6



- CSFB event flows on Bob



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

Anything else ?



The Rest of Talk

7

- Experimental Methodology
- Issues found
- Insights
- Solutions
- Summary

Experimental Methodology

8

- 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 later
- The experiments are conducted on
 - ▣ Apple iPhone5
 - ▣ Samsung Galaxy S3/S4
 - ▣ HTC One
 - ▣ LG Optimus G.

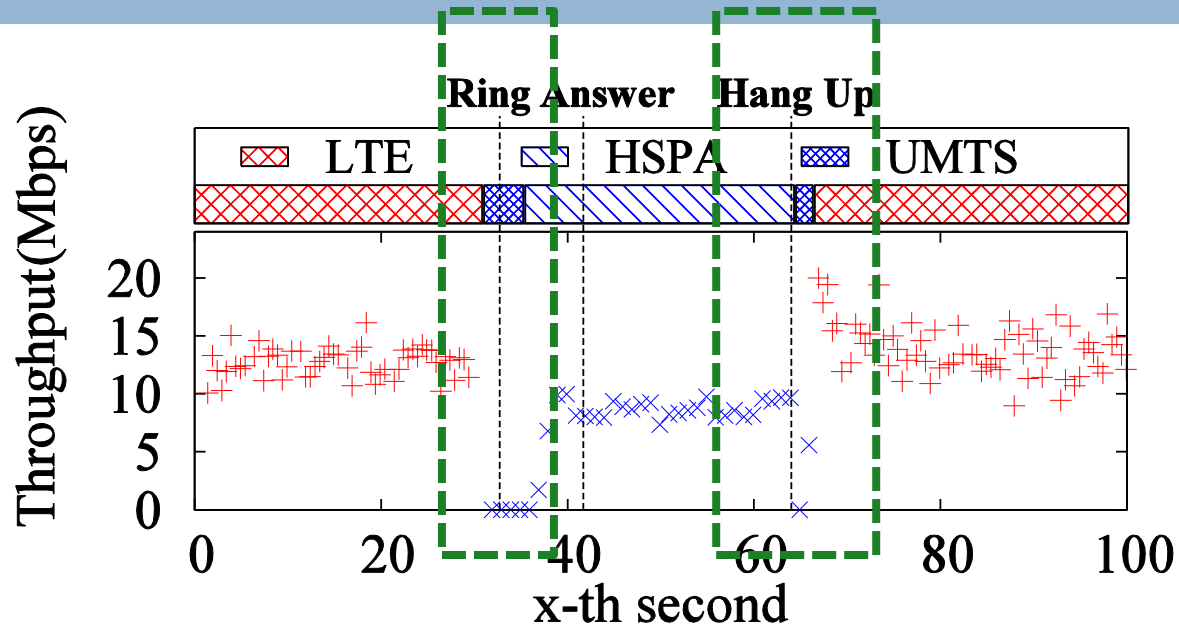


9

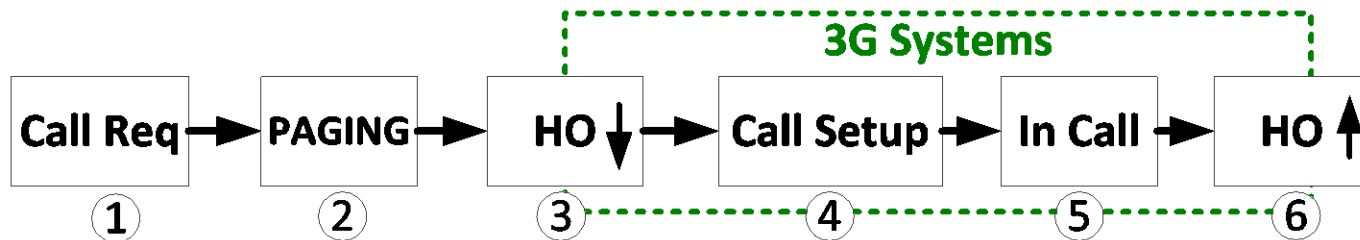
Unexpected Throughput Slump

Throughput Slump

10



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

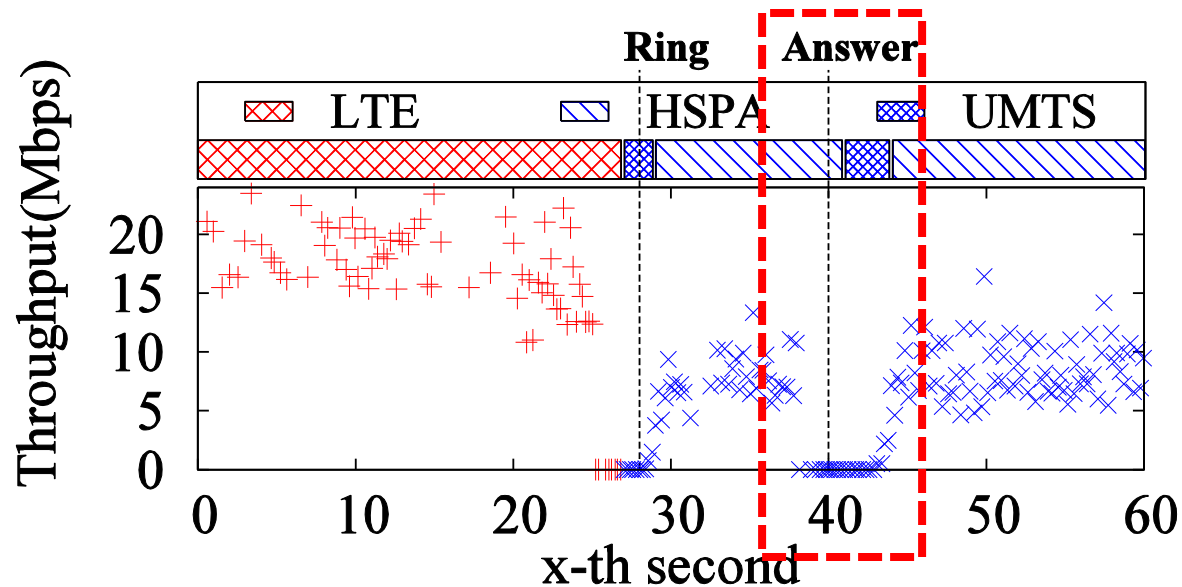


Anything else ?



One More Slump

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

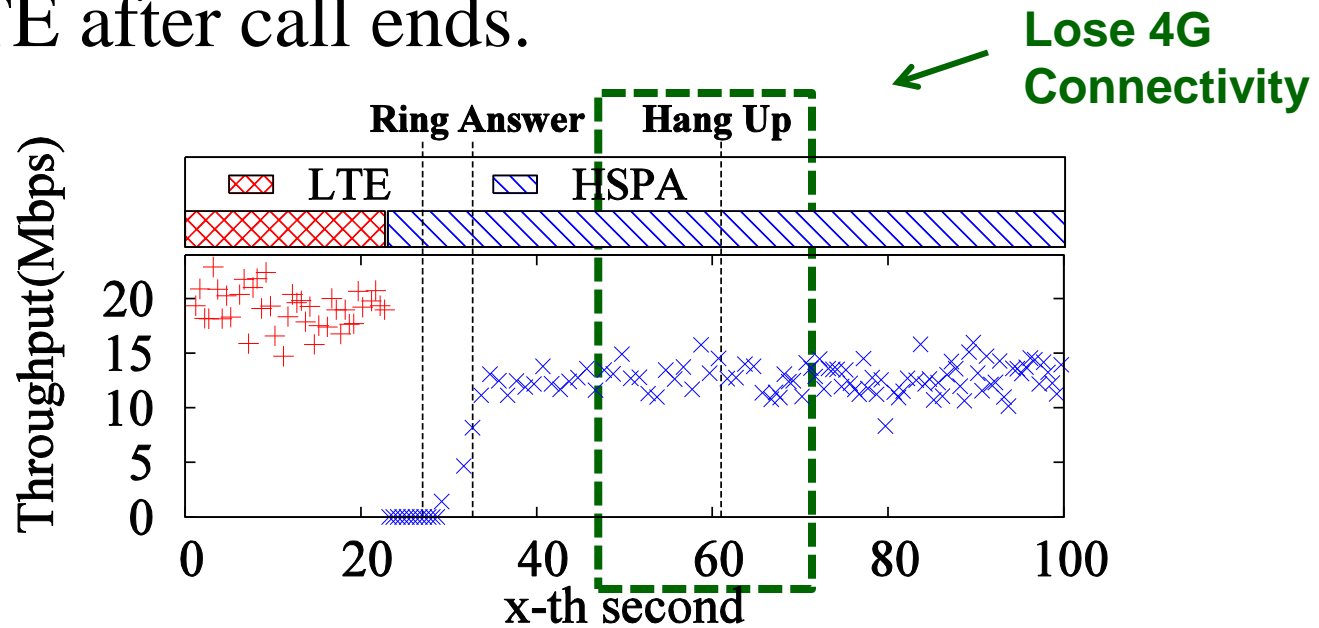


Logs of data throughput (4G:+, 3G:x) in OP-I

Even Worse

12

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



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

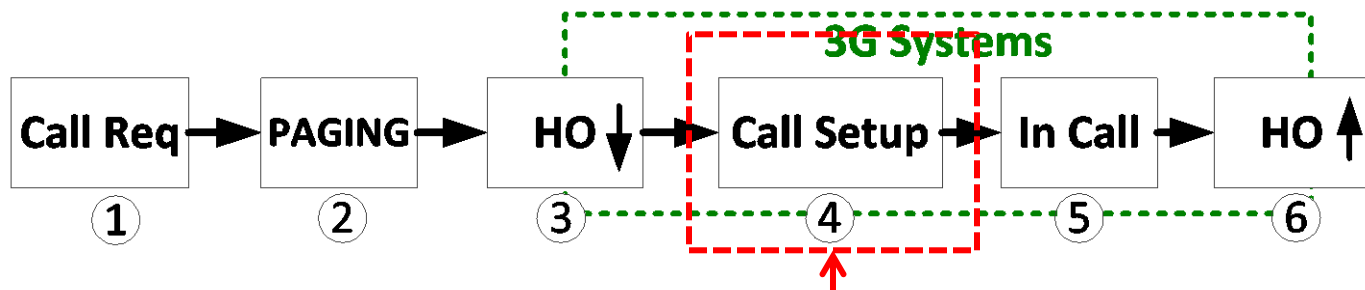
Is it OP-II specific issue?
How long it lasts for?



Lose 4G Connectivity

13

- In OP-I, Bob cannot go back to 4G LTE when..
 - ▣ 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

- Bob may be stuck in 3G longer than **10** hours under certain conditions.

What factor influences the duration?

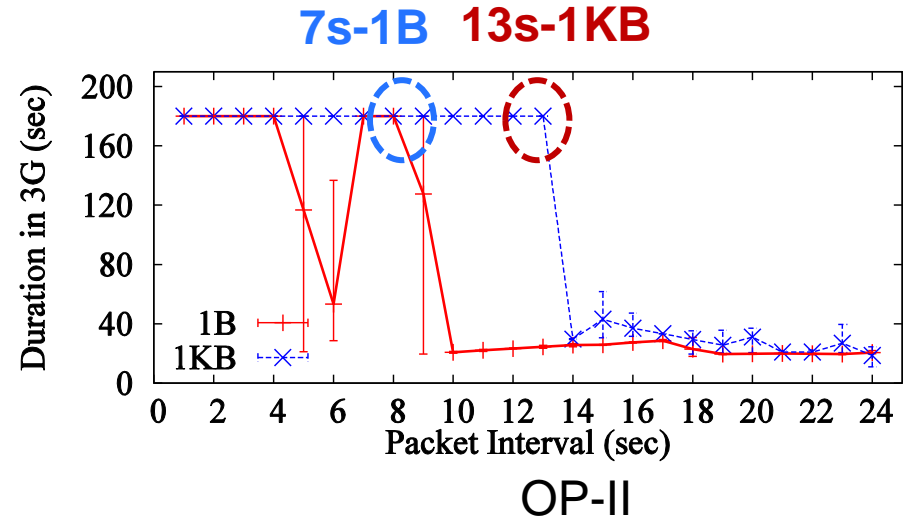
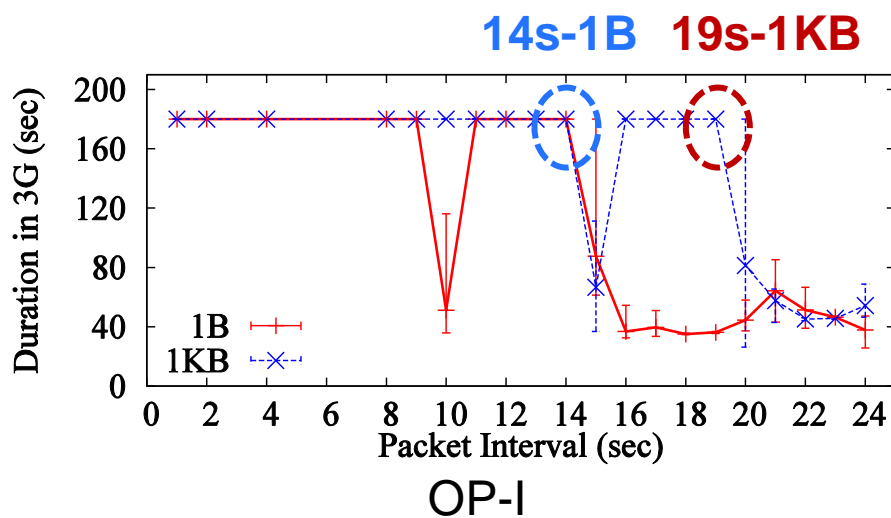


Data Services

- 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 record **how long** Bob is stuck in 3G after call ends with following settings.
 - ▣ Two kinds of packet size: 1B or 1KB
 - ▣ Various packet interval: 1~24 seconds
 - ▣ Experiment duration: 180 seconds

Experiment Results

When Packet-Interval is less than 14s and packet size is 1byte, OP-I 4G users will stuck in 3G



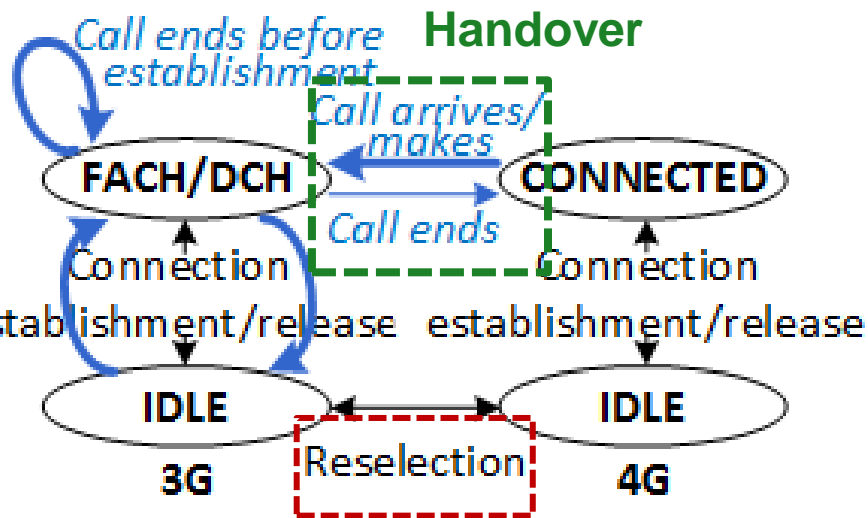
Why does it depend on traffic pattern ?



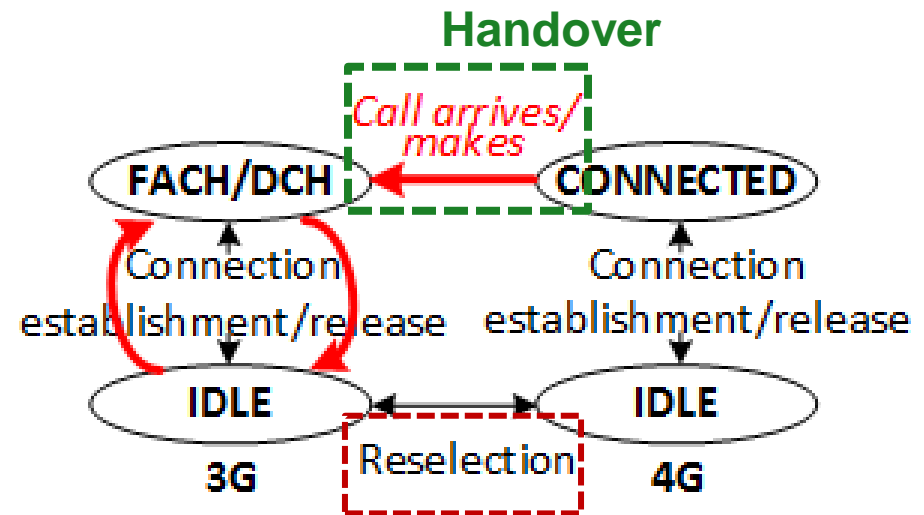
RRC State Transition

16

- RRC State Transitions observed in OP-I and OP-II



Simplified RRC State for OP-I



Simplified RRC State for OP-II

Both OP-I and OP-II choose “Reselection” which is triggered in IDLE state to move users back to 4G LTE in some scenarios. However, once PS traffic is higher than threshold shown previous slide, UE will stay in FACH/DCH state for PS traffic and cannot go back to 4G LTE.

17

Applications Abort

Data Applications Abort Due to Voice Call

18

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

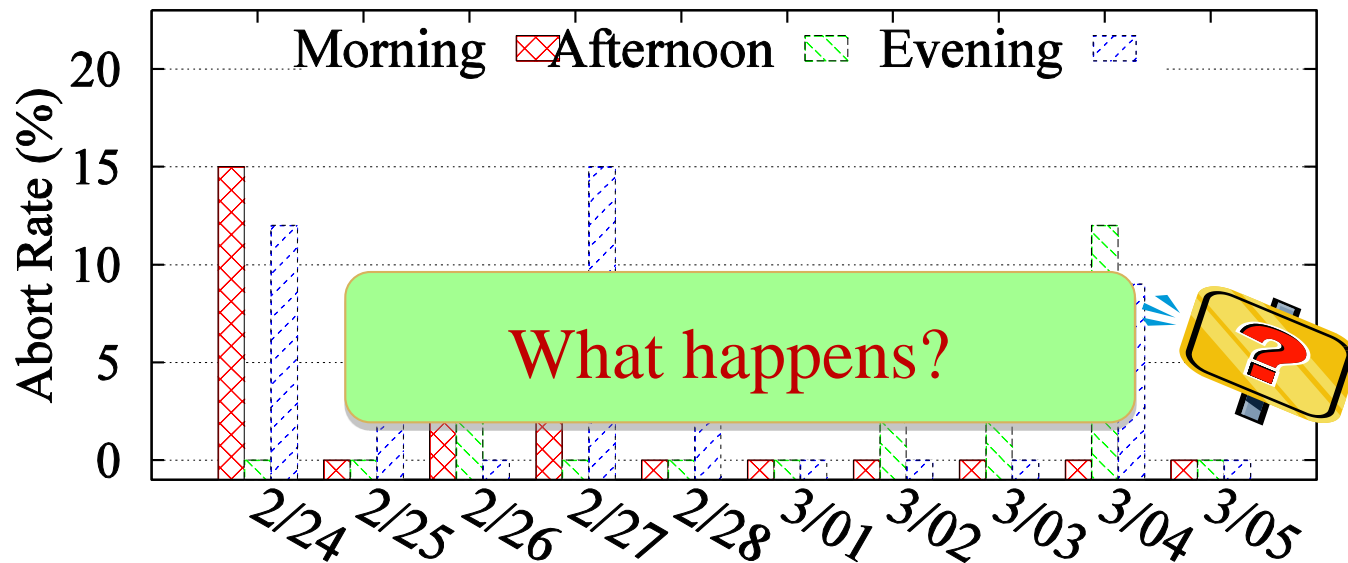


- We find that **Browsing, Gmail, FTP, Skype** and **Facebook** may abort due to CSFB calls.
 - ▣ **Browsing/Facebook**: content is not displayed
 - ▣ **FTP/Gmail**: downloading is terminated
 - ▣ **Skype**: voice call is aborted

How Often Applications Abort

19

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



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

Detached

- The users are implicitly detached by carriers and lose 3G/4G LTE connectivity.

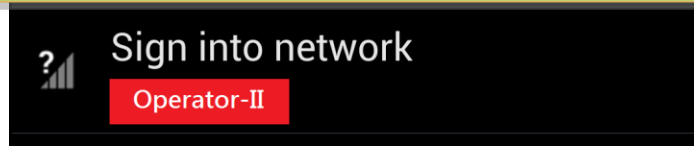
Seconds	Carrier Name	EVENT	Network Type	CID	RSSI	UE's IP
52.84	OP-I	CALL	HANG UP			10.xx.xx.51
53.41	OP-I	NET	UMTS	5****075	-67	10.xx.xx.51
54.30	OP-I	NET	UMTS	5****075	-67	10.xx.xx.51
55.26	Unknown	NET	Unknown	n/a	-113	n/a
56.28	Unknown	NET	Unknown	n/a	-113	n/a
...
69.26	OP-I	NET	LTE	1*****223	-70	10.yy.yy.11

Detached → (points to the 'Unknown' rows)

Reattached → (points to the 'OP-I' row at 69.26)

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

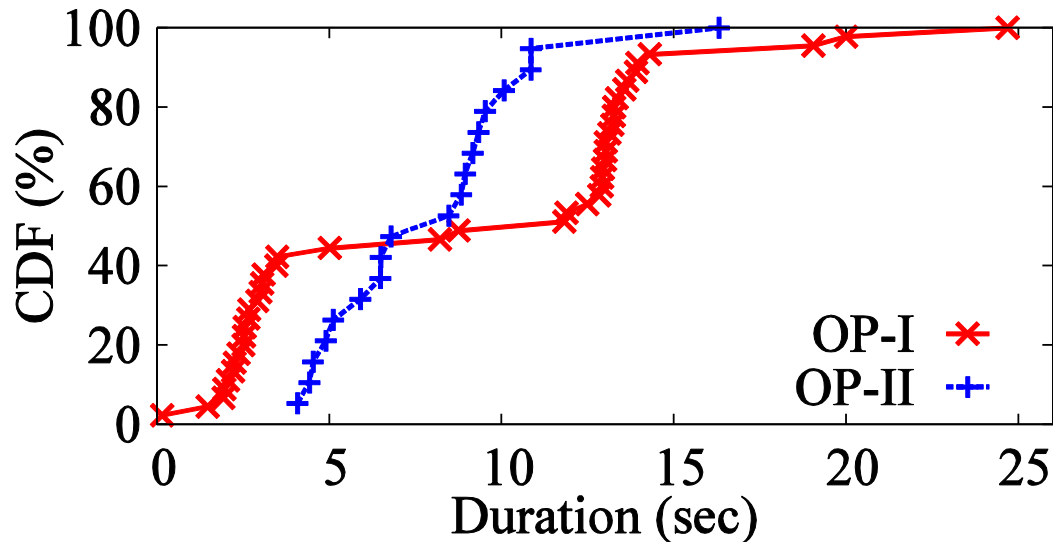
How long does it recover the connectivity?



Resign into network (OP-II).

Reattach Duration

21



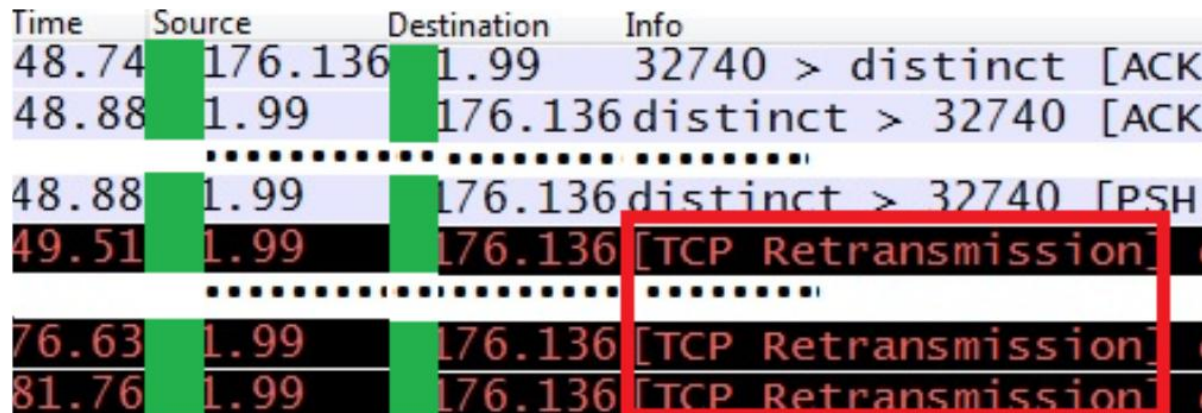
- For OP-I, **95%** of re-attaches finish within **11** seconds.
- For OP-II, **90%** of re-attaches finish within **15** seconds.

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

Invalid TCP retransmission

22

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



The image shows a Wireshark packet capture with columns for Time, Source, Destination, and Info. The first packet at 48.74s is an ACK from 176.136.1.99 to 176.136.1.99. The second packet at 48.88s is a PSH packet from 176.136.1.99 to 176.136.1.99. The third packet at 49.51s is a retransmission from 176.136.1.99 to 176.136.1.99, highlighted with a red box. The fourth packet at 76.63s is another retransmission from 176.136.1.99 to 176.136.1.99, also highlighted with a red box. The fifth packet at 81.76s is a third retransmission from 176.136.1.99 to 176.136.1.99, also highlighted with a red box.

Time	Source	Destination	Info
48.74	176.136.1.99	176.136.1.99	32740 > distinct [ACK]
48.88	176.136.1.99	176.136.1.99	distinct > 32740 [ACK]
48.88	176.136.1.99	176.136.1.99	distinct > 32740 [PSH]
49.51	176.136.1.99	176.136.1.99	[TCP Retransmission]
76.63	176.136.1.99	176.136.1.99	[TCP Retransmission]
81.76	176.136.1.99	176.136.1.99	[TCP Retransmission]

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.

23

Missed Call Due To Data Service

Miss Call

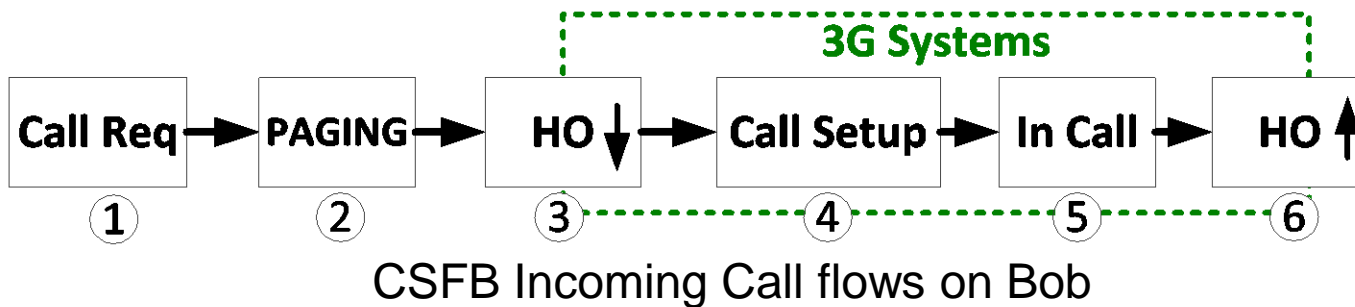
24

- 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

25



- 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.

26

Insights & Solutions

Insights

27

- For throughput slump
 - ▣ Temporary rate slumps to 0 Mbps is caused by handovers which are requested by CSFB standards and are inevitable.
 - ▣ Perfect solution may not be available.
- 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** or **cell reselection** 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

28

- 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 freely launch tons of handovers which induce *data transmission suspension* and *over-accounting* issues to the victims.
 - ▣ Introduce significant signaling overhead to operators

Solutions

- For throughput slump
 - ▣ Middle-box approach to shorten transmission recovery time
- For loss of 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 15s).
- For miss call due to PS service
 - ▣ Defer the notification of user alerting sent to caller until the callee has been successfully handedover 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 **implicitly detached** by operators after CSFB call ends
 - Applications abort due to unsuccessful receipt of packets from their applications servers.
- Users may miss voice call without indications because **alerting tone early comes** to caller.

Questions?