LTE security and protocol exploits

Roger Piqueras Jover
Wireless Security Research Scientist – Security Architecture – Bloomberg LP

ShmooCon – January 2016

About me

- Wireless Security Researcher (aka Security Architect) at Bloomberg LP
  - http://www.bloomberg.com/company/announcements/mobile-security-a-conversation-with-roger-piqueras-jover/
- Formerly (5 years) Principal Member of Technical Staff at AT&T Security Research
  - http://src.att.com/projects/index.html
- Mobile/wireless network security research
  - LTE security and protocol exploits
  - Advanced radio jamming
  - Control plane signaling scalability in mobile networks
  - 5G mobile networks and new mobile core architectures
- If it communicates wirelessly, I am interested in its security
  - Bluetooth and BLE
  - 802.11
  - Zigbee, Zigwave
  - LoRa, SIgFox…
- More details
  - http://www.ee.columbia.edu/~roger/ - @rgoestotheshows

Mobile network security

- Often thought at the “app” layer
  - Certificates
  - Encryption
  - SSL
  - Recent examples
    - iOS SSL bug
    - Android malware
    - XcodeGhost iOS infected apps
    - Long etc

- My areas of interest
  - PHY layer
  - “Layer 2” protocols (RRC, NAS, etc)
  - Circuit-switched mobile core architecture for packet-switched traffic → No bueno!
  - Recent examples
    - LTE jamming
    - Low-cost LTE IMSI catchers and protocol exploits
    - IM app causes huge mobile operators outage
    - Mobile operators trouble with “signaling storms”

Mobile network security

The first mobile networks were not designed with a strong security focus (no support for encryption in 1G!!!)

GSM	3G	4G LTE
"Old" encryption Device authentication	Strong encryption Mutual authentication	Stronger encryption Mutual authentication

Basic security principles

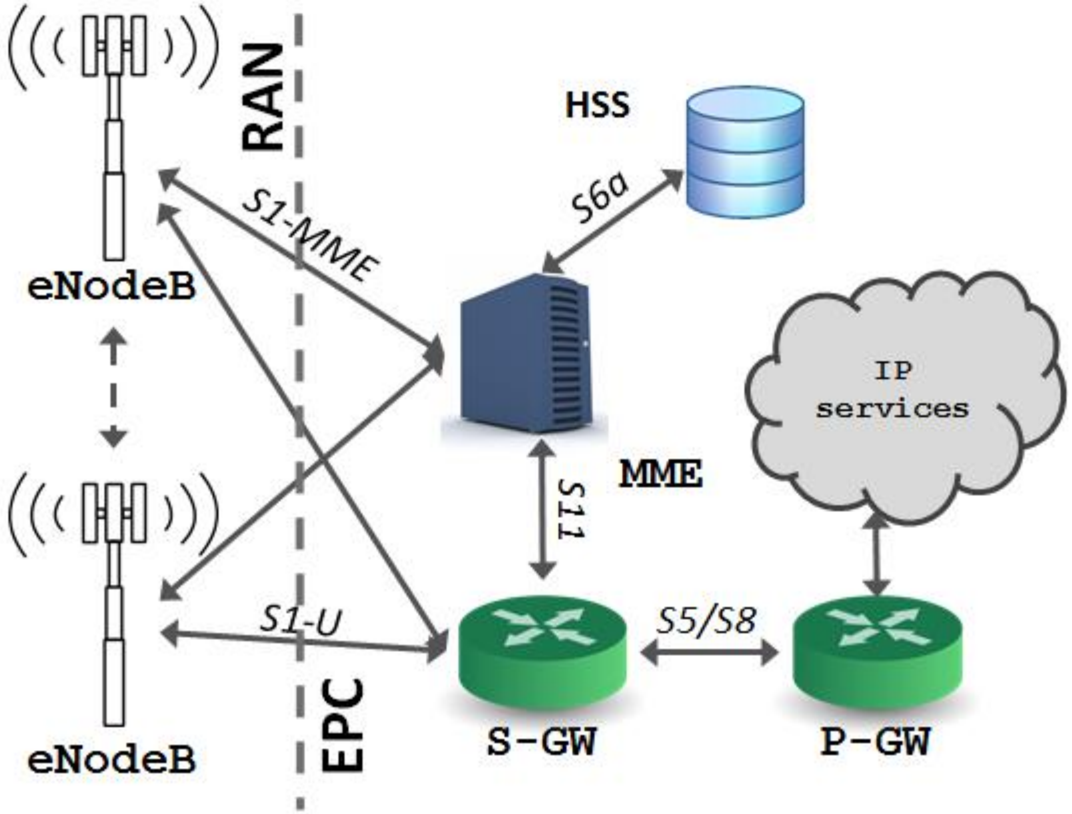
- Confidentiality
- Authentication
- Availability

Confidentiality, Authentication → Protecting user data

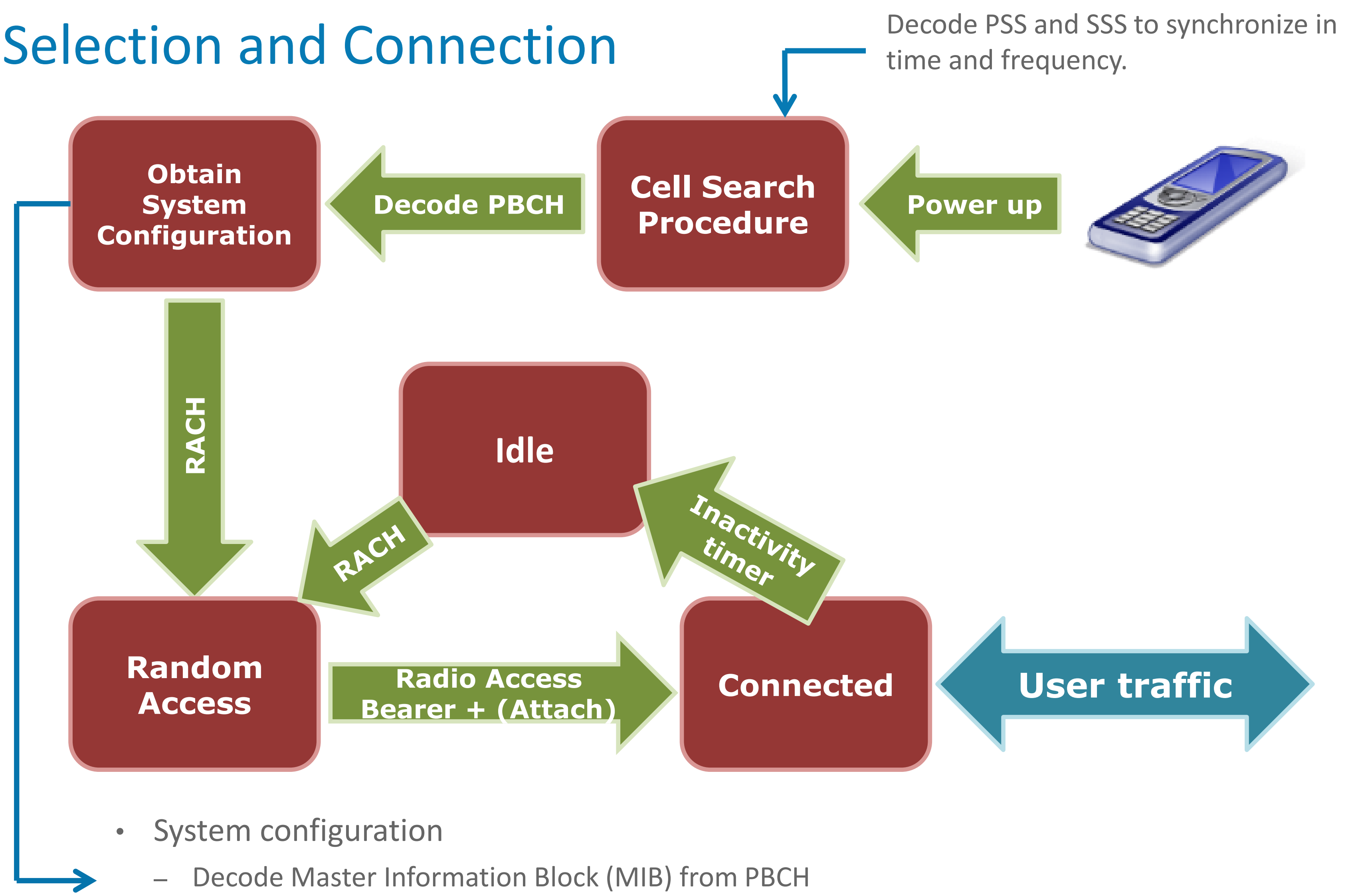
Availability → Mobile connectivity availability against security threats

LTE basics…

LTE mobile network architecture

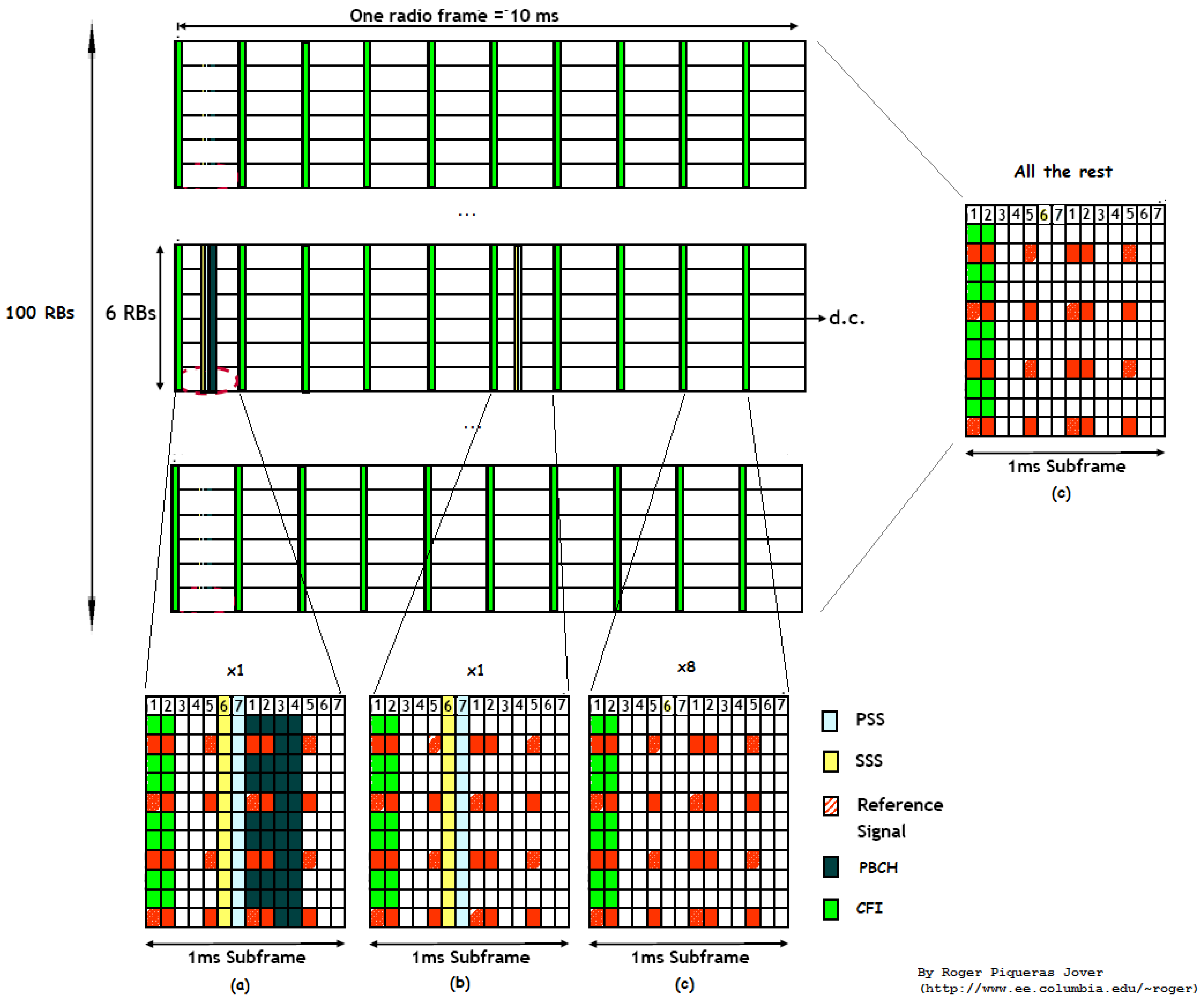


LTE Cell Selection and Connection



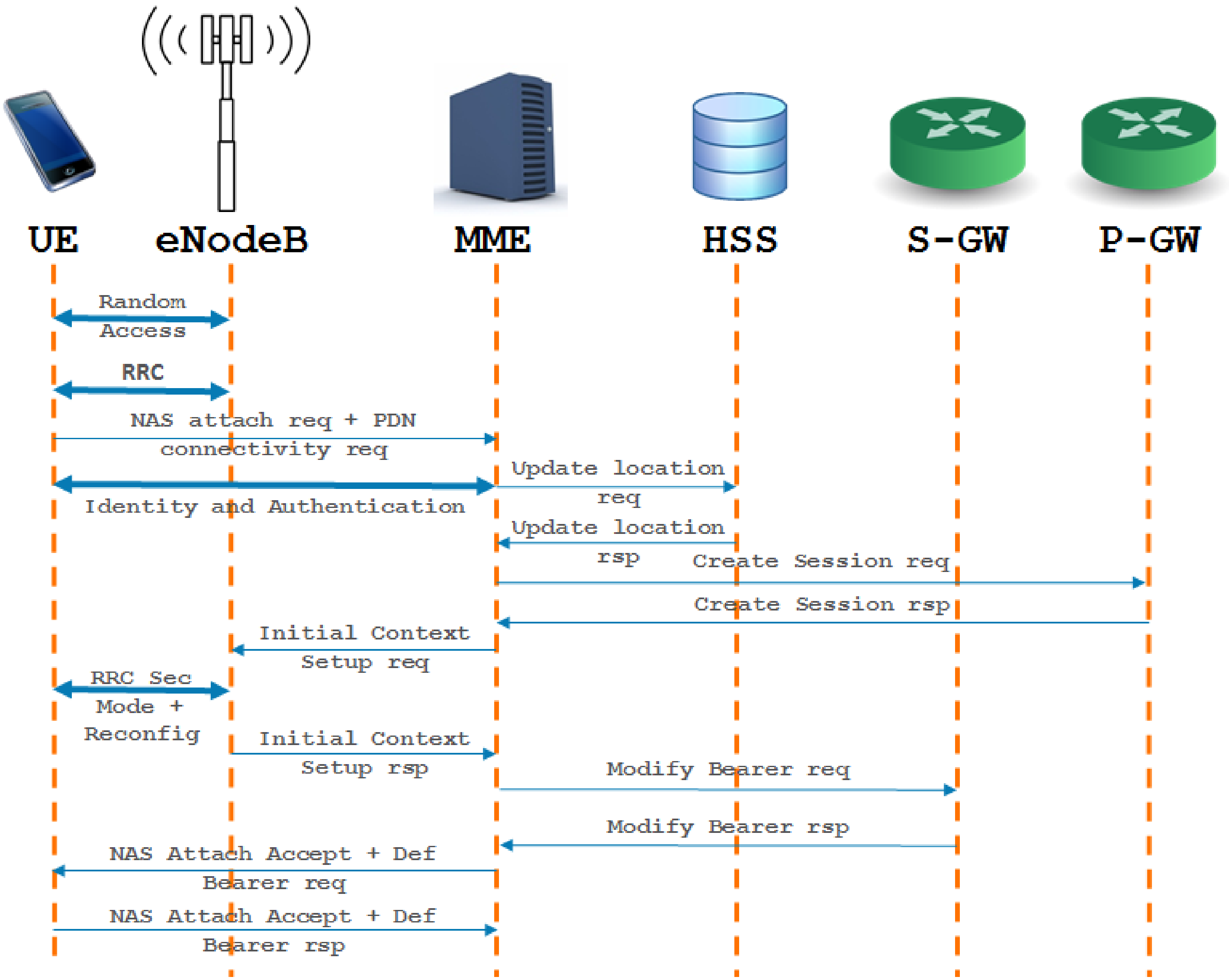
- System configuration
  - Decode Master Information Block (MIB) from PBCH
  - Decode System Information Blocks (SIBs) from PDSCH

LTE frame



One radio frame = 10 ms
100 RBs
6 RBs
d.c.
All the rest
1ms Subframe
(c)
x1
x1
x8
1ms Subframe
(a)
1ms Subframe
(b)
1ms Subframe
(c)
PSS
SSS
Reference Signal
PBCH
CFI
By Roger Piqueras Jover
(http://www.ee.columbia.edu/~roger)

LTE NAS Attach procedure



Mobile network user/device identifiers

IMEI – “Serial number” of the device

IMSI – secret id of the SIM that should never be disclosed
TMSI – temporary id used by the network once it knows who you are

MSISDN – Your phone number.

LTE security and protocol exploits…

LTE security and protocol exploits

- Sniffing base station and network configuration broadcast messages
- LTE security
- LTE IMSI catchers
- Mapping of {phone number, TMSI, IMSI}
- Bricking/blocking devices and SIMs
- LTE location leaks and tracking target devices

Sniffing base station configuration

```
Subframe: 0
  BCCH-BCH-Message
    message
      dl-Bandwidth: n50
      phich-Config
        phich-Duration: normal
        phich-Resource: one
      systemFrameNumber: {8
bits|0x17}
      spare: {10 bits|0x0000|Right
Aligned}
```

LTE PBCH MIB packet

Sniffing base station configuration

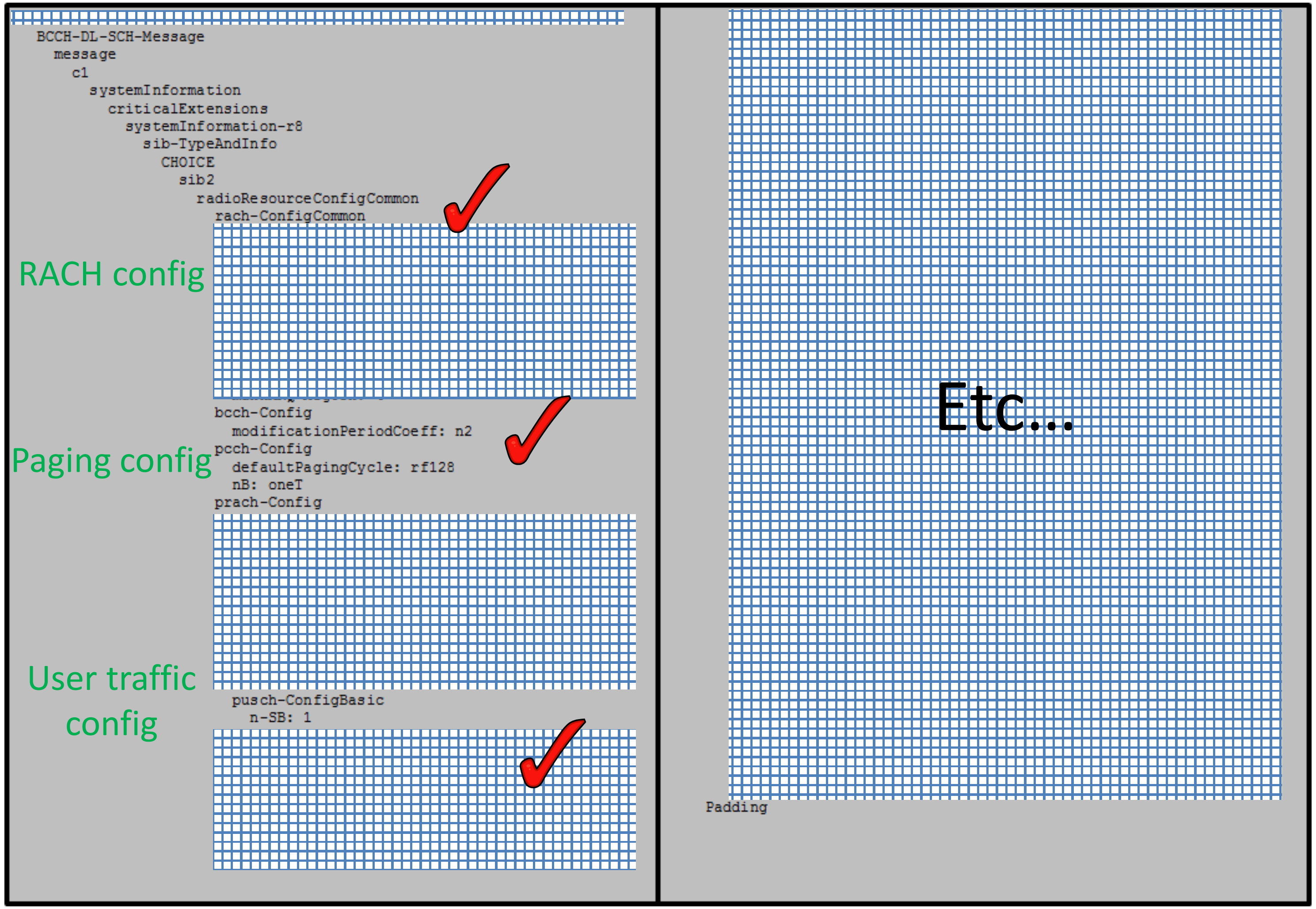
```
[redacted]
  BCCH-DL-SCH-Message
    message
      c1
        systemInformationBlockType1
          cellAccessRelatedInfo
            plmn-IdentityList
              PLMN-IdentityInfo
                plmn-Identity
                  mcc
                    MCC-MNC-Digit: 3
                    MCC-MNC-Digit: 1
                    MCC-MNC-Digit: 0
                  mnc
                    MCC-MNC-Digit:[redacted]
                    MCC-MNC-Digit:[redacted]
                    MCC-MNC-Digit:[redacted]
                cellReservedForOperatorUse: reserved
            trackingAreaCode: {16 bits|[redacted]
            cellIdentity: {28 bits|[redacted]|Right Aligned}
            cellBarred: notBarred
            intraFreqReselection: allowed
            csg-Indication: false
          cellSelectionInfo
            q-RxLevMin: -[redacted]
          freqBandIndicator: [redacted]
          schedulingInfoList
            SchedulingInfo
              si-Periodicity: rf8
              sib-MappingInfo
                SIB-Type: sibType3
          si-WindowLength: ms10
          systemInfoValueTag: 11
    Padding
```

Mobile operator

Cell ID

RX power to select that cell

Sniffing base station configuration



LTE PDSCH SIB2/3 packet

Sniffing base station configuration

- MIB/SIB messages are necessary for the operation of the network
  - Some things must be sent in the clear (i.e. a device connecting for the first time)
  - But perhaps not everything
- Things an attacker can learn from MIB and SIB messages
  - Optimal tx power for a rogue base station (no need to set up your USRP to its max tx power)
  - High priority frequencies to force priority cell reselection
  - Mobile operator who owns that tower
  - Tracking Area of the legitimate cell (use a different one in your rogue eNodeB to force TAU update messages)
  - Mapping of signaling channels
  - Paging channel mapping and paging configuration
  - Etc

LTE security

Name	Start time	Dl/Ul	Cell	Cell ID	Frame	Subf	RCE	Power	Length	Errs	Retrans	Decr	Valid	Sf RSSI	SINR
RACH	01:32:03.954999	U	[redacted]		440	1	-16.64	-57.98	0						16.64
MAC Random Access Response	01:32:03.958999	D	[redacted]		440	5	-16.41	-45.73	7	OK				-39.20	16.41
RRCConnectionRequest	01:32:03.964999	U	[redacted]		441	1	-23.85	-51.14	6	OK					23.85
RRCConnectionSetup	01:32:03.979999	D	[redacted]		442	6	-15.11	-42.21	26	OK				-38.72	15.11
RRCConnectionSetupComplete	01:32:04.013999	U	[redacted]		446	0			56	OK					
Attach Request	01:32:04.013999	U	[redacted]		446	0	-25.25	-49.36	53	OK					25.25
PDN Connectivity Request	01:32:04.013999	U	[redacted]		446	0	-25.25	-49.36	36	OK					25.25
DLInformationTransfer	01:32:04.088999	D	[redacted]		453	5			39	OK					
Authentication Request	01:32:04.088999	D	[redacted]		453	5	-15.00	-41.33	36	OK				-38.44	15.00
ULInformationTransfer	01:32:04.225999	U	[redacted]		467	2			22	OK					
Authentication Response	01:32:04.225999	U	[redacted]		467	2	-20.80	-53.66	19	OK					20.80
DLInformationTransfer	01:32:04.267999	D	[redacted]		471	4			17	OK					
Security Protected NAS Message	01:32:04.267999	D	[redacted]		471	4	-15.52	-44.04	14	OK		Not...	No...	-39.22	15.52
Security Mode Command	01:32:04.267999	D	[redacted]		471	4	-15.52	-44.04	8	OK				-39.22	15.52
ULInformationTransfer	01:32:04.285999	U	[redacted]		473	2			22	OK					
Security Protected NAS Message	01:32:04.285999	U	[redacted]		473	2	-22.49	-52.16	19	OK		No...	No...		22.49
Unknown NAS	01:32:04.285999	U	[redacted]		473	2	-22.49	-52.16	13	OK					22.49
DLInformationTransfer	01:32:04.327999	D	[redacted]		477	4			12	OK					
Security Protected NAS Message	01:32:04.327999	D	[redacted]		477	4	-14.73	-45.68	9	OK		No...	No...	-39.27	14.73
Unknown NAS	01:32:04.327999	D	[redacted]		477	4	-14.73	-45.68	3	OK				-39.27	14.73
ULInformationTransfer	01:32:04.345999	U	[redacted]		479	2			24	OK					
Security Protected NAS Message	01:32:04.345999	U	[redacted]		479	2	-21.36	-53.39	21	OK		No...	No...		21.36
Unknown NAS	01:32:04.345999	U	[redacted]		479	2	-21.36	-53.39	15	OK					21.36
SecurityModeCommand	01:32:04.472999	D	[redacted]		491	9			3	OK					
Ciphered RRC	01:32:04.495999	U	[redacted]		494	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.501999	D	[redacted]		494	8			3	OK		No...	No...		
Ciphered RRC	01:32:04.515999	U	[redacted]		496	2			18	OK		No...	No...		
Ciphered RRC	01:32:04.536999	D	[redacted]		498	3			165	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U	[redacted]		502	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U	[redacted]		502	2			16	OK		No...	No...		
Ciphered RRC	01:32:04.604999	D	[redacted]		505	1			30	OK		No...	No...		
Ciphered data	01:32:14.426997	U	[redacted]		463	3			96	OK		No...			
Ciphered data	01:32:14.475997	U	[redacted]		468	2			40	OK		No...			
Ciphered data	01:32:14.513997	U	[redacted]		472	0			96	OK		No...			

RACH handshake between UE and eNB

RRC handshake between UE and eNB

Connection setup (authentication, set-up of encryption, tunnel set-up, etc)

Encrypted traffic

LTE security

IntelliJudge

Count	Name	Start time	Dl/Ul	Cell ID	Frame	RNTI	RCE	Power	Errs
1	RACH	00:04:42.942818	U		651		-6.42	-64.65	
2	MAC Random Access Response	00:04:42.946818	D		651		-8.50	-45.23	OK
3	RRCConnectionRequest	00:04:42.952818	U		652		-19.19	-56.46	OK
4	RRCConnectionSetup	00:04:42.967818	D		653		-9.07	-43.18	OK
5	RRCConnectionSetupComplete	00:04:43.001818	U		657				OK
6	Attach Request	00:04:43.001818	U		657				OK
7	PDN Connectivity Request	00:04:43.001818	U		657		-17.59	-60.11	OK
8	DLInformationTransfer	00:04:43.080818	D		664				OK
9	Authentication Request	00:04:43.080818	D		664		-8.86	-42.27	OK
10	ULInformationTransfer	00:04:43.213818	U		678				OK
11	Authentication Response	00:04:43.213818	U		678		-12.51	-65.43	OK
12	DLInformationTransfer	00:04:43.258818	D		682				OK
13	Security Protected NAS Message	00:04:43.258818	D		682		-8.90	-44.51	OK
14	Security Mode Command	00:04:43.258818	D		682		-8.90	-44.51	OK
15	ULInformationTransfer	00:04:43.273818	U		684				OK
16	Security Protected NAS Message	00:04:43.273818	U		684		-11.14	-64.93	OK
17	Unknown NAS	00:04:43.273818	U		684		-11.14	-64.93	OK
18	DLInformationTransfer	00:04:43.318818	D		688				OK
19	Security Protected NAS Message	00:04:43.318818	D		688		-8.88	-45.69	OK
20	Unknown NAS	00:04:43.318818	D		688		-8.88	-45.69	OK
21	ULInformationTransfer	00:04:43.333818	U		690				OK
22	Security Protected NAS Message	00:04:43.333818	U		690		-11.82	-63.66	OK
23	Unknown NAS	00:04:43.333818	U		690		-11.82	-63.66	OK
24	SecurityModeCommand	00:04:43.451818	D		702				OK
25	Ciphered RRC	00:04:43.479818	D		704				OK
26	Ciphered RRC	00:04:43.503818	U		707				OK
27	Ciphered RRC	00:04:43.524818	D		709				OK
28	Ciphered RRC	00:04:43.563818	U		713				OK
29	Ciphered RRC	00:04:43.563818	U		713				OK
30	Ciphered RRC	00:04:43.594818	D		716				OK
31	Ciphered data	00:04:52.021817	D		535				OK
32	Ciphered data	00:04:52.021817	D		535				OK
33	Ciphered data	00:04:52.113817	U		544				OK
34	Ciphered data	00:04:52.153817	U		548				OK

Unencrypted and unprotected. I can sniff these messages and I can transmit them pretending to be a legitimate base station.

Other things sent in the clear:

- Measurement reports
- Measurement report requests
- (Sometimes) GPS coordinates
- HO related messages
- Paging messages
- Etc

LTE security

Regardless of mutual authentication and strong encryption, a mobile device engages in a substantial exchange of unprotected messages with *any* LTE base station (malicious or not) that advertises itself with the right broadcast information.

LTE open source implementations

- There are a few somewhat fully functional LTE open source implementations
  - OpenLTE – End to end implementation: RAN and “EPC”.
    - http://sourceforge.net/projects/openlte/
  - gr-LTE – Based on gnuradio-companion. Great for people new to software radio.
    - https://github.com/kit-cel/gr-lte
  - OpenAirInterface – Industry/Academia consortium.
    - http://www.openairinterface.org/
  - srsLTE – Almost complete implementation. Includes srsUE, device open source implementation.
    - https://github.com/srsLTE
- Hardware setup
  - USRP B210 for active rogue base station
  - **BUDGET**: USRP B210 ($1100) + GPSDO ($625) + LTE Antenna (2x$30) = **$1785**
  - Machine running Ubunutu
  - US dongles (hackRF, etc) for passive sniffing.

All LTE active radio experiments MUST be performed inside a faraday cage.

LTE traffic captures

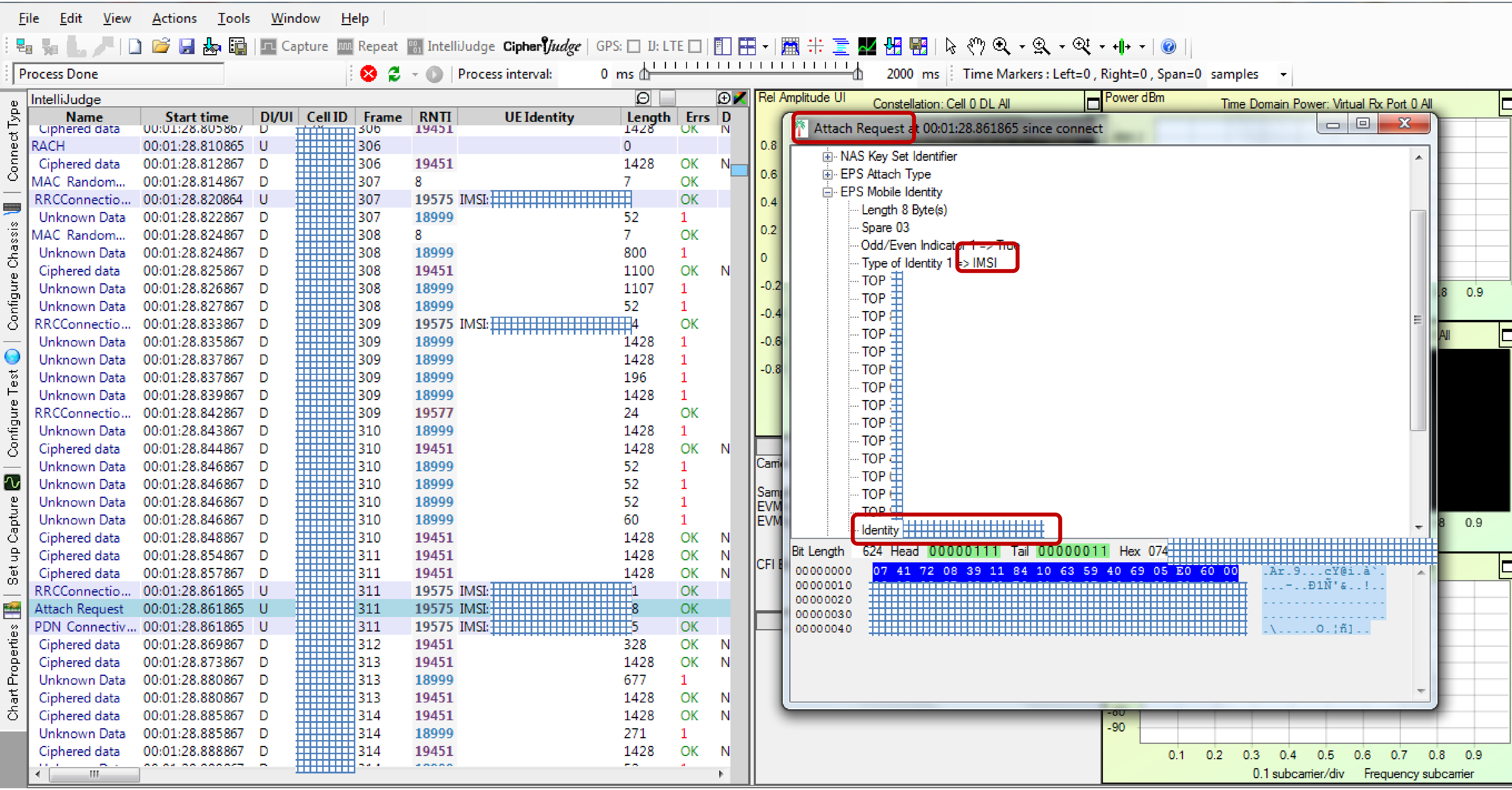
- Sanjole WaveJudge 5000 with IntelliJudge traffic processor
  - Reception and sniffing from multiple eNBs simultaneously
  - Decoding of messages at very low SNR regime
  - Retransmission of captures
  - Thanks to Sanjole for helping out and providing all the captures shown in this presentation!
  - http://www.sanjole.com/our-products/lte-analyzer/

- Other options
  - openLTE pcap traffic dump
  - WireShark LTE RRC library
  - hackRF
  - Other LTE open source implementations

LTE IMSI catcher (Stingray)

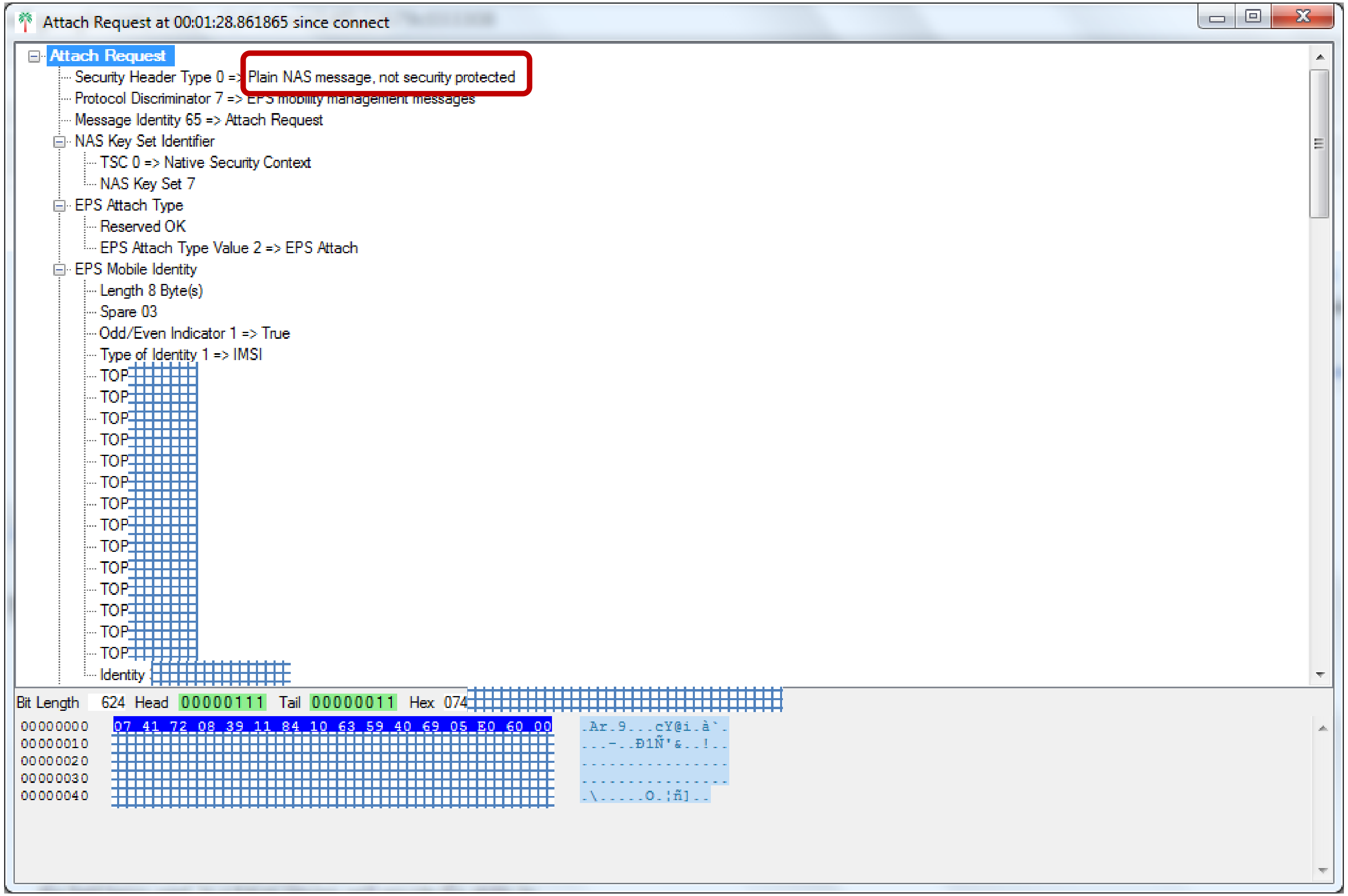
- Despite common assumptions, in LTE the IMSI is always transmitted in the clear at least once
  - If the network has never seen that UE, it must use the IMSI to claim its identity
  - A UE will trust *any* eNodeB that claims it has never seen that device (pre-authentication messages)
  - IMSI can also be transmitted in the clear in error recovery situations (very rare)
- Implementation
  - USRP B210 + Ubuntu 14.10 + gnuradio 3.7.2
  - LTE base station – OpenLTE’s LTE_fdd_eNodeB (slightly modified)
    - Added feature to record IMSI from Attach Request messages
  - Send attach reject after IMSI collection

- Stingrays also possible in LTE without need to downgrade connection to GSM



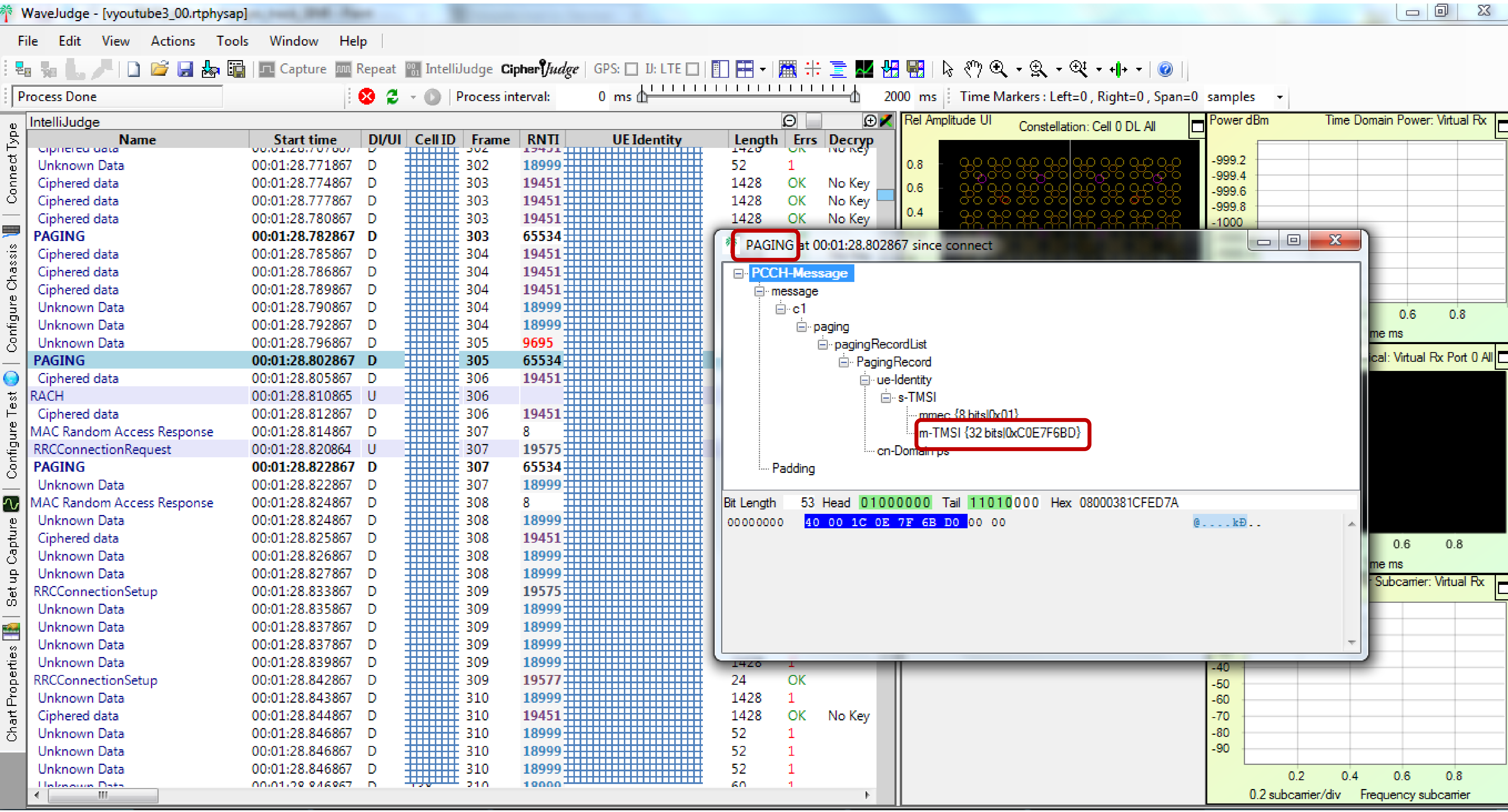
File Edit View Actions Tools Window Help
Capture Repeat IntelliJudge CipherJudge GPS: IJ: LTE
Process Done
Process interval: 0 ms 2000 ms
Time Markers : Left=0 , Right=0 , Span=0 samples
IntelliJudge
Name Start time Dl/Ul Cell ID Frame RNTI UE Identity Length Errs D
RACH 00:01:28.810865 U 306 0
Ciphered data 00:01:28.812867 D 306 19451 1428 OK N
MAC Random... 00:01:28.814867 D 307 8 7 OK
RRCConnectio... 00:01:28.820864 U 307 19575 IMSI: OK
Unknown Data 00:01:28.822867 D 307 18999 52 1
RRCConnectio... 00:01:28.861865 U 311 19575 IMSI: 1 OK
Attach Request 00:01:28.861865 U 311 19575 IMSI: 8 OK
PDN Connectiv... 00:01:28.861865 U 311 19575 IMSI: 5 OK
Attach Request at 00:01:28.861865 since connect
NAS Key Set Identifier
EPS Attach Type
EPS Mobile Identity
Length 8 Byte(s)
Spare 03
Odd/Even Indicator 1 => True
Type of Identity 1 => IMSI
TOP
Identity
Bit Length 624 Head 00000111 Tail 00000011 Hex 074
00000000 07 41 72 08 39 11 84 10 63 59 40 69 05 E0 60 00
00000010
00000020
00000030
00000040
Rel Amplitude UI
Constellation: Cell 0 DL All
Power dBm
Time Domain Power: Virtual Rx Port 0 All
0.1 subcarrier/div
Frequency subcarrier
Connect Type
Configure Chassis
Configure Test
Set up Capture
Chart Properties

LTE IMSI catcher



Mapping {phone number, TMSI, IMSI}

- Given a phone number
  - Paging messages broadcasted in the clear and addressed to the TMSI
  - Silent text messages to target device
- Setting up a rogue base station
  - UE will attempt first with TMSI
  - Then intercept IMSI
- Cool new tricks in a paper I will discuss shortly…


WaveJudge - [vyoutube3_00.rtphysap]
File Edit View Actions Tools Window Help
Process Done
Process interval: 0 ms 2000 ms
Time Markers : Left=0 , Right=0 , Span=0 samples
IntelliJudge
Name Start time DI/UI Cell ID Frame RNTI UE Identity Length Errs Decryp
PAGING 00:01:28.782867 D 303 65534
PAGING 00:01:28.802867 D 305 65534
RACH 00:01:28.810865 U 306
MAC Random Access Response 00:01:28.814867 D 307 8
RRCConnectionRequest 00:01:28.820864 U 307 19575
PAGING 00:01:28.822867 D 307 65534
RRCConnectionSetup 00:01:28.833867 D 309 19575
RRCConnectionSetup 00:01:28.842867 D 309 19577
PAGING at 00:01:28.802867 since connect
PCCH-Message
message
c1
paging
pagingRecordList
PagingRecord
ue-Identity
s-TMSI
mmec {8 bits|0x01}
m-TMSI {32 bits|0xC0E7F6BD}
cn-Domain ps
Padding
Bit Length 53 Head 01000000 Tail 11010000 Hex 08000381CFED7A
00000000 40 00 1C 0E 7F 6B D0 00 00
Rel Amplitude UI
Constellation: Cell 0 DL All
Power dBm
Time Domain Power: Virtual Rx
0.2 subcarrier/div Frequency subcarrier

(Intermission) - Some excellent related work

- A team at TU Berlin, University of Helsinki and Aalto University doing excellent work in the same area
  - More results on SIM/device bricking with Attach/TAU reject messages
  - LTE location leaks
  - Detailed implementation and results
  - Paper to be presented at NDSS: http://arxiv.org/abs/1510.07563

- Prof. Seifert's team at TU Berlin responsible for other previous VERY COOL projects
  - Respond to phone calls and receive text messages that are intended for somebody else (USENIX 2013)
  - Preventing signaling-based attacks coming from smartphones (IEEE DSN 2012)
  - SMS baseband fuzzing (USENIX 2011)
  - Mobile botnets (MALWARE 2010)

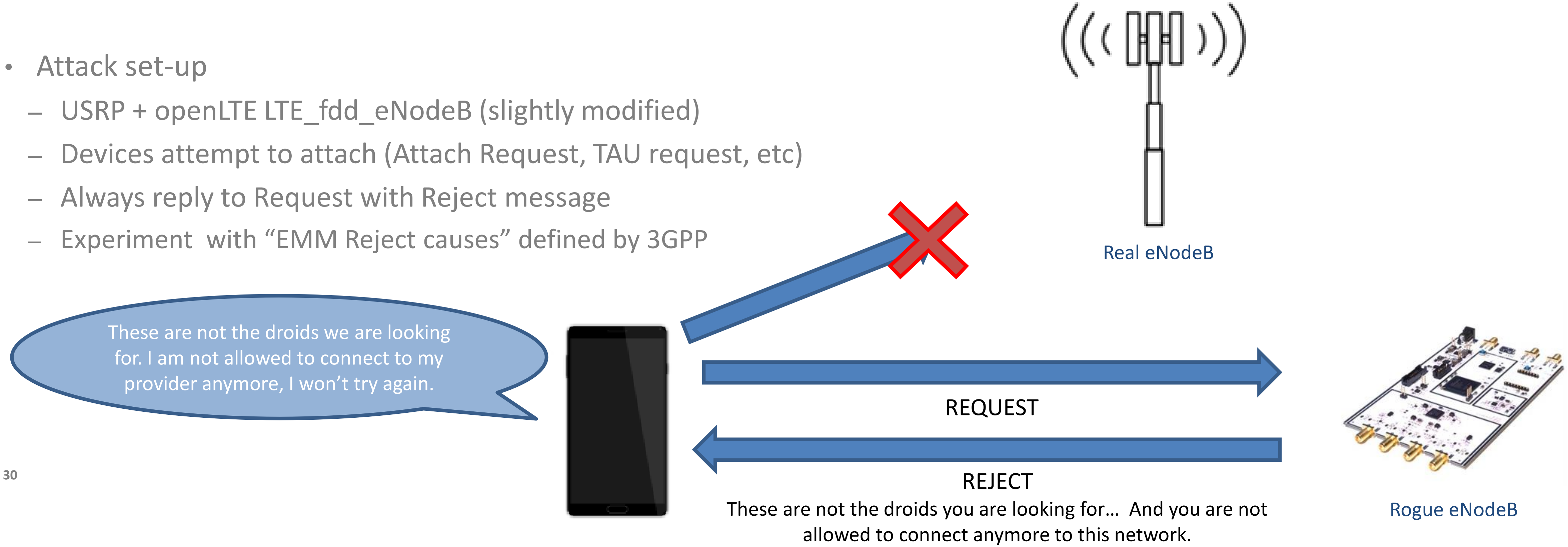
- The authors have submitted their Wireshark LTE dissectors and are being merged into the application
  - Really looking forward to this…

Device and SIM temporary block

- Attach reject and TAU (Tracking Area Update) reject messages not encrypted/integrity-protected

- Spoofing this messages one can trick a device to
  - Believe it is not allowed to connect to the network (blocked)
  - Believe it is supposed to downgrade to or only allowed to connect to GSM

- Attack set-up
  - USRP + openLTE LTE_fdd_eNodeB (slightly modified)
  - Devices attempt to attach (Attach Request, TAU request, etc)
  - Always reply to Request with Reject message
  - Experiment with “EMM Reject causes” defined by 3GPP



Device and SIM temporary block

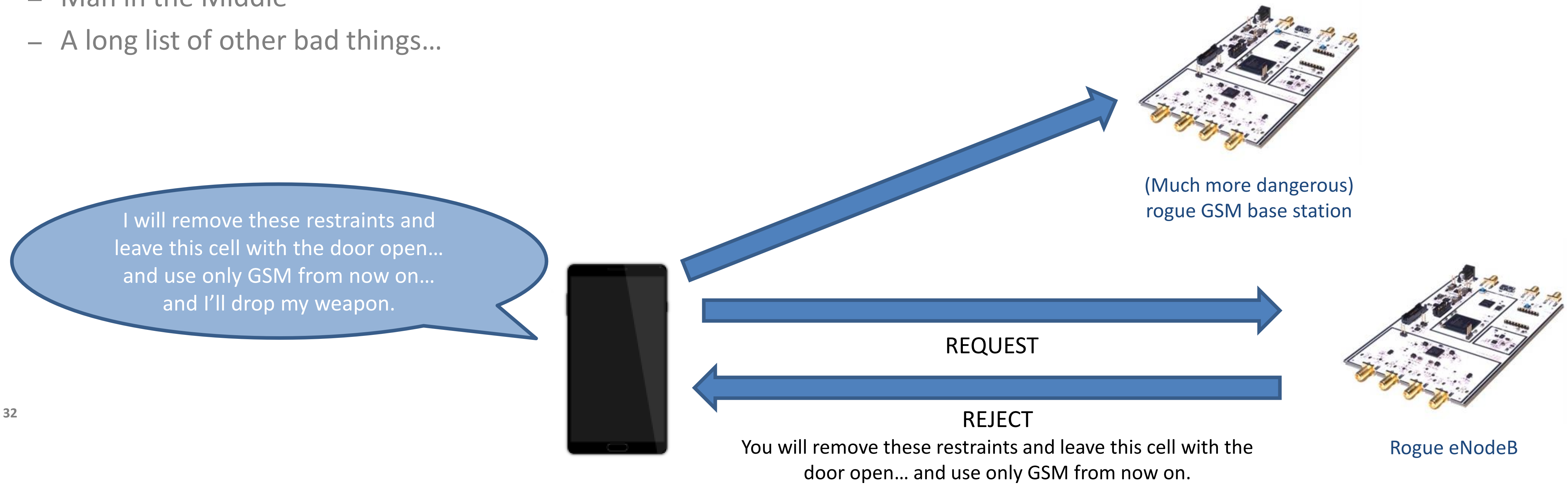
- Some results
  - **The blocking of the device/SIM is only temporary**
  - Device won't connect until rebooted
  - SIM won't connect until reboot
  - SIM/device bricked until timer T3245 expires (24 to 48 hours!)
  - Downgrade device to GSM and get it to connect to a rogue BS

- If the target is an M2M device, it could be a semi-persistent attack
  - Reboot M2M device remotely?
  - Send a technician to reset SIM?
  - Or just wait 48 hours for your M2M device to come back online…

Soft downgrade to GSM

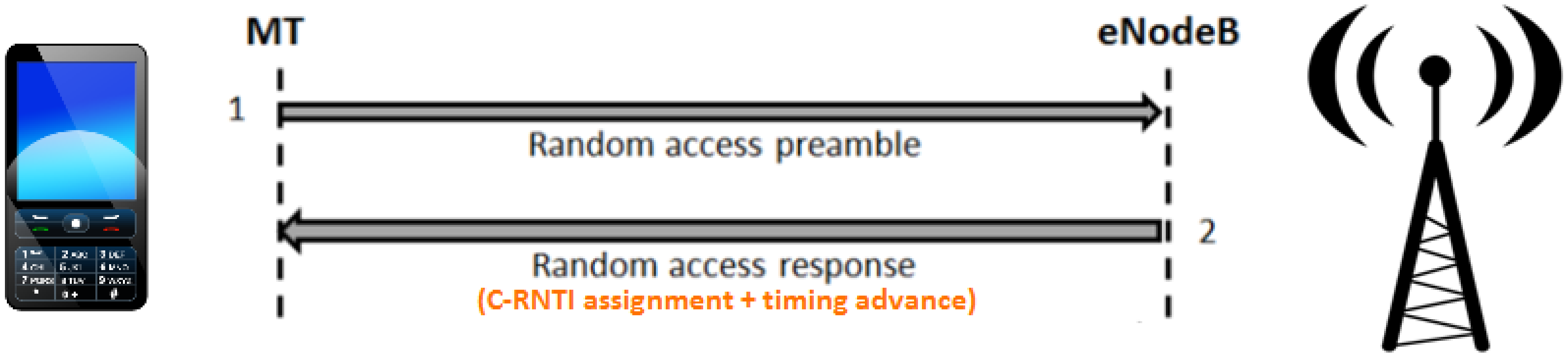
- Use similar techniques to “instruct” the phone to downgrade to GSM
  - Only GSM services allowed OR LTE and 3G not allowed

- Once at GSM, the phone to connects to your rogue base station
  - Bruteforce the encryption
  - Listen to phone calls, read text messages
  - Man in the Middle
  - A long list of other bad things…

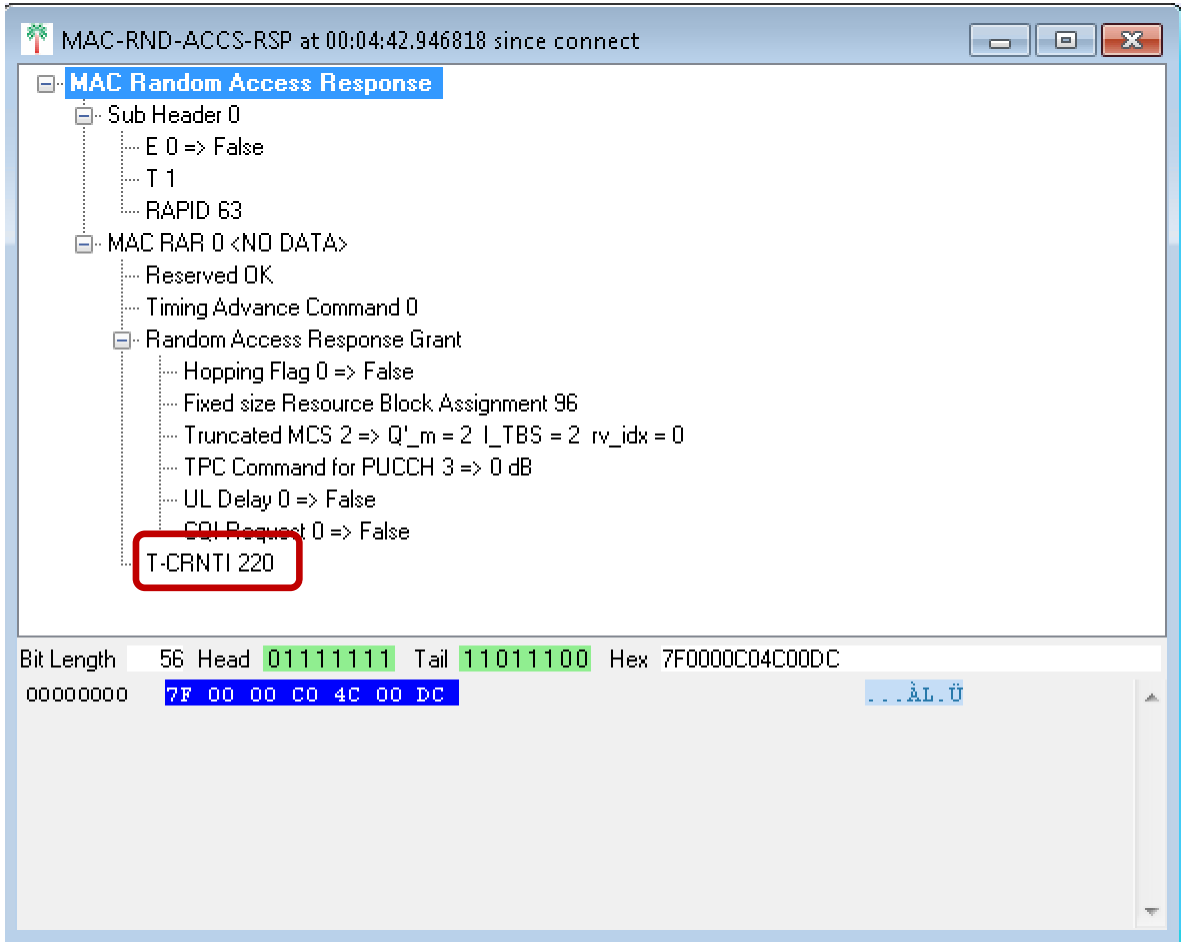


LTE location leaks and potential target device tracking

- RNTI
  - PHY layer id sent in the clear in EVERY SINGLE packet, both UL and DL
  - Identifies uniquely every UE within a cell
  - Changes infrequently
    - Based on several captures in the NYC and Honolulu areas
    - No distinguishable behavior per operator or per base station manufacturer
  - Assigned by the network in the MAC RAR response to the RACH preamble



LTE location leaks and potential target device tracking



LTE location leaks and potential target device tracking

Name	Start time	DI/UI	Cell ID	Frame	RNTI	UE Identity	Length	Errs
RACH	00:02:26.830866	U		988			0	
MAC Random Access Response	00:02:26.834868	D		989	8		7	OK
RRCConnectionRequest	00:02:26.840866	U		989	19841		6	OK
RRCConnectionSetup	00:02:26.853868	D		991	19841		24	OK
Ciphered data	00:02:26.855868	D		991	**19681**		1280	OK
Ciphered data	00:02:26.856868	D		991	**19681**		1280	OK
Ciphered data	00:02:26.857868	D		991	**19681**		1280	OK
Ciphered data	00:02:26.858868	D		991	**19681**		1280	OK
Unknown Data	00:02:26.871868	D		992	12381		52	1
Unknown Data	00:02:26.871868	D		992	12381		109	1
RRCConnectionSetupComplete	00:02:26.874866	U		993	19841		7	OK
Service Request	00:02:26.874866	U		993	19841		4	OK
Ciphered data	00:02:26.894868	D		995	**19681**		1280	OK
Ciphered data	00:02:26.895868	D		995	**19681**		1280	OK
Ciphered data	00:02:26.900868	D		995	**19681**		1280	OK
Ciphered data	00:02:26.901868	D		995	**19681**		1280	OK
Ciphered data	00:02:26.902868	D		995	**19681**		1280	OK
SecurityModeCommand	00:02:26.909868	D		996	19841		3	OK
Ciphered data	00:02:26.931868	D		998	**19681**		1280	OK
Ciphered data	00:02:26.932868	D		998	**19681**		1280	OK
SecurityModeComplete	00:02:26.932866	U		998	19841		2	OK
Ciphered data	00:02:26.933868	D		999	**19681**		1280	OK
Ciphered data	00:02:26.934868	D		999	**19681**		1280	OK
Ciphered data	00:02:26.952868	D		1000	**19681**		1280	OK
Ciphered data	00:02:26.953868	D		1001	**19681**		1280	OK
Ciphered data	00:02:26.954868	D		1001	**19681**		1280	OK
Ciphered data	00:02:26.955868	D		1001	**19681**		1280	OK
RRCConnectionReconfiguration	00:02:26.957868	D		1001	19841		84	OK
RRCConnectionReconfigurationC...	00:02:26.972866	U		1002	19841		2	OK
IP Data (IPv4 UDP)	00:02:26.972866	U		1002	19841		70	OK
Ciphered data	00:02:26.974868	D		1003	**19681**		1280	OK
Ciphered data	00:02:26.975868	D		1003	**1[illegible]81**		404	OK
MAC Random Access Response	00:02:26.984868	D		1004			7	OK
RRCConnectionSetup	00:02:27.003868	D		1006	1[illegible]3		24	OK
Unknown Data	00:02:27.020868	D		1007	1[illegible]1		1428	1
Ciphered RRC	00:02:27.021868	D		1007	1[illegible]5		2	OK

LTE location leaks and potential target device tracking

- Potential RNTI tracking use cases
  - Know how long you stay at a given location
    - and meanwhile someone robs your house…
  - Estimate the UL and DL load of a given device
    - Signaling traffic on the air interface << Data traffic on the air interface
  - Potentially identify the hot-spot/access point in an LTE-based ad-hoc network

- Phone # - TMSI – RNTI mapping is trivial
  - If the passive sniffer is within the same cell/sector as the target

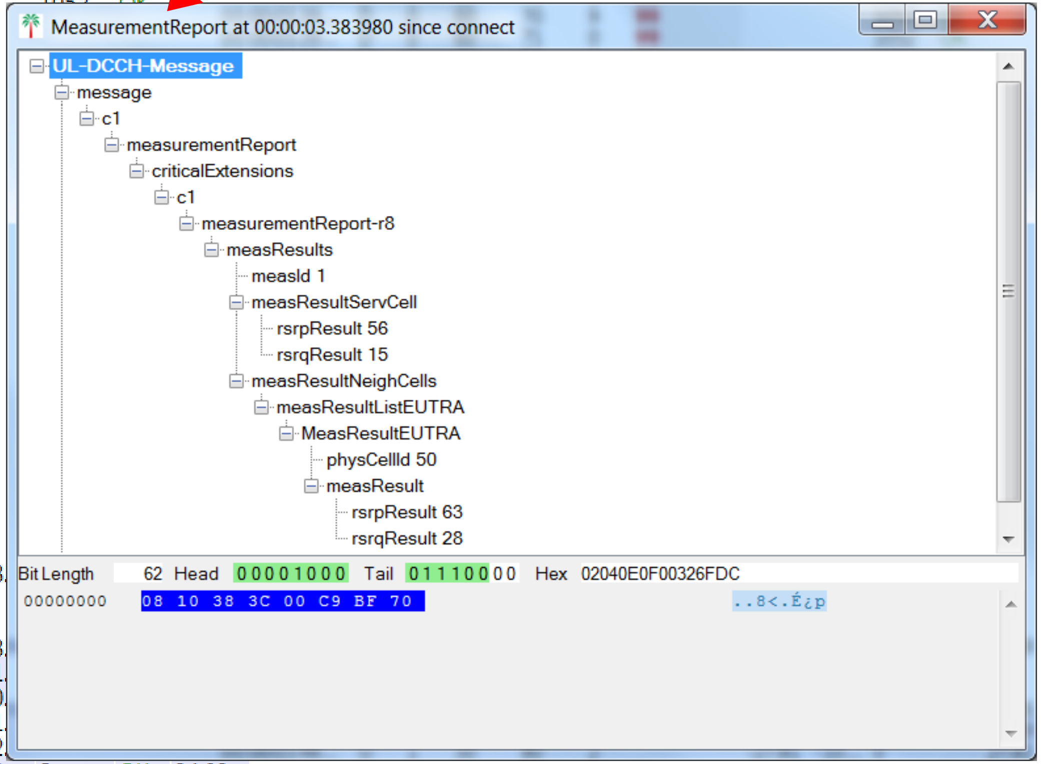
Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8	99			1052	OK	
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9	99	-33.59	-48....	108	OK	33.59
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0	99			1052	OK	
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3	99	-27.26	-48....	108	OK	27.26
RACH	00:00:03.48...	U	0	60	80	2		-27.49	-11....	0		27.49
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

Cell ID = 60

Cell ID = 50

Handoff between cell 60 and cell 50

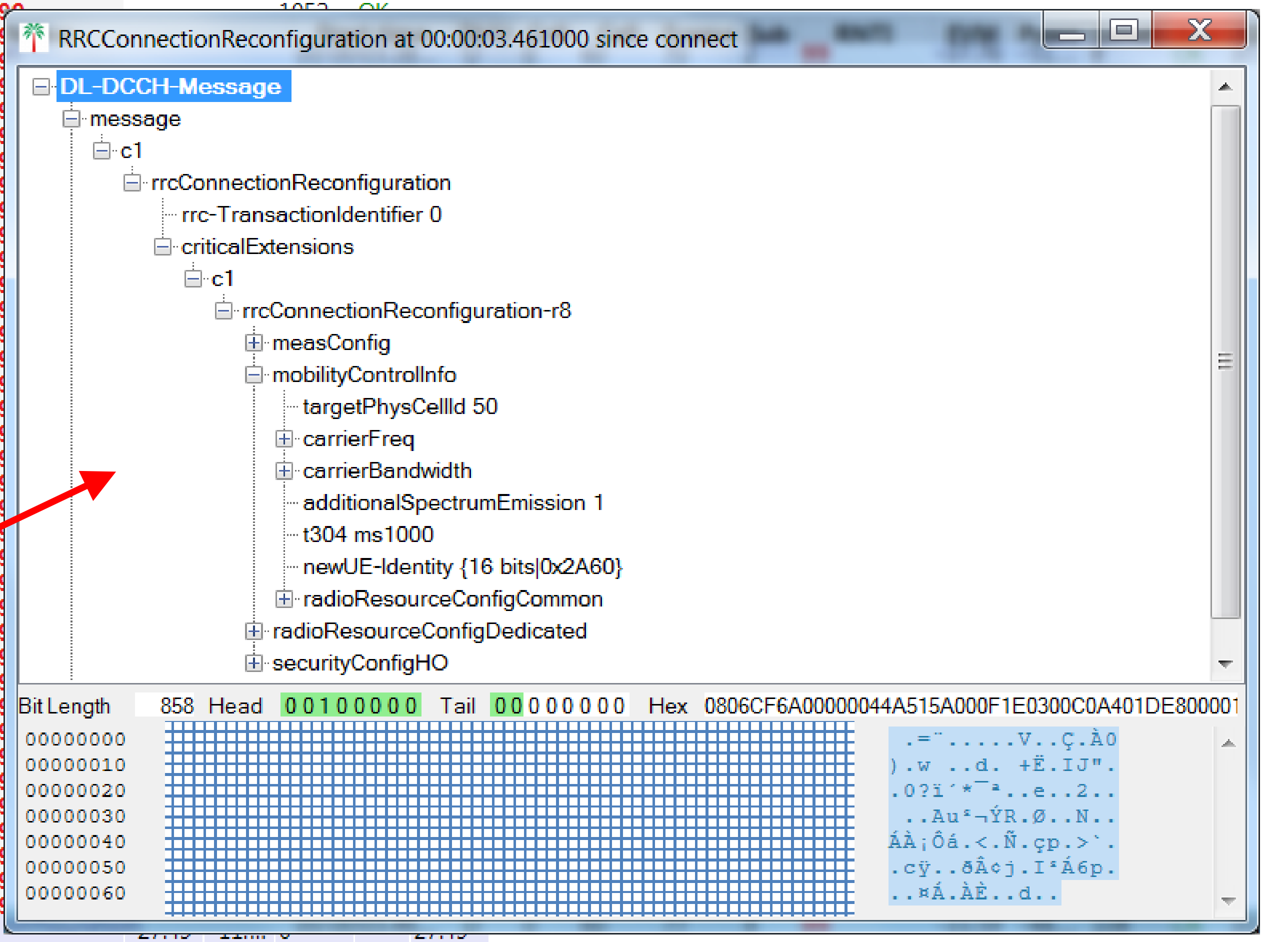
Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3	99					
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4	99					
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5	99					
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5	99					
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8	99					
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9	99	-33.59	-48.			
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9	99					
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0	99					
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3	99	-27.26	-48.			
RACH	00:00:03.48...	U	0	60	80	2		-27.49	-11.			
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10.			
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61.			
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52.			
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

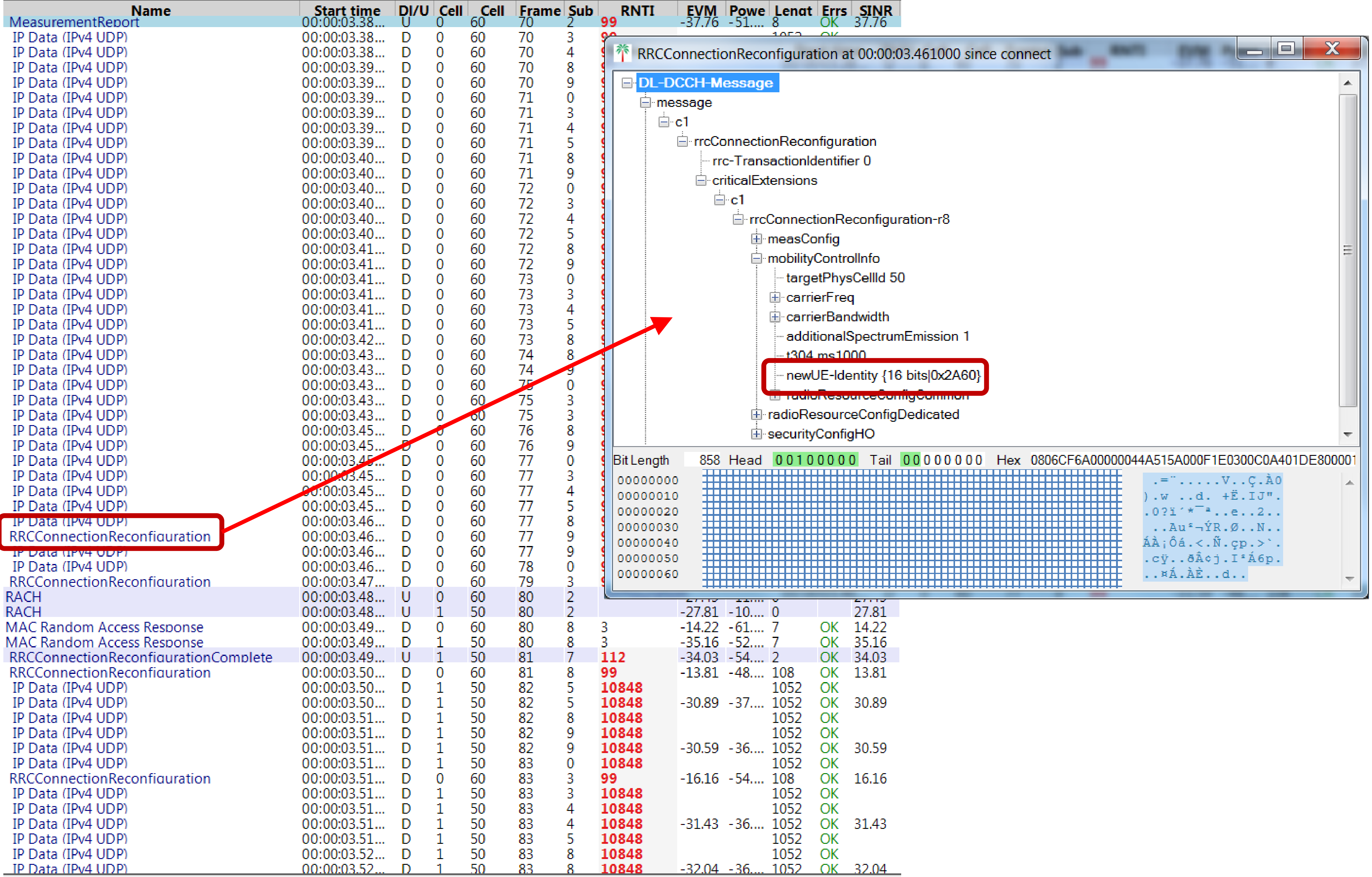


Handoff between cell 60 and cell 50

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3						
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5						
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8						
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0						
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3						
RACH	00:00:03.48...	U	0	60	80	2						
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

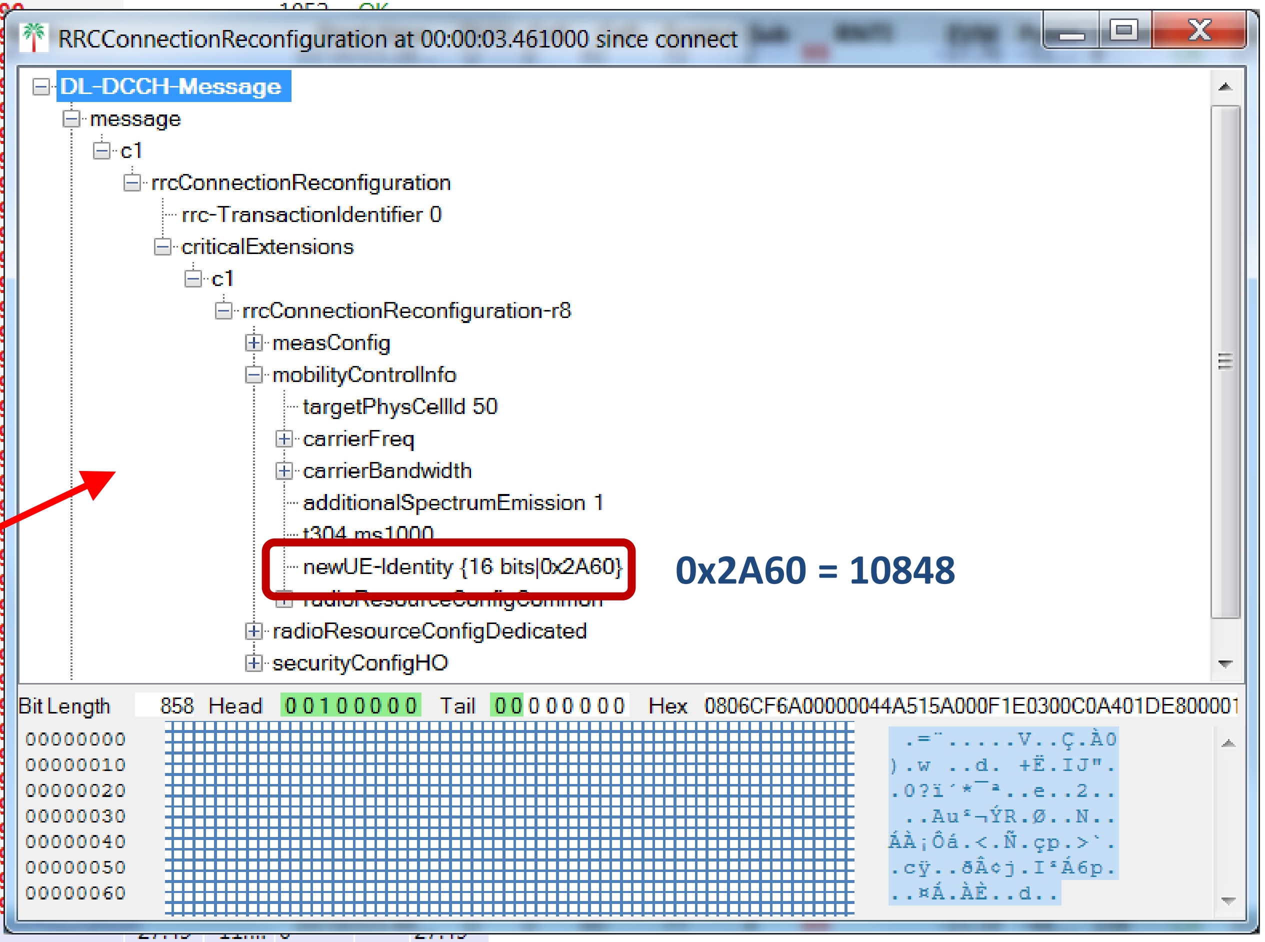




Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5						
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8						
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0						
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3						
RACH	00:00:03.48...	U	0	60	80	2						
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

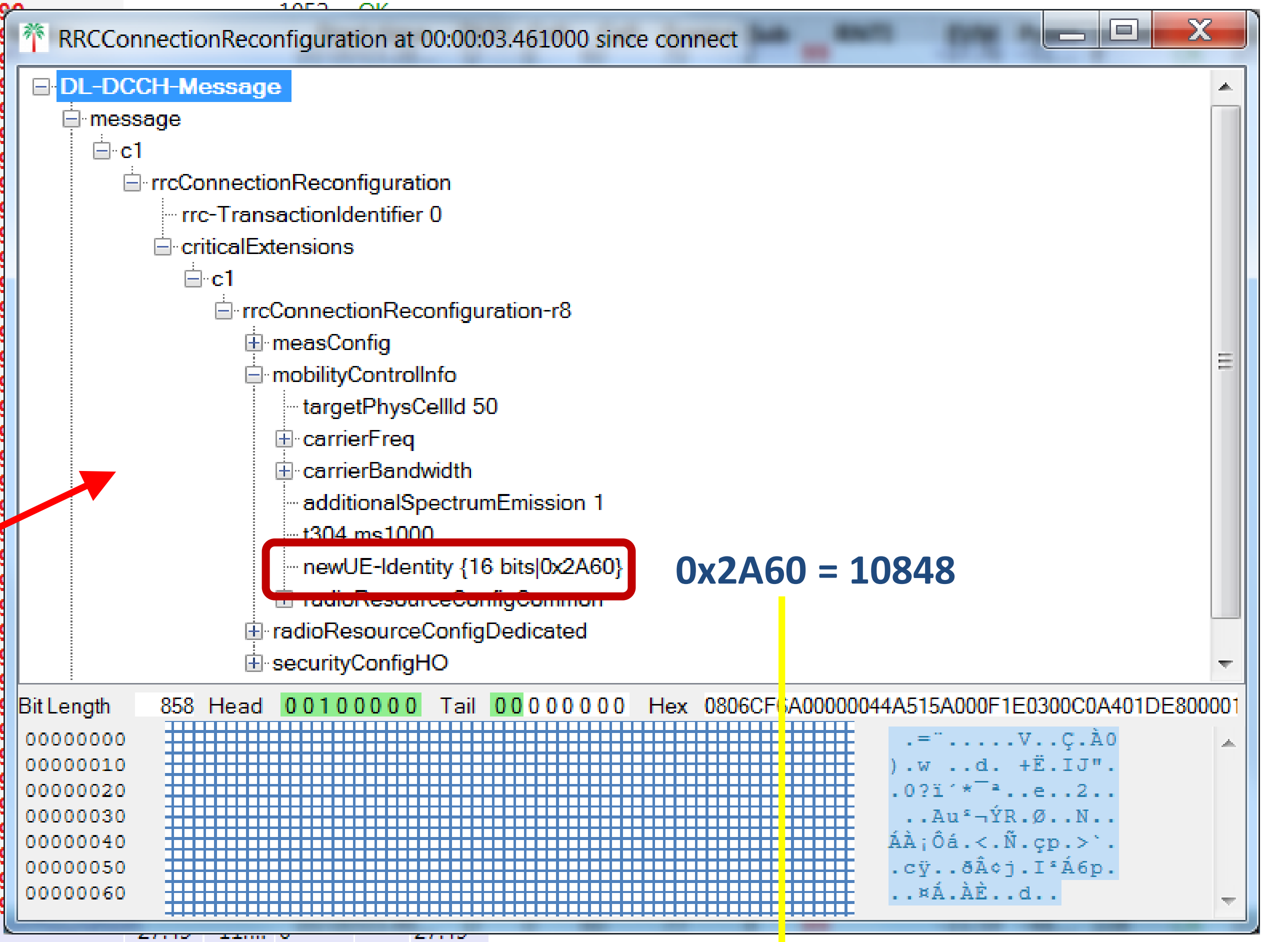
Handoff between cell 60 and cell 50



0x2A60 = 10848

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3						
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5						
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8						
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0						
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3						
RACH	00:00:03.48...	U	0	60	80	2						
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04



0x2A60 = 10848

Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77							
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78							
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79							
RACH	00:00:03.48...	U	0	60	80							
RACH	00:00:03.48...	U	1	50	80							
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.05	-34....	2	OK	34.05
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

MAC-RND-ACCS-RSP at 00:00:03.490000 since connect

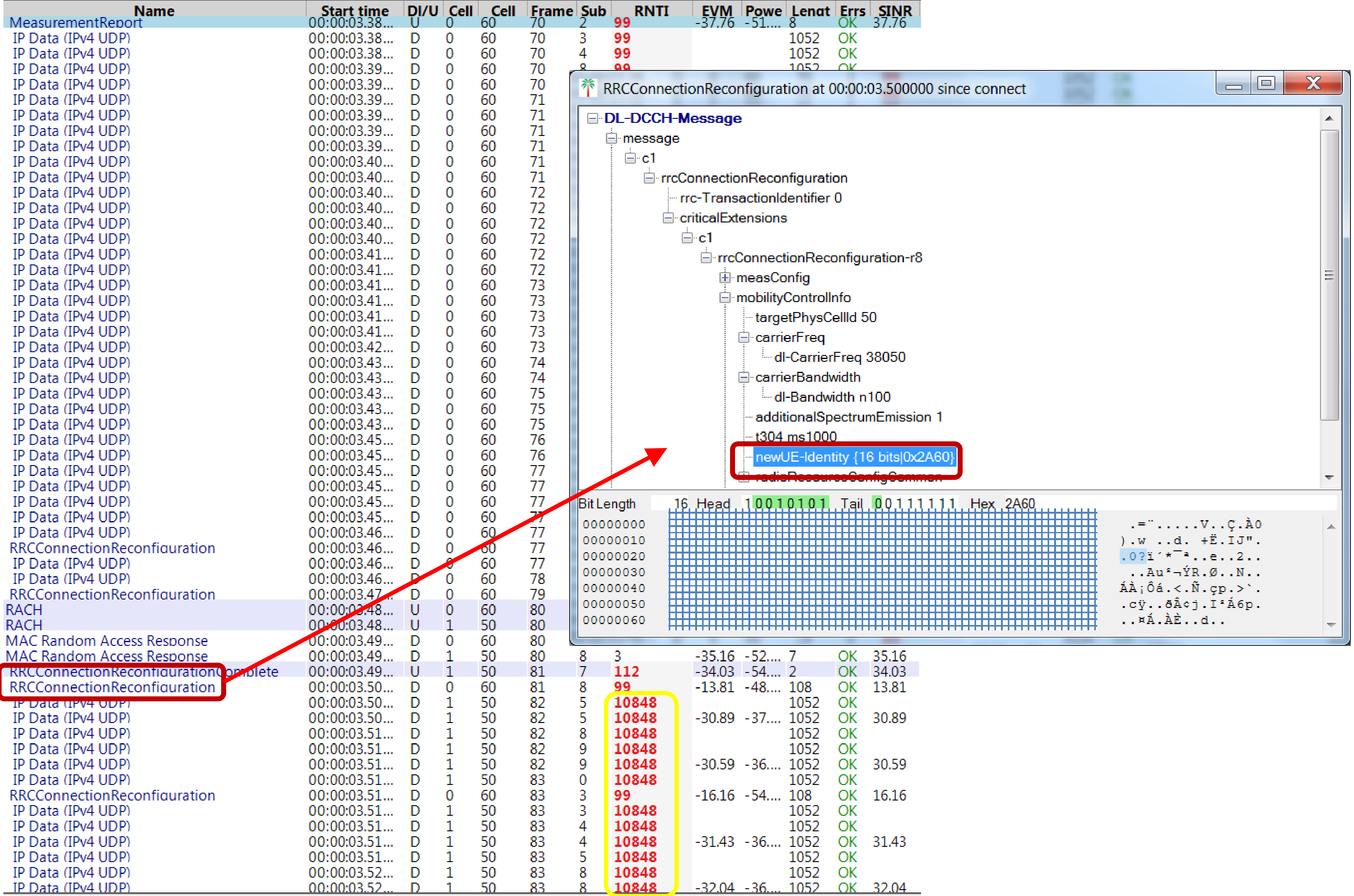
- MAC Random Access Response
  - Sub Header 0
    - E 0 => False
    - T 1
    - RAPID 45
  - MAC RAR 0 <NO DATA>
    - Reserved OK
    - Timing Advance Command 2
    - Random Access Response Grant
      - Hopping Flag 0 => False
      - Fixed size Resource Block Assignment 284
      - Truncated MCS 2 => Q'_m = 2 I_TBS = 2 rv_idx = 0
      - TPC Command for PUCCH 0 => -6 dB
      - UL Delay 0 => False
      - CQI Request 0 => False
    - T-CRNTI 112

Bit Length 16 Head 00000000 Tail 01110000 Hex 0070

00000000 6D 00 22 38 40 00 70 m."8@.p

RNTI = 112

Handoff between cell 60 and cell 50



Handoff between cell 60 and cell 50

LTE location leaks and potential target device tracking

- According to 3GPP TS 36.300, 36.331, 36.211, 36.212, 36.213, 36.321
  - C-RNTI is a unique identification used for identifying RRC Connection and scheduling which is dedicated to a particular UE.
  - After connection establishment or re-establishment the Temporary C-RNTI (as explained above) is promoted to C-RNTI.
  - During Handovers within E-UTRA or from other RAT to E-UTRA, C-RNTI is explicitly provided by the eNB in MobilityControlInfo container with IE newUE-Identity.

- No specific guidelines on how often to refresh the RNTI and how to assign it
  - In my passive analysis I have seen RNTIs unchanged for long periods of time
  - Often RNTI_new_user = RNTI_assigned_last + 1

Challenges and solutions

- Potential solutions
  - Refresh the RNTI each time the UE goes from idle to connected
  - Randomize RNTI
  - Analyze the necessity of explicitly indicating the RNTI in the handover message

- If RNTI is not refreshed rather frequently
  - MIT+Bell Labs work - LTE Radio Analytics Made Easy and Accessible (SigComm’14)
  - Track a device and map measurements to it based on RNTI (paper’s section 8.7)
  - When RNTI changes, PHY layer measurements still allow to map it to a given UE (SINR, RSSI, etc)
    - MIMO measurements and metrics

- Recent discussion with GSMA
  - The RRC Connection Reconfiguration message should be sent encrypted – This would make tracking more difficult
  - But one could monitor traffic from adjacent cells and wait to see new RNTI with similar RF/traffic signature
  - Ongoing discussions to address these potential issues

Some final thoughts…

LTE security and protocol exploits

- Mobile security research very active since ~2009
- Most cool mobile security research exclusively on GSM (until now)
  - GSM location leaks (NDSS'12)
  - Wideband GSM sniffing (Nohl and Munaut – 27C3)
  - Hijacking mobile connections (Blackhat Europe'09)
  - Carmen Sandiego project (Blackhat'10)
  - GSM RACH flooding (Spaar – DeepSec'09)
  - …
- Recent availability of open source LTE implementations
  - I expect a surge in LTE-focused security research
  - Very interesting PhD topic

- The more research in the area, the more secure networks will be

- I am actively advocating for specific protocol security focus in 5G and next-gen standards

Thanks!

Q&A

http://www.ee.columbia.edu/~roger/ ---- @rgoestotheshows

Huge THANK YOU to Sanjole for providing the captures used in this presentation.
http://www.sanjole.com/