

TUTORIAL:
**LTE AND 5G PROTOCOL SECURITY PROCEDURES AND
VULNERABILITY ANALYSES USING SOFTWARE RADIO TESTBEDS**

PART II – UPPER LAYERS

Vuk Marojevic, Roger Piqueras Jover

Vuk.marojevic@ece.msstate.edu, rpiquerasjov@bloomberg.net

October 30th 2018

ABOUT – ROGER PIQUERAS JOVER

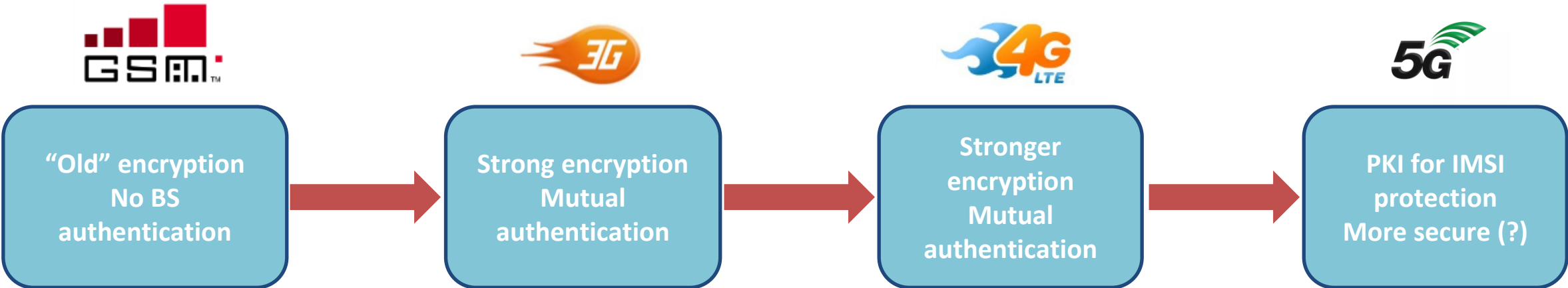
- Recent dad who goes to a lot of live music shows, plays and watches too much soccer, and does some security research on the side
- Security Researcher (aka Senior Security Architect), Office of the CTO at Bloomberg
- Formerly (5 years) Principal Member of Technical Staff at AT&T Security Research
- Mobile/wireless network security research
 - Mostly LTE PHY and upper layers
- If it communicates wirelessly, I am interested in its security
 - BLE
 - 802.11
 - Zigbee, Zigwave
 - LoRaWAN
- More details
 - <http://rogerpiquerasjover.net/>



@rgoestotheshows

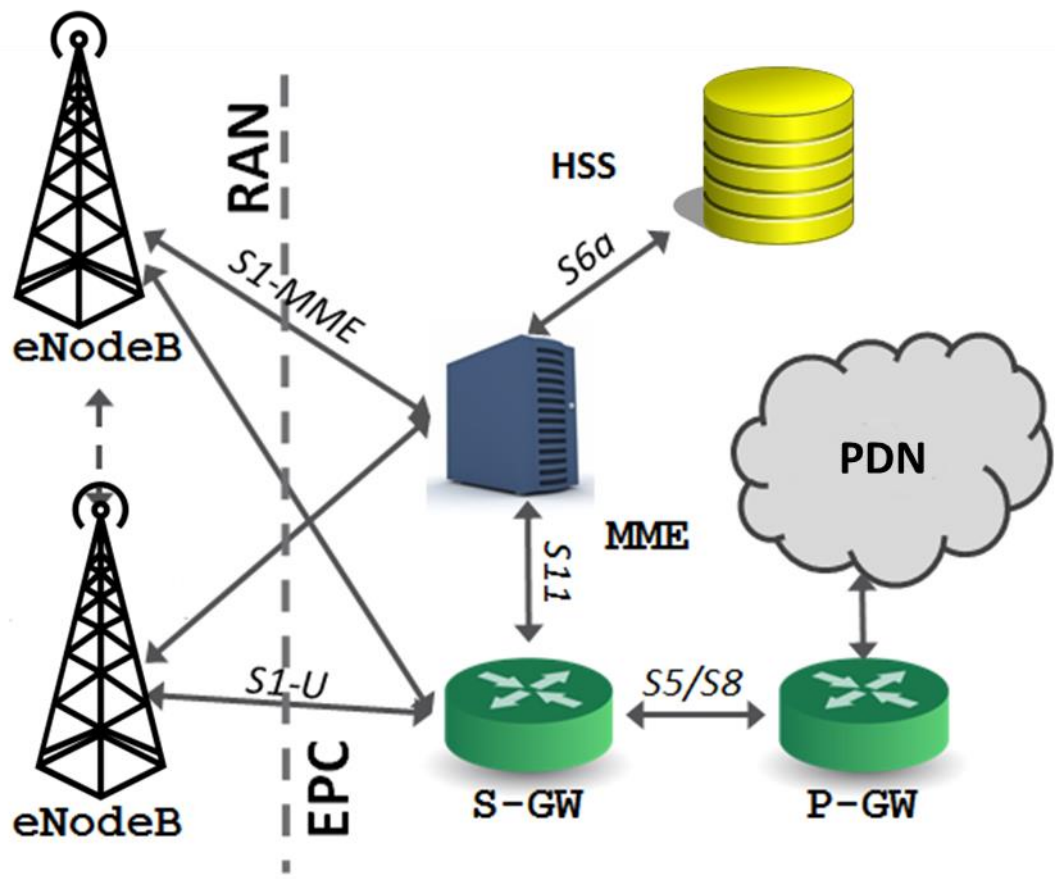
EXPLORING MOBILE NETWORK PROTOCOL SECURITY

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

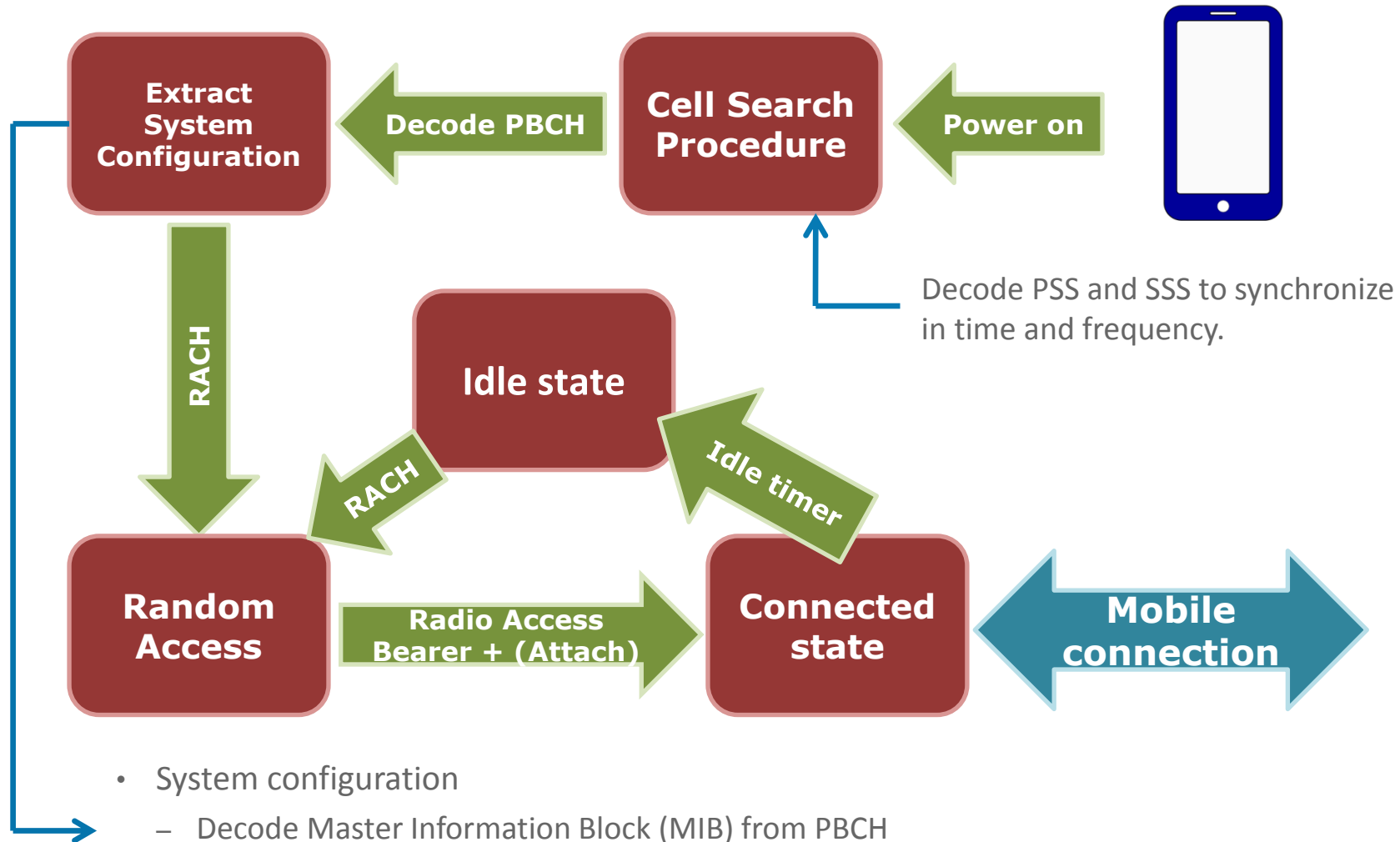


LTE BASICS

LTE MOBILE NETWORK ARCHITECTURE

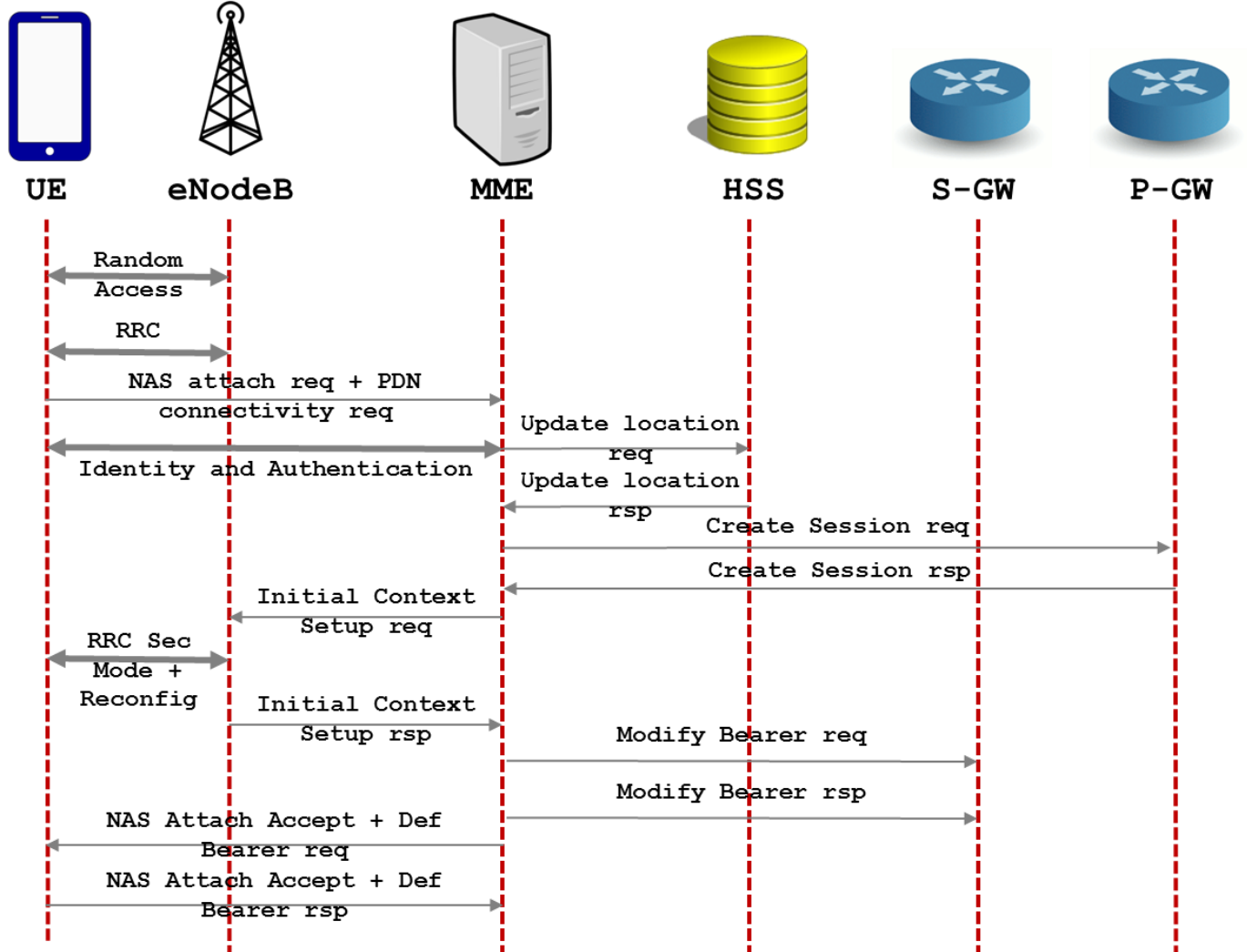


LTE CELL SELECTION AND CONNECTION

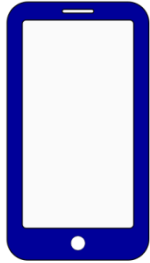


- System configuration
 - Decode Master Information Block (MIB) from PBCH
 - Decode System Information Blocks (SIBs) from PDSCH

LTE 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



XYZ-867-5309

MSISDN – Your phone number.

LTE (IN)SECURITY RATIONALE

LTE (IN)SECURITY RATIONALE

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

Count	Name	Start time	DI/UI	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:

- Base station config (broadcast messages)
- Measurement reports
- Measurement report requests
- (Sometimes) GPS coordinates
- HO related messages
- Paging messages
- Etc

LTE (IN)SECURITY RATIONALE

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.

Spoiler alert – This also potentially applies to 5G. No viable solution proposed in the specifications yet.

(more on this later)

EXPLORING LTE SECURITY WITH SOFTWARE-RADIO

TOOLSET

- LTE open source implementation (eNB+UE)
 - Modified OpenLTE - <http://openlte.sourceforge.net/>
 - Recent work with modified srsLTE – <https://github.com/srsLTE>
 - **First available UE stack implementation!!!!!!**
 - LTE sniffer
 - Modifications to source for protocol exploit experimentation
- HW setup
 - USRP B210/USRP mini for active rogue base station
 - BUDGET: USRP B210 (\$1100) + GPSDO (\$625) + LTE Antenna (2x\$30) = \$1785
 - Machine running Ubuntu

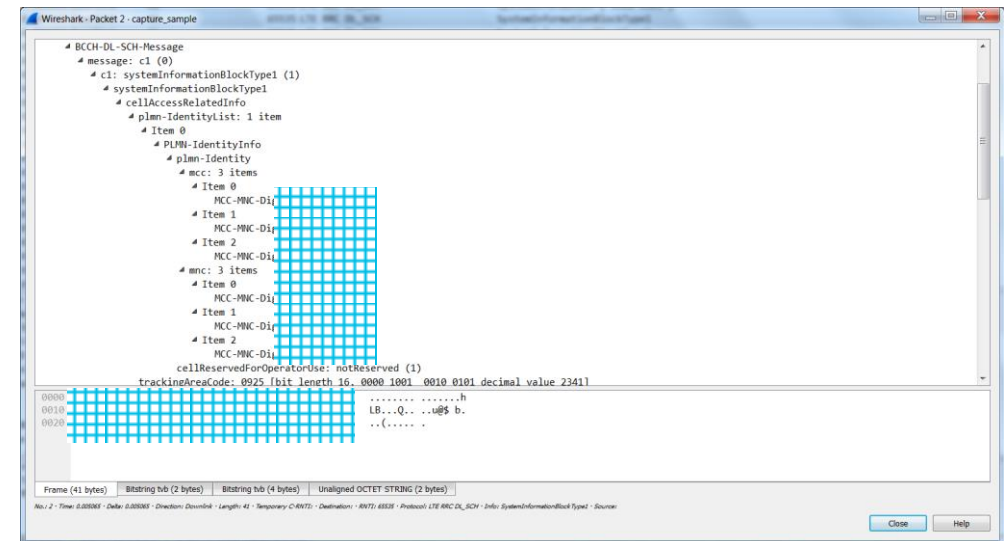


All LTE active radio experiments MUST be performed inside a faraday cage!!!

SNIFFING BASE STATION CONFIGURATION

- Base station configuration broadcasted in the clear in MIB and SIB messages.
- srsLTE + AirScope
 - Dump everything on pcap
- Very useful information that could be leveraged by and adversary
 - Optimal tx power for a rogue base station
 - High priority frequencies to force priority cell reselection
 - 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
- Broadcast message scanning tools available in both srsLTE and openLTE

LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation. Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, Jeffrey H. Reed. IEEE Communications Magazine. Special issue on Critical Communications and Public Safety Networks. April 2016.



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

```
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
```

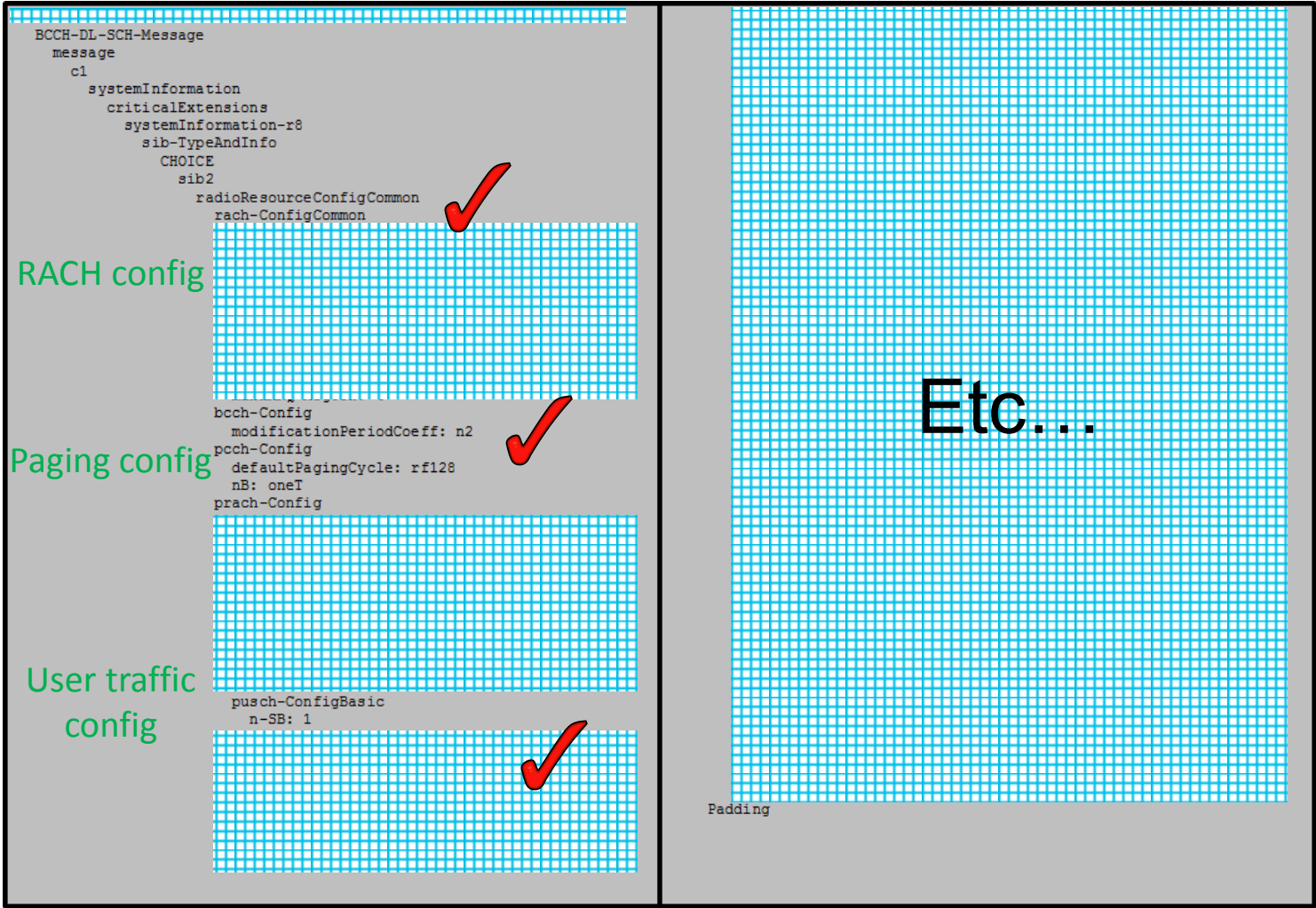
Mobile operator

Cell ID

RX power to select that cell

LTE PDSCH SIB1 packet

SNIFFING BASE STATION CONFIGURATION



LTE PDSCH SIB2/3 packet

SNIFFING BASE STATION CONFIGURATION

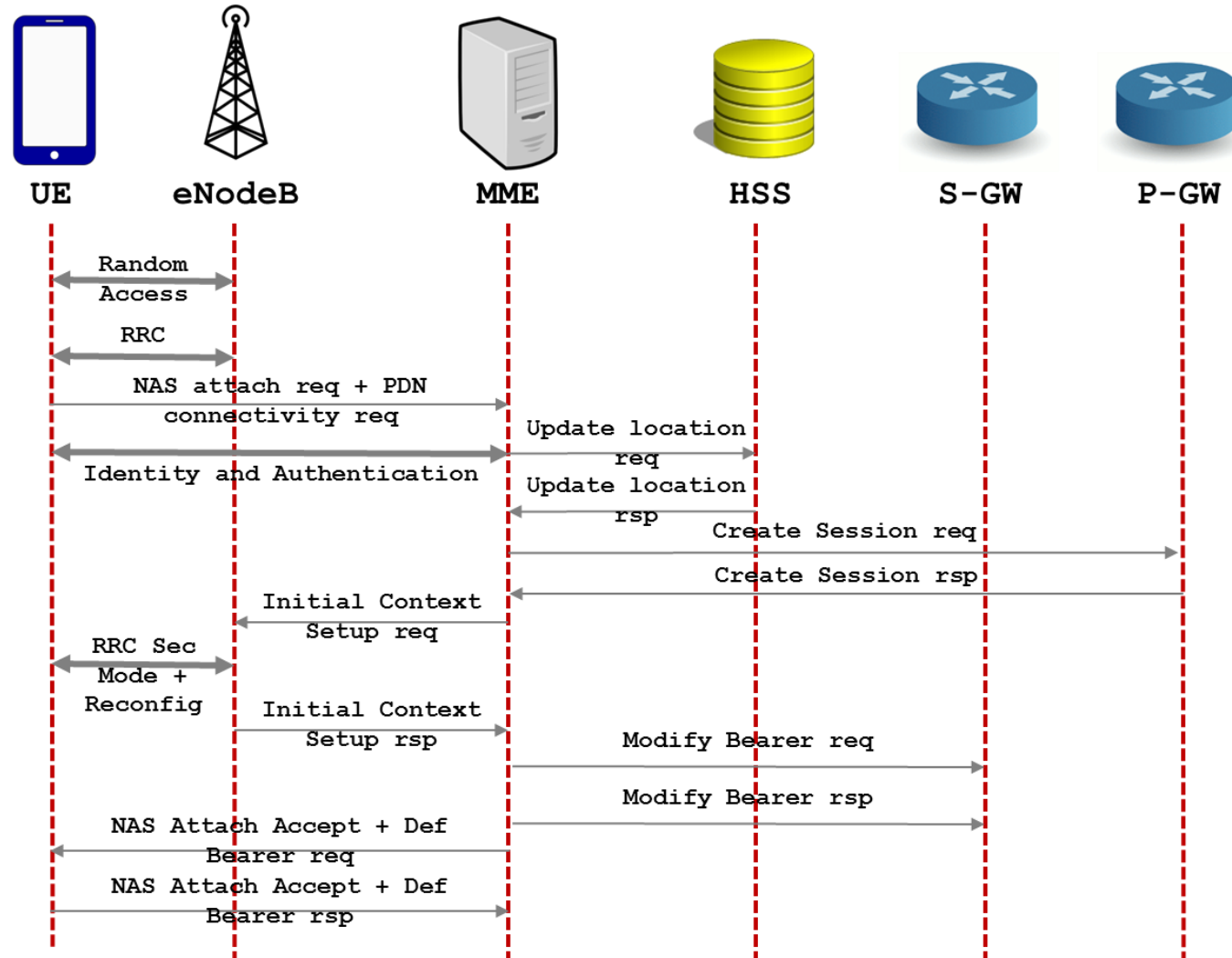
- MIB/SIB messages are necessary for the operation of the network
 - Some things must be sent in the clear (i.e. a device connecting for the first time)
 - But perhaps not everything
- Things an attacker can learn from MIB and SIB messages
 - Optimal tx power for a rogue base station (no need to set 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/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation. Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, Jeffrey H. Reed. **IEEE Communications Magazine.** Special issue on Critical Communications and Public Safety Networks. April 2016.

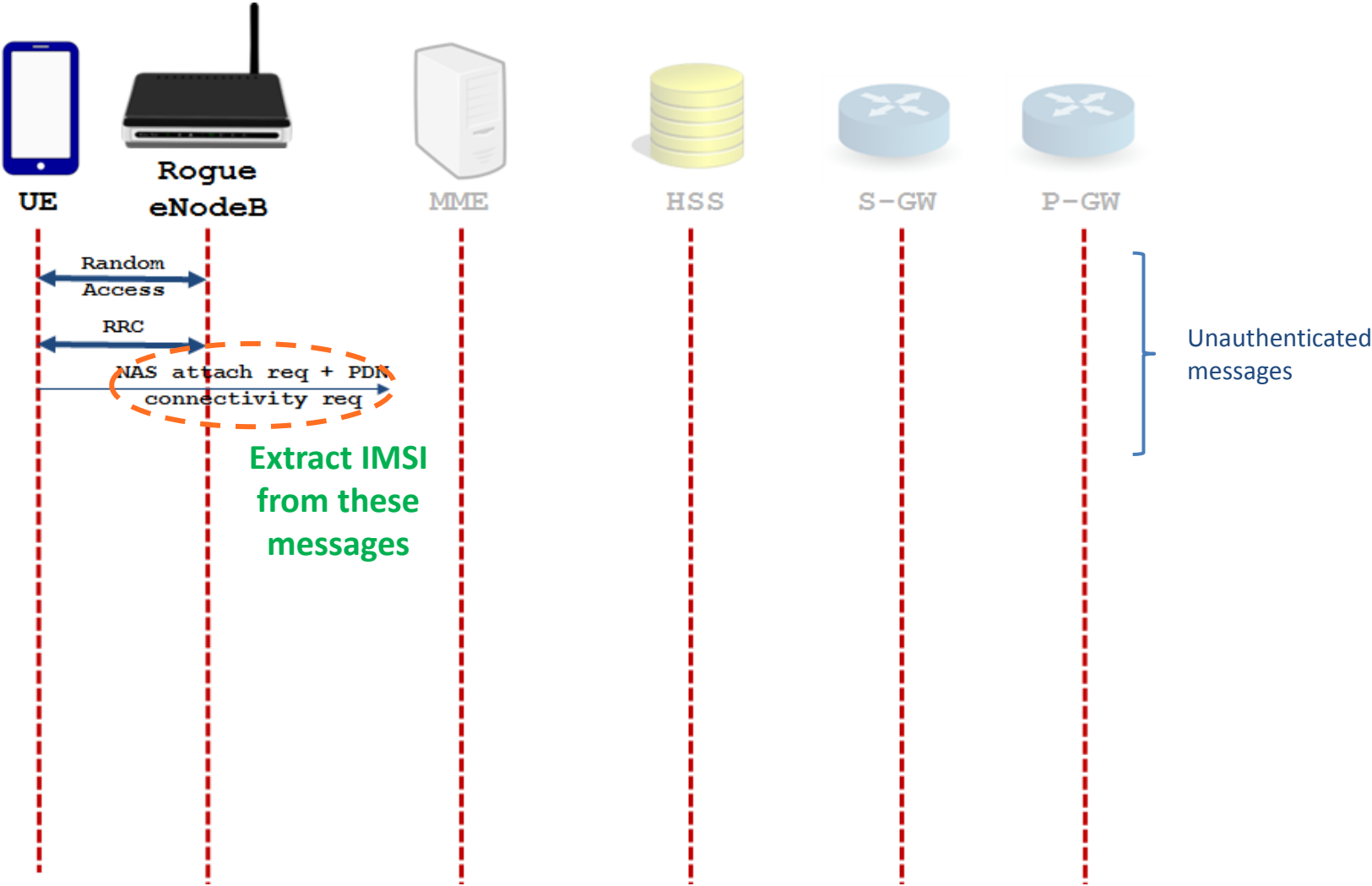
IMSI CATCHERS(STINGRAY)

- Active device that intercepts mobile devices
 - Malicious base station advertising itself as legitimate
 - Transmits the same configuration and broadcast information as real base station
 - Forces all mobile devices in its range do disclose their IMSI in the clear
 - After catching the IMSI, releases connection and mobile device reconnects to real base station
- Wrongly assumed to require downgrading to GSM
 - Jam/block 3G and LTE signals
 - Use GSM-based IMSI catcher
- Can be implemented easily using open source tools
 - openBTS (GSM)
 - srsLTE/OpenLTE (LTE)

IMSI CATCHERS(STINGRAY)



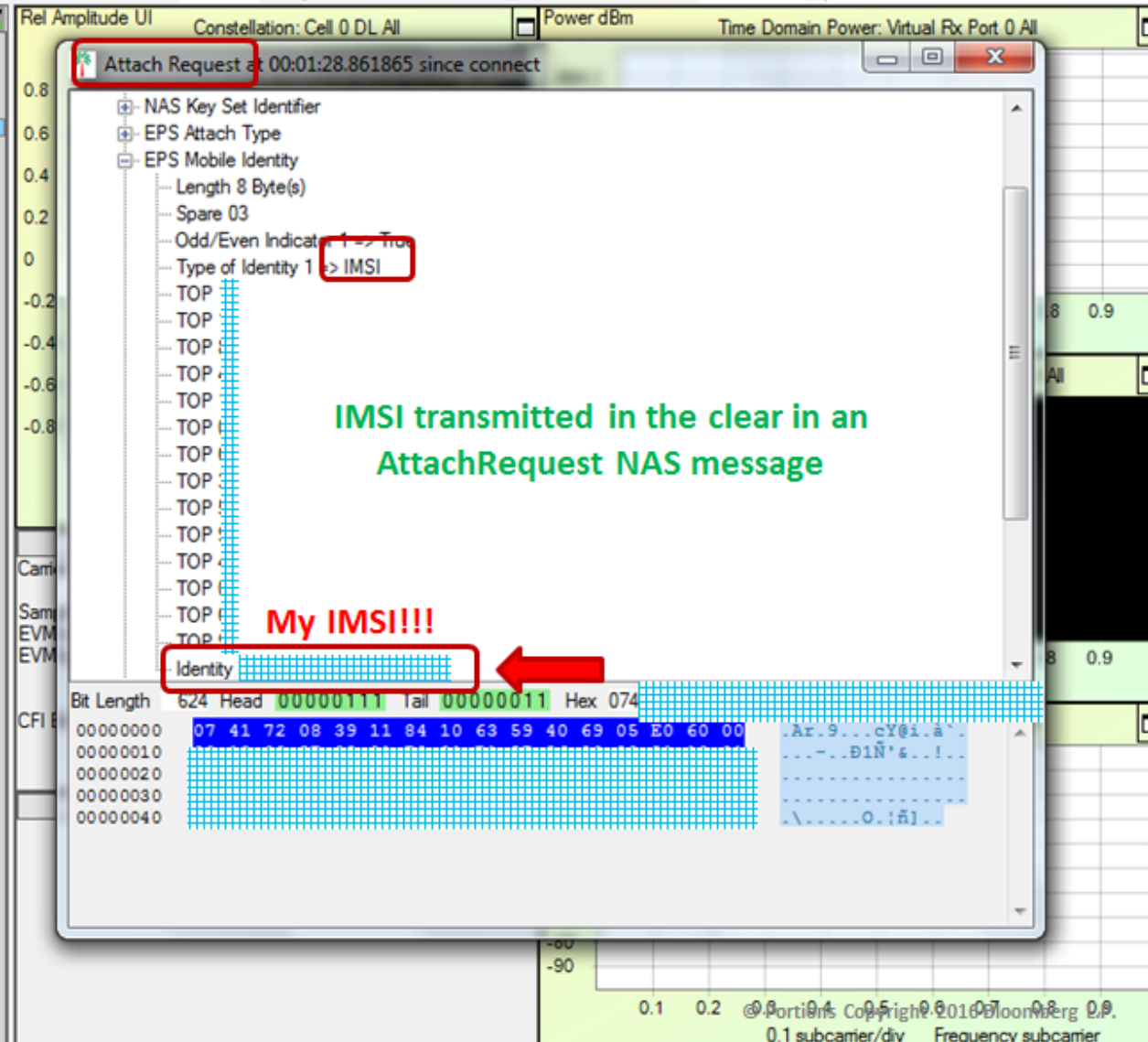
IMSI CATCHERS(STINGRAY)



LOW-COST 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
 - Not possible to implement a MitM threat (mutual authentication)

Name	Start time	DI/UI	Cell ID	Frame	RNTI	UE Identity	Length	Errs	D
Ciphered data	00:01:28.805867	U		306	19451		1428	OK	N
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: [REDACTED]		OK	
Unknown Data	00:01:28.822867	D		307	18999		52	1	
MAC Random...	00:01:28.824867	D		308	8		7	OK	
Unknown Data	00:01:28.824867	D		308	18999		800	1	
Ciphered data	00:01:28.825867	D		308	19451		1100	OK	N
Unknown Data	00:01:28.826867	D		308	18999		1107	1	
Unknown Data	00:01:28.827867	D		308	18999		52	1	
RRCConnectio...	00:01:28.833867	D		309	19575	IMSI: [REDACTED]	4	OK	
Unknown Data	00:01:28.835867	D		309	18999		1428	1	
Unknown Data	00:01:28.837867	D		309	18999		1428	1	
Unknown Data	00:01:28.837867	D		309	18999		196	1	
Unknown Data	00:01:28.839867	D		309	18999		1428	1	
RRCConnectio...	00:01:28.842867	D		309	19577		24	OK	
Unknown Data	00:01:28.843867	D		310	18999		1428	1	
Ciphered data	00:01:28.844867	D		310	19451		1428	OK	N
Unknown Data	00:01:28.846867	D		310	18999		52	1	
Unknown Data	00:01:28.846867	D		310	18999		52	1	
Unknown Data	00:01:28.846867	D		310	18999		52	1	
Unknown Data	00:01:28.846867	D		310	18999		60	1	
Ciphered data	00:01:28.848867	D		310	19451		1428	OK	N
Ciphered data	00:01:28.854867	D		311	19451		1428	OK	N
Ciphered data	00:01:28.857867	D		311	19451		1428	OK	N
RRCConnectio...	00:01:28.861865	U		311	19575	IMSI: [REDACTED]	1	OK	
Attach Request	00:01:28.861865	U		311	19575	IMSI: [REDACTED]	8	OK	
PDN Connectiv...	00:01:28.861865	U		311	19575	IMSI: [REDACTED]	5	OK	
Ciphered data	00:01:28.869867	D		312	19451		328	OK	N
Ciphered data	00:01:28.873867	D		313	19451		1428	OK	N
Unknown Data	00:01:28.880867	D		313	18999		677	1	
Ciphered data	00:01:28.880867	D		313	19451		1428	OK	N
Ciphered data	00:01:28.885867	D		314	19451		1428	OK	N
Unknown Data	00:01:28.885867	D		314	18999		271	1	
Ciphered data	00:01:28.888867	D		314	19451		1428	OK	N



LOW-COST LTE IMSI CATCHER (STINGRAY)

The image shows a Wireshark packet capture window titled "Attach Request at 00:01:28.861865 since connect". The packet list pane shows an "Attach Request" packet. The packet details pane is expanded to show the "EPS Mobile Identity" section, where "Type of Identity 1" is set to "IMSI". A red box highlights the text "Plain NAS message, not security protected" in the "Security Header Type 0" field. Another red box highlights "IMSI" in the "Type of Identity 1" field. A red arrow points to the "Identity" field in the packet bytes pane, which shows a grid of bits. The packet bytes pane also displays the hex value "074" and the hex dump "07 41 72 08 39 11 84 10 63 59 40 69 05 E0 60 00".

Security Header Type 0 => Plain NAS message, not security protected

Protocol Discriminator 7 => EPS mobility management messages

Message Identity 65 => Attach Request

NAS Key Set Identifier

... TSC 0 => Native Security Context

... NAS Key Set 7

EPS Attach Type

... Reserved OK

... EPS Attach Type Value 2 => EPS Attach

EPS Mobile Identity

... Length 8 Byte(s)

... Spare 03

... Odd/Even Indicator 1 => True

Type of Identity 1 => IMSI

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

TOP

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 .Ar.9...cY@i.à`.

00000010ðlÑ'&...!

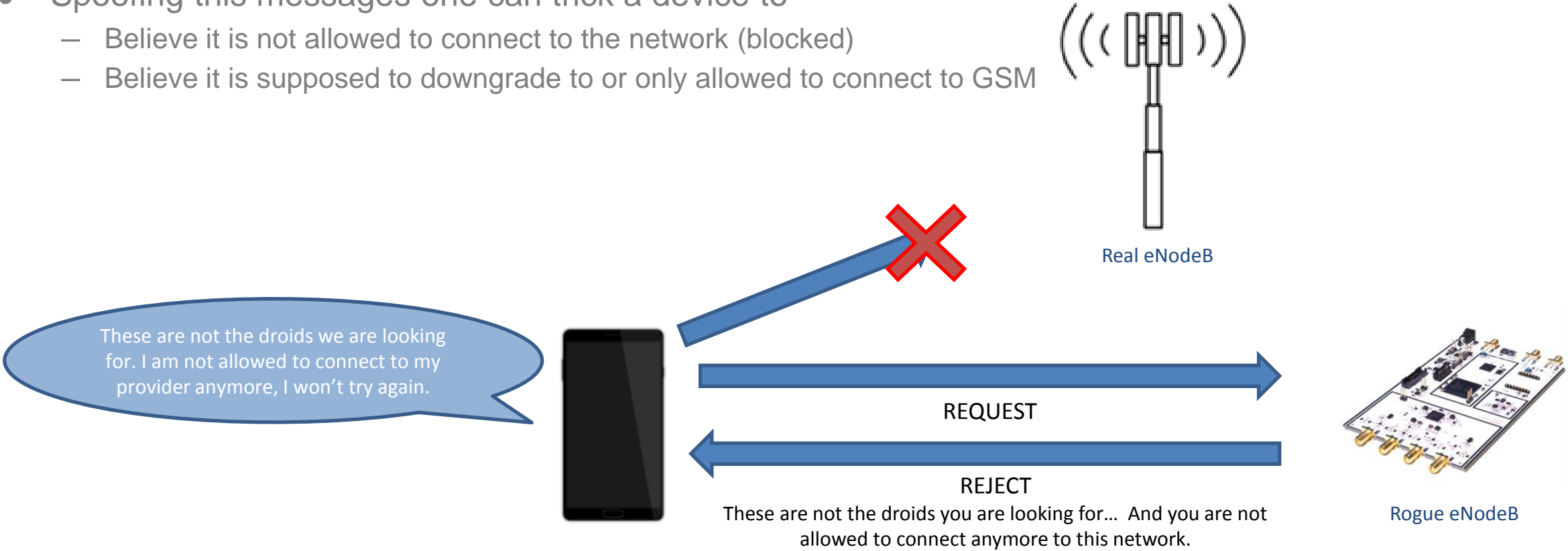
00000020

00000030

00000040 \.....O.ñl..

DEVICE AND SIM TEMPORARY LOCK

- 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

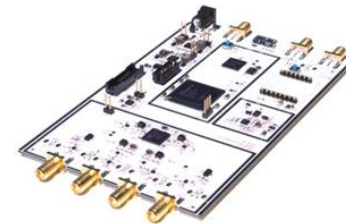
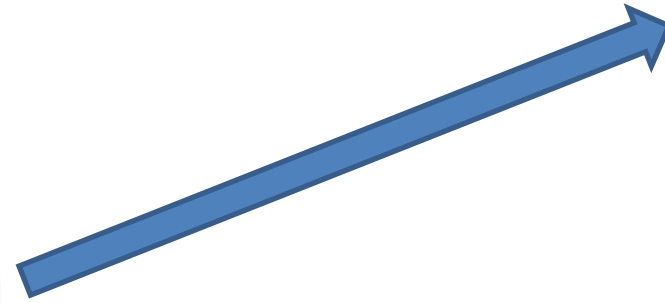


Jover, Roger Piqueras. "LTE security, protocol exploits and location tracking experimentation with low-cost software radio." *arXiv preprint arXiv:1607.05171* (2016).

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...

I will remove these restraints and leave this cell with the door open... and use only GSM from now on... and I'll drop my weapon.



(Much more dangerous) rogue GSM base station

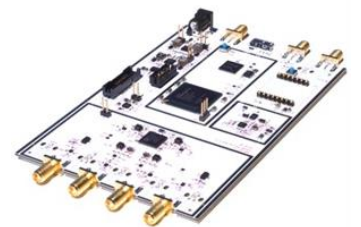


REQUEST



REJECT

You will remove these restraints and leave this cell with the door open... and use only GSM from now on.



Rogue eNodeB

DEVICE TEMPORARY LOCK AND SOFT DOWNGRADE

- 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...

CONNECTION HIJACKING IN LTE

- LTE layer 2 encryption and integrity protection
 - Packets with known structure
 - AES Counter Mode (AES-CTR)
 - 16 bit checksum in the IP-UDP DNS request packets
- Protocol exploit
 - Track user (RNTI)
 - Identify DNS requests
 - MitM DNS requests (some “radio” challenges)
 - Apply mask to flip bits on destination IP address
 - Forward DNS requests to malicious DNS server

EXPLORING UPLINK PROTOCOL SECURITY

SRSUE

- First open-source implementation of the mobile device stack
 - <https://github.com/srsLTE/srsLTE/tree/master/srsue>
 - First commit May 2017
- Platform to experiment with UL pre-authentication messages
- Now researchers can analyze exploits in the eNodeB and the mobile core network

CONNECTION DETACH HANDSHAKE

- Procedure through which the UE disconnects from the network
 - Switch off UE
 - Airplane mode
 - Remove SIM
- Can be UE initiated and does not require ACK from network (!!!)
- Authentication/integrity protection (???)

CONNECTION DETACH HANDSHAKE

- NAS detach request message
 - Includes EPS mobile identity
 - Can be GUTI or IMSI
 - It can even be the IMEI
- In some cases it does not require integrity protection
 - It can be spoofed!

3GPP TS 24.301 V13.7.0 (2016-09)

5.5.2.2.1 - UE initiated detach procedure initiation

Page 122

NAS Detach Request can be sent with TMSI and even just the IMEI

3GPP TS 24.301
V13.7.0 (2016-09)

4.4.4.3 - Integrity checking of
NAS signalling messages in
the MME

Page 47

**NAS Detach Request NOT
integrity protected**

THERE'S MORE...

3GPP TS 24.301 V13.7.0 (2016-09)

4.4.4.3 - Integrity checking of NAS signalling messages in the MME

Between page 47 and 48

Even NAS security context is active, MME will process a NAS Detach Request with a MAC that fails integrity check or cannot be verified

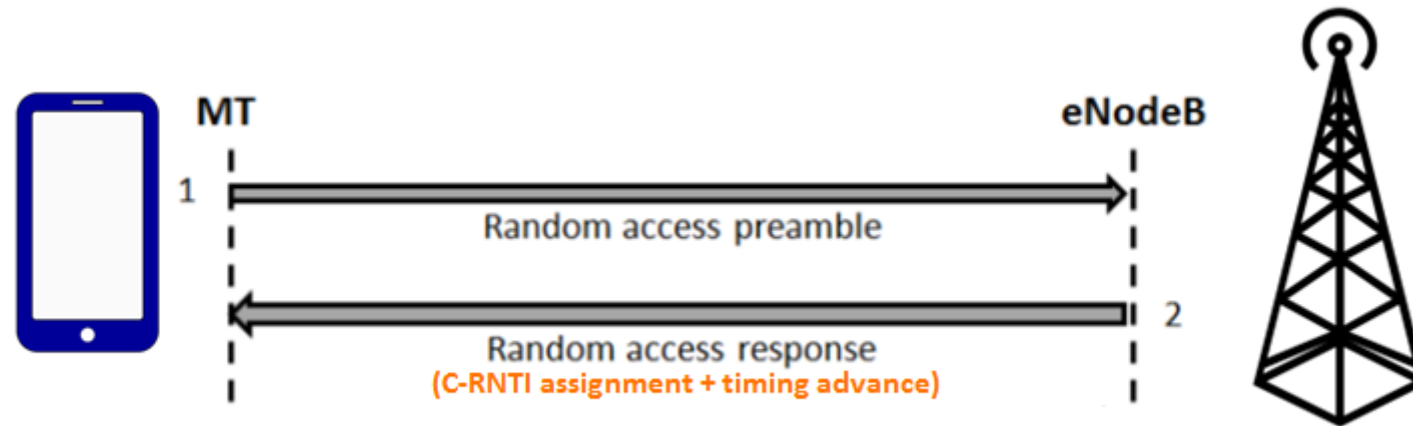
REMOTE DEVICE DETACH

- Set up
 - Test smartphone (victim)
 - Linux box #1
 - USRP B210 running srsUE (adversary)
 - Linux box #2
 - USRP B210 running srsENB
 - Open source LTE EPC
- Run RRC handshake and spoof Detach Request message with victim's identity
- Knock out victim from network remotely
 - Though in the lab it is not "remotely"
- Testing it in a real network would be easy
 - But not legal
 - Next tests → commercial picocell
- **Might not work in a real network if inter-layer integrity checks are well implemented**

LTE LOCATION LEAKS

LOCATION LEAKS AND DEVICE TRACKING - RNTI

- 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



LOCATION LEAKS AND DEVICE TRACKING - RNTI

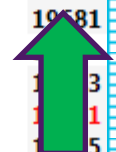
MAC-RND-ACCS-RSP at 00:04:42.946818 since connect

- MAC Random Access Response
 - Sub Header 0
 - E 0 => False
 - T 1
 - RAPID 63
 - MAC RAR 0 <NO DATA>
 - Reserved OK
 - Timing Advance Command 0
 - Random Access Response Grant
 - Hopping Flag 0 => False
 - Fixed size Resource Block Assignment 96
 - Truncated MCS 2 => Q'_m = 2 L_TBS = 2 rv_idx = 0
 - TPC Command for PUCCH 3 => 0 dB
 - UL Delay 0 => False
 - CQI Request 0 => False
 - T-CRNTI 220**

Bit Length 56 Head 01111111 Tail 11011100 Hex 7F0000C04C00DC
00000000 7F 00 00 C0 4C 00 DC ...ÀL.Ü

LOCATION LEAKS AND DEVICE TRACKING - RNTI

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	19681		404	OK
MAC Random Access Response	00:02:26.984868	D		1004			7	OK
RRCConnectionSetup	00:02:27.003868	D		1006			24	OK
Unknown Data	00:02:27.020868	D		1007			1428	1
Ciphered RRC	00:02:27.021868	D		1007			0	OK



RNTI TRACKING WITH OPEN-SOURCE TOOLS

RNTIs being tracked
within this cell
(srsLTE)

```
roger@ny731-6w-080messi: ~/SRC/LTE_new_scanner
0x 27: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.7 kb, mcs=21.0, prb= 4.0 - timeout=0s 116 ms
0x1ea9: dl: 2.7 kb, mcs= 2.6, prb=12.4 - ul: 0.6 kb, mcs= 3.8, prb= 3.8 - timeout=0s 90 ms
0xaf73: dl: 0.9 kb, mcs=17.0, prb=10.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=1s 621 ms
0x122c: dl: 2.7 kb, mcs= 4.7, prb= 4.7 - ul: 3.0 kb, mcs= 6.2, prb= 3.6 - timeout=0s 8 ms
0x1513: dl: 1.6 kb, mcs=11.0, prb= 9.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 405 ms
0x214b: dl: 0.1 kb, mcs= 7.0, prb= 3.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=1s 509 ms
0x 2fe: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=1s 451 ms
0x1f7d: dl: 0.3 kb, mcs= 2.2, prb= 3.0 - ul: 0.6 kb, mcs= 9.5, prb= 2.9 - timeout=0s 5 ms
0x1fd3: dl: 0.2 kb, mcs= 7.0, prb= 3.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=1s 401 ms
0x 1f: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.7 kb, mcs=21.0, prb= 4.0 - timeout=0s 921 ms
0x 10: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.7 kb, mcs=21.0, prb= 4.0 - timeout=0s 88 ms
0x211d: dl: 2.3 kb, mcs= 5.9, prb=13.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 305 ms
0x3dfc: dl: 0.6 kb, mcs= 7.0, prb=20.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=1s 84 ms
0x 41e: dl: 80.0 kb, mcs=16.2, prb=19.6 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 529 ms
0x523a: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.2 kb, mcs=20.0, prb= 3.0 - timeout=1s 40 ms
0xe386: dl: 0.7 kb, mcs= 2.0, prb=37.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 585 ms
0x6023: dl: 0.8 kb, mcs= 8.0, prb=10.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 365 ms
0xc4d5: dl: 0.4 kb, mcs= 6.5, prb=14.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 861 ms
0x826f: dl: 2.0 kb, mcs= 9.5, prb=26.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 61 ms
0xc42b: dl: 0.5 kb, mcs= 7.0, prb= 4.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 5 ms
0x1f5b: dl: 1.5 kb, mcs= 6.0, prb=30.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 21 ms
0x 2b: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.1 kb, mcs=21.0, prb= 1.0 - timeout=0s 633 ms
0x5efa: dl: 0.2 kb, mcs= 5.5, prb= 4.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 311 ms
0xa8ce: dl: 0.8 kb, mcs=15.5, prb=15.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 360 ms
0xbd37: dl: 0.1 kb, mcs= 2.0, prb=13.0 - ul: 1.3 kb, mcs=24.0, prb=20.0 - timeout=0s 337 ms
0x17ee: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 543 ms
0x 322: dl: 4.3 kb, mcs= 9.5, prb=32.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 45 ms
0x1770: dl: 4.0 kb, mcs= 2.2, prb= 9.3 - ul: 3.8 kb, mcs=13.7, prb= 3.5 - timeout=0s 106 ms
0xb439: dl: 0.6 kb, mcs=11.5, prb= 9.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 521 ms
0xfb15: dl: 0.3 kb, mcs= 4.5, prb= 7.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 346 ms
0x15ff: dl: 0.3 kb, mcs= 2.0, prb= 6.0 - ul: 1.1 kb, mcs= 9.0, prb= 5.4 - timeout=0s 49 ms
0x1bb0: dl: 0.8 kb, mcs= 3.3, prb= 6.3 - ul: 0.8 kb, mcs=10.3, prb= 3.4 - timeout=0s 109 ms
0x b0: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 1.7 kb, mcs=21.0, prb= 4.0 - timeout=0s 146 ms
0x1ca6: dl: 0.6 kb, mcs= 3.6, prb= 6.0 - ul: 0.5 kb, mcs=10.5, prb= 3.4 - timeout=0s 149 ms
0x 28: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.2 kb, mcs=20.0, prb= 4.0 - timeout=0s 394 ms
0x1bb7: dl: 1.0 kb, mcs= 2.3, prb= 6.4 - ul: 0.7 kb, mcs= 3.9, prb= 3.9 - timeout=0s 48 ms
0x93fa: dl: 0.0 kb, mcs= 0.5, prb= 4.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 232 ms
0x257d: dl: 0.6 kb, mcs=13.0, prb= 8.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 205 ms
0x8a56: dl: 0.3 kb, mcs= 9.5, prb= 6.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 202 ms
0x115a: dl: 0.8 kb, mcs= 2.0, prb= 7.4 - ul: 0.7 kb, mcs= 8.8, prb= 3.3 - timeout=-1s 998 ms
0x 36: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.2 kb, mcs=21.0, prb= 4.0 - timeout=0s 145 ms
0x 3b: dl: 0.0 kb, mcs= 0.0, prb= 0.0 - ul: 0.2 kb, mcs=21.0, prb= 4.0 - timeout=0s 140 ms
0xc8c6: dl: 0.2 kb, mcs= 3.0, prb=16.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 71 ms
0xecac: dl: 0.0 kb, mcs=15.5, prb=19.0 - ul: 0.0 kb, mcs= 0.0, prb= 0.0 - timeout=0s 0 ms
```


Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lenat	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	
RRCConnectionReconfiauration	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	
RRCConnectionReconfiauration	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
RRCConnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiauration	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	
RRCConnectionReconfiauration	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	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lenat	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	
RRCConnectionReconfiauration	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					
RRCConnectionReconfiauration	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			
RRCConnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiauration	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	
RRCConnectionReconfiauration	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

MeasurementReport at 00:00:03.383980 since connect

```
UL-DCCH-Message
├── message
│   └── c1
│       ├── measurementReport
│       │   ├── criticalExtensions
│       │   │   └── c1
│       │   │       ├── measurementReport-r8
│       │   │       │   ├── measResults
│       │   │       │   │   └── measId 1
│       │   │       │   │       ├── measResultServCell
│       │   │       │   │       │   ├── rsrpResult 56
│       │   │       │   │       │   └── rsrqResult 15
│       │   │       │   │       └── measResultNeighCells
│       │   │       │   │           └── measResultListEUTRA
│       │   │       │   │               └── MeasResultEUTRA
│       │   │       │   │                   └── physCellId 50
│       │   │       │   │                       └── measResult
│       │   │       │   │                           ├── rsrpResult 63
│       │   │       │   │                           └── rsrqResult 28
│       │   └── measResults
│       │       └── measId 1
│       │           ├── measResultServCell
│       │           │   ├── rsrpResult 56
│       │           │   └── rsrqResult 15
│       │           └── measResultNeighCells
│       │               └── measResultListEUTRA
│       │                   └── MeasResultEUTRA
│       │                       └── physCellId 50
│       │                           └── measResult
│       │                               ├── rsrpResult 63
│       │                               └── rsrqResult 28
│       └── measResults
│           └── measId 1
│               ├── measResultServCell
│               │   ├── rsrpResult 56
│               │   └── rsrqResult 15
│               └── measResultNeighCells
│                   └── measResultListEUTRA
│                       └── MeasResultEUTRA
│                           └── physCellId 50
│                               └── measResult
│                                   ├── rsrpResult 63
│                                   └── rsrqResult 28
```

Bit Length 62 Head 00001000 Tail 01110000 Hex 02040E0F00326FDC
00000000 08 10 38 3C 00 C9 BF 70

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Frame	Sub	RNTI	EVM	Power	Lenat	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)	00:00:03.45...	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					
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					
RRCConnectionReconfiauration	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					
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-27.81	-10....	0	27.81
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-14.22	-61....	7	OK 14.22
RRCConnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112	-35.16	-52....	7	OK 35.16
RRCConnectionReconfiauration	00:00:03.50...	D	0	60	81	8	99	-34.03	-54....	2	OK 34.03
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-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)	00:00:03.51...	D	1	50	82	8	10848	-30.89	-37....	1052	OK 30.89
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
RRCConnectionReconfiauration	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

RRCConnectionReconfiguration at 00:00:03.461000 since connect

DL-DCCH-Message

- message
 - c1
 - rrcConnectionReconfiguration
 - rrc-TransactionIdentifier 0
 - criticalExtensions
 - c1
 - rrcConnectionReconfiguration-r8
 - measConfig
 - mobilityControllInfo
 - targetPhysCellId 50
 - carrierFreq
 - carrierBandwidth
 - additionalSpectrumEmission 1
 - t304 ms1000
 - newUE-Identity {16 bits|0x2A60}
 - radioResourceConfigCommon
 - radioResourceConfigDedicated
 - securityConfigHO

Bit Length 858 Head 00100000 Tail 00000000 Hex 0806CF6A00000044A515A000F1E0300C0A401DE800001

```
00000000
00000010
00000020
00000030
00000040
00000050
00000060
```

..=".....V..Ç.À0
)..w..d..+È.IJ".
.0?i'*.~^..e..2..
..Au~YR.Ø..N..
ÀÀ;Ôá.<.Ñ.çp.>..
.cÿ..ðÀçj.I*À6p..
..#Á.ÀÈ..d..

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Frame	Sub	RNTI	EVM	Power	Lenat	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)	00:00:03.45...	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					
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					
RRCCOnnectionReconfiauration	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					
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-27.81	-10....	0	27.81
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-14.22	-61....	7	OK 14.22
RRCCOnnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112	-35.16	-52....	7	OK 35.16
RRCCOnnectionReconfiauration	00:00:03.50...	D	0	60	81	8	99	-34.03	-54....	2	OK 34.03
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-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)	00:00:03.51...	D	1	50	82	8	10848	-30.89	-37....	1052	OK 30.89
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
RRCCOnnectionReconfiauration	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

RRCCOnnectionReconfiauration at 00:00:03.461000 since connect

DL-DCCH-Message

- message
 - c1
 - rrcConnectionReconfiguration
 - rrc-TransactionIdentifier 0
 - criticalExtensions
 - c1
 - rrcConnectionReconfiguration-r8
 - measConfig
 - mobilityControllInfo
 - targetPhysCellId 50
 - carrierFreq
 - carrierBandwidth
 - additionalSpectrumEmission 1
 - t304.ms1000
 - newUE-Identity {16 bits|0x2A60}**
 - radioResourceConfigCommon
 - radioResourceConfigDedicated
 - securityConfigHO

Bit Length 858 Head 00100000 Tail 00000000 Hex 0806CF6A00000044A515A000F1E0300C0A401DE800001

```
00000000
00000010
00000020
00000030
00000040
00000050
00000060
```

..=".....V..Ç.À0
)..w..d..+È.IJ".
.0?i'*.~^..e..2..
..Au~YR.Ø..N..
ÀÀ;Ôá.<.Ñ.çp.>..
.cÿ..ðÀçj.I*À6p..
..#Á.ÀÈ..d..

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Frame	Sub	RNTI	EVM	Power	Lenat	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)	00:00:03.45...	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					
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					
RRCConnectionReconfiauration	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					
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-27.81	-10....	0	27.81
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-14.22	-61....	7	OK 14.22
RRCConnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112	-35.16	-52....	7	OK 35.16
RRCConnectionReconfiauration	00:00:03.50...	D	0	60	81	8	99	-34.03	-54....	2	OK 34.03
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-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)	00:00:03.51...	D	1	50	82	8	10848	-30.89	-37....	1052	OK 30.89
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
RRCConnectionReconfiauration	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

RRCConnectionReconfiguration at 00:00:03.461000 since connect

DL-DCCH-Message

- message
 - c1
 - rrcConnectionReconfiguration
 - rrc-TransactionIdentifier 0
 - criticalExtensions
 - c1
 - rrcConnectionReconfiguration-r8
 - measConfig
 - mobilityControllInfo
 - targetPhysCellId 50
 - carrierFreq
 - carrierBandwidth
 - additionalSpectrumEmission 1
 - t304.ms1000
 - newUE-Identity {16 bits|0x2A60}** **0x2A60 = 10848**
 - radioResourceConfigCommon
 - radioResourceConfigDedicated
 - securityConfigHO

Bit Length 858 Head 00100000 Tail 00000000 Hex 0806CF6A00000044A515A000F1E0300C0A401DE800001

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Frame	Sub	RNTI	EVM	Power	Lenat	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	-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)	00:00:03.45...	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					
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					
RRCConnectionReconfiauration	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					
MAC Random Access Response	00:00:03.49...	D	0	60	80	8					
MAC Random Access Response	00:00:03.49...	D	1	50	80	8					
RRCConnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112				
RRCConnectionReconfiauration	00:00:03.50...	D	0	60	81	8	99				
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848				
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848				
RRCConnectionReconfiauration	00:00:03.51...	D	0	60	83	3	99				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848				
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848				
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848				
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848				

RRCConnectionReconfiguration at 00:00:03.461000 since connect

DL-DCCH-Message

- message
 - c1
 - rrcConnectionReconfiguration
 - rrc-TransactionIdentifier 0
 - criticalExtensions
 - c1
 - rrcConnectionReconfiguration-r8
 - measConfig
 - mobilityControllInfo
 - targetPhysCellId 50
 - carrierFreq
 - carrierBandwidth
 - additionalSpectrumEmission 1
 - t304.ms1000
 - newUE-Identity {16 bits|0x2A60}**
 - radioResourceConfigCommon
 - radioResourceConfigDedicated
 - securityConfigHO

Bit Length 858 Head 00100000 Tail 00000000 Hex 0806CF0A00000044A515A000F1E0300C0A401DE800001

Hex dump: 00000000, 00000010, 00000020, 00000030, 00000040, 00000050, 00000060

ASCII dump: .=V..Ç.À0,).w ..d. +È.IJ", .0?i' *~^..e..2.., ..Au=-ÝR.Ø..N., ÅÅ;Ôá.<.Ñ.çp.>., .cÿ..ðÅçj.I*Å6p., ..#Á.ÀÈ..d..

0x2A60 = 10848

10848
10848
10848
10848
10848
10848
10848
10848
10848
10848
10848
10848

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Frame	Sub	RNTI	EVM	Power	Lenat	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)	00:00:03.40...	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)	00:00:03.42...	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)	00:00:03.45...	D	0	60	77						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77						
RRCConnectionReconfiauration	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						
RRCConnectionReconfiauration	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
RRCConnectionReconfiaurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.05	-54....	2	OK 34.05
RRCConnectionReconfiauration	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
RRCConnectionReconfiauration	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

RNTI = 112

Handoff between cell 60 and cell 50

Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lenat	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							
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)	00:00:03.39...	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)	00:00:03.45...	D	0	60	77							
RRCConnectionReconfiauration	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							
RRCConnectionReconfiauration	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							
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfiauration complete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiauration	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	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiauration	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

RRCConnectionReconfiguration at 00:00:03.500000 since connect

DL-DCCH-Message

- message
 - c1
 - rrcConnectionReconfiguration
 - rrc-TransactionIdentifier 0
 - criticalExtensions
 - c1
 - rrcConnectionReconfiguration-r8
 - measConfig
 - mobilityControllInfo
 - targetPhysCellId 50
 - carrierFreq
 - dl-CarrierFreq 38050
 - carrierBandwidth
 - dl-Bandwidth n100
 - additionalSpectrumEmission 1
 - t304 ms1000
 - newUE-Identity {16 bits|0x2A60}
 - radioResourceConfigCommon

Bit Length 16 Head 10010101 Tail 00111111 Hex 2A60

00000000
00000010
00000020
00000030
00000040
00000050
00000060

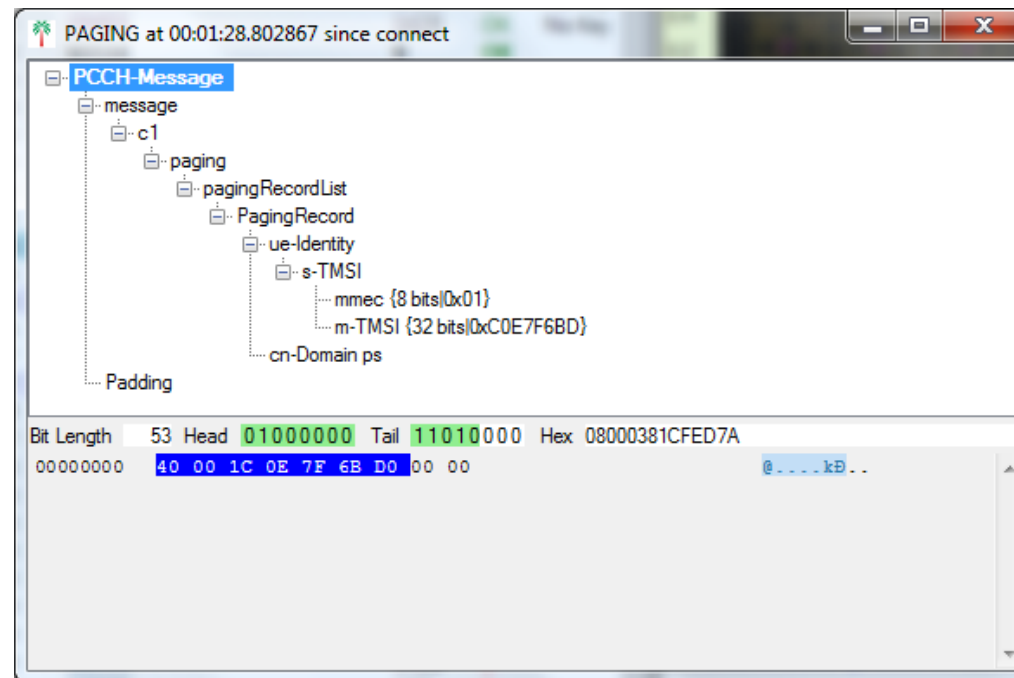
.=".....V..Ç.À0
) .w . .d. +Ë.IJ".
.0?i' *~a...e..2..
..Au*-ÝR.Ø..N..
ÁÀ;Ôá.<.Ñ.çp.>`.
.çý..8Ãçj.I*Ã6p.
..#Á.ÀË..d..

RNTI LOCATION LEAKS AND DEVICE TRACKING

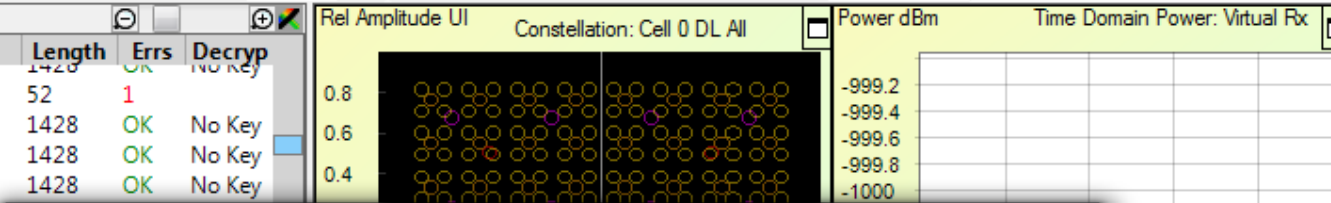
- Unprotected RRC Connection Reconfiguration message for handover should **not** occur
 - eNBs that used to have this issue have since been configured correctly
- According to 3GPP TR 33.899 V1.3.0 (2017-08)
 - RNTI tracking is not a privacy issue because RNTI is not a long lived id
 - But I keep seeing in the lab the RNTI of my devices not changing for hours...
 - TMSI can be mapped to RNTI, but TMSI is also short lived id
 - But the TMSI changes rather infrequently as well...
- LTE hijacking paper shows it is indeed possible!
 - https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

OTHER POTENTIAL LTE LOCATION LEAKS

- Paging messages sent in the clear
 - Known location tracking techniques based on sniffing paging messages
 - Silent text message to target IMSI/TMSI/MSISDN
 - If a paging is sniffed, the UE is in the same Tracking Area as the sniffer
 - If connection establishment is sniffed, the UE is in the same cell as the sniffer



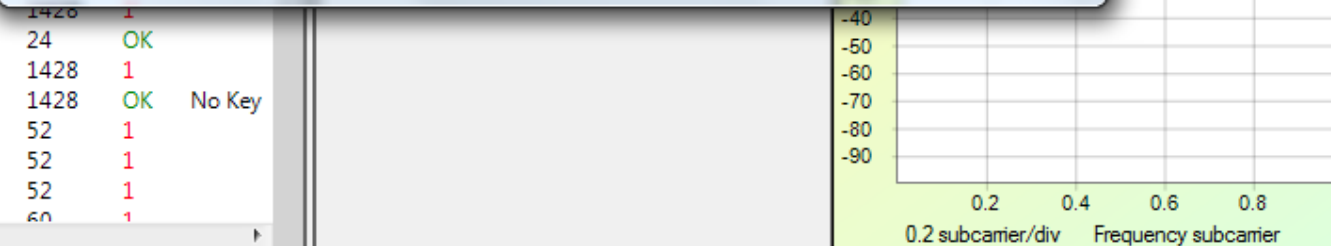
Name	Start time	D/U/I	Cell ID	Frame	RNTI	UEIdentity
Ciphered data	00:01:28.707867	D	138	302		
Unknown Data	00:01:28.771867	D	138	302		
Ciphered data	00:01:28.774867	D	138	303		
Ciphered data	00:01:28.777867	D	138	303		
Ciphered data	00:01:28.780867	D	138	303		
PAGING	00:01:28.782867	D	138	303		
Ciphered data	00:01:28.785867	D	138	304		
Ciphered data	00:01:28.786867	D	138	304		
Ciphered data	00:01:28.789867	D	138	304		
Unknown Data	00:01:28.790867	D	138	304		
Unknown Data	00:01:28.792867	D	138	304		
Unknown Data	00:01:28.796867	D	138	305		
PAGING	00:01:28.802867	D	138	305		
Ciphered data	00:01:28.805867	D	138	306		
RACH	00:01:28.810865	U	138	306		
Ciphered data	00:01:28.812867	D	138	306		
MAC Random Access Response	00:01:28.814867	D	138	307		
RRCConnectionRequest	00:01:28.820864	U	138	307		
PAGING	00:01:28.822867	D	138	307		
Unknown Data	00:01:28.822867	D	138	307		
MAC Random Access Response	00:01:28.824867	D	138	308		
Unknown Data	00:01:28.824867	D	138	308		
Ciphered data	00:01:28.825867	D	138	308		
Unknown Data	00:01:28.826867	D	138	308		
Unknown Data	00:01:28.827867	D	138	308		
RRCConnectionSetup	00:01:28.833867	D	138	309		
Unknown Data	00:01:28.835867	D	138	309		
Unknown Data	00:01:28.837867	D	138	309		
Unknown Data	00:01:28.837867	D	138	309		
Unknown Data	00:01:28.839867	D	138	309		
RRCConnectionSetup	00:01:28.842867	D	138	309		
Unknown Data	00:01:28.843867	D	138	310		
Ciphered data	00:01:28.844867	D	138	310		
Unknown Data	00:01:28.846867	D	138	310		
Unknown Data	00:01:28.846867	D	138	310		
Unknown Data	00:01:28.846867	D	138	310		
Unknown Data	00:01:28.846867	D	138	310		



PAGING at 00:01:28.802867 since connect

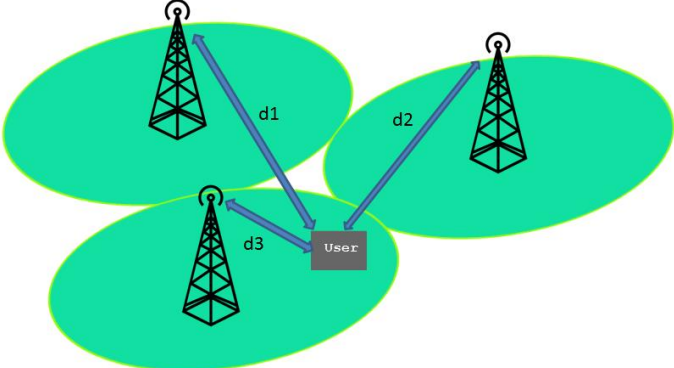
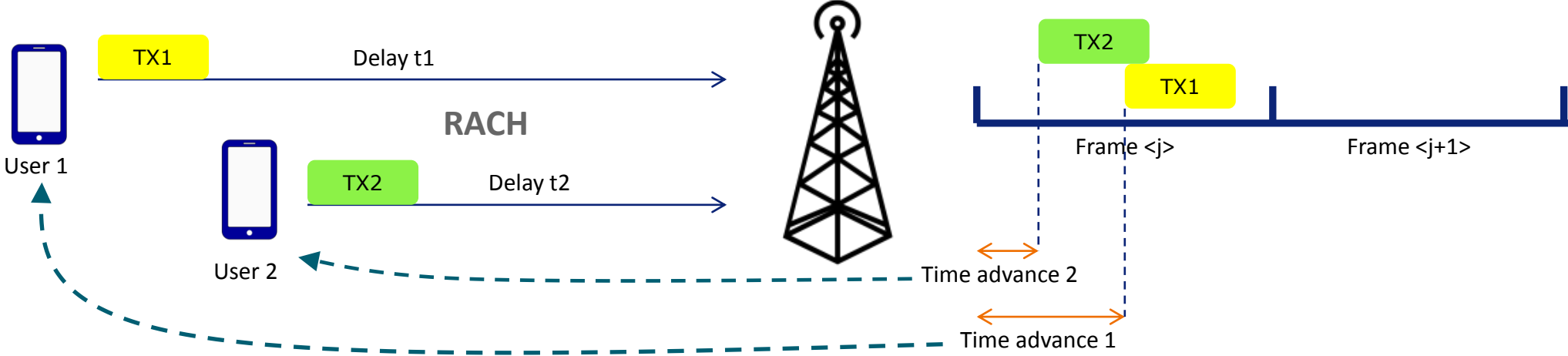
- PCCH-Message
 - message
 - c1
 - paging
 - pagingRecordList
 - PagingRecord
 - ue-identity
 - s-TMSI
 - m-mec {8 bits(0x01)}
 - m-TMSI
 - cn-Domain ps
 - Padding

Bit Length 53 Head 01000000 Tail 11010000 Hex 08000381CFED7A
00000000 40 00 1C 0E 7F 6B D0 00 00 @ kB . .



OTHER POTENTIAL LTE LOCATION LEAKS

- Simple location inference
 - Eavesdrop MAC RAR messages
 - Time Advance \rightarrow distance from eNodeB
 - Very low resolution unless one captures MAC RARs from multiple base stations



Tri-lateration of user's location with eavesdropped MAC-RAR messages

5G SECURITY

5G STANDARDS

- 5G largely a marketing buzz word
 - But there's some actual very interesting technology behind
 - First deployments and tests already happening
- Release 15 of the 3GPP standards
 - December 2017
 - First release of 5G – New Radio + 5G System
- Most changes at the PHY layer
 - mmWave
 - Massive MIMO
- Work to address some protocol exploits
 - IMSI obfuscation and encryption
 - PKI for IMSI concealing
- Security standards published in March 2018
 - 3GPP TS 33.501 V1.0.0 (2018-03)

IMSI PROTECTION

- IMSI encrypted (concealed) with public key of home operator
 - Probabilistic asymmetric encryption
 - Same IMSI encrypted multiple times results in different ciphertexts (to avoid tracking)
- IMSI catching much harder
- Challenges
 - What happens if private key of home operator is “lost” or needs to be rotated?
 - New SIM?
 - New public key burned in SIM?
 - *“Outside of the scope of the 3GPP specifications”*

SUPI – THE NEW IMSI

- SUPI – Subscription Permanent Identifier
 - New IMSI in 5G
 - SUCI (SUbscription Concealed Identifier) – Encrypted SUPI
- Challenges
 - *“If the home network has not provisioned the public key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME.”*
 - Null cipher still supported
 - *“In case of an unauthenticated emergency call, privacy protection for SUPI is not required.”*
 - Can a rogue base station fool a UE to initiate such an emergency call?

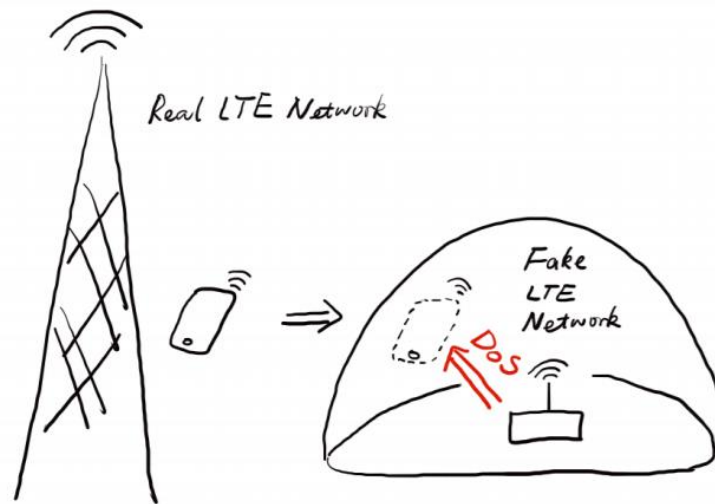
PROTOCOL EXPLOITS IN 5G

- Most LTE protocol exploits caused by implicit trust in pre-authentication messages
 - RRC, MAC, NAS layers
- 5G aims to tackle known exploits in LTE
 - E.g. AttachReject DoS and downgrade to GSM mentioned explicitly
- Leverage public key of home operator?
 - Does not work with roaming devices
 - Public key from all operators?
 - Not scalable
 - Unrealistic
- How are the 5G security specifications preventing exploiting pre-authentication messages?
 - **As of now, 5G appears to be vulnerable to pre-authentication message protocol exploits**

PROTOCOL EXPLOITS IN 5G

- I am not the only one claiming this...

Fake 5G Base Station may still Exist



DoS attack examples:

- ✓ You are an illegal cellphone!
- ✓ Here is NO network available. You could shut down your modem.

The root cause is the initial broadcasting message from network can not be proved to be trustable.

NO **PKI infrastructure** solution reaches agreement in 3GPP.



“OUT OF SCOPE”

This works for most wireless security specifications:

**Ctrl+F for {“scope”, “out of scope”, “out of the scope”, etc}
In mobile communication standard documents**

- 5.2.5 – Subscriber privacy
 - “The provisioning and updating of the home network public key is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism.”
- 12.2 – Mutual authentication
 - “The structure of the PKI used for the certificate is out of scope of the present document.”
- C.3.3 – Processing on home network side
 - “How often the home network generates new public/private key pair and how the public key is provisioned to the UE are out of the scope of this clause.”

NULL CIPHERING

- Supported ciphering modes
 - **NEA0 - Null ciphering algorithm**
 - 128-NEA1 - 128-bit SNOW 3G based algorithm
 - 128-NEA2 - 128-bit AES based algorithm
 - 128-NEA3 - 128-bit ZUC based algorithm
- **Null ciphering** is a supported option
 - **Same for null integrity**
 - Potential security edge cases
 - Bidding down attacks
 - Public key of home operator burned in SIM
 - How to authenticate a bidding down request at a foreign (roaming) network?
- Note null ciphering support often a requirement for Lawful Interception

POTENTIAL SECURITY EDGE CASES

- *“In case the UE registers for Emergency Services and receives an Identifier Request, the UE shall use the null-scheme for generating the SUCI in the Identifier Response.”*
- *“If the UE receives a NAS security mode command selecting NULL integrity and ciphering algorithms, the UE shall accept this as long as the IMS Emergency session progresses.”*
- *“If the authentication failure is detected in the AMF then the UE is not aware of the failure in the AMF, but still needs to be prepared, according to the conditions specified in TS 24.301, to accept a NAS SMC from the AMF requesting the use of the NULL ciphering and integrity algorithms.”*
- *“If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.”*
- ...

5G SECURITY - ARE WE THERE YET?

NAS integrity activation:

“Replay protection shall be activated when integrity protection is activated, except when the NULL integrity protection algorithm is selected.”

Are we there yet? The long path to securing 5G mobile communication networks“
<https://www.linkedin.com/pulse/we-yet-long-path-securing-5g-mobile-communication-piqueras-jover>

Q&A

<http://rogerpiquerasjover.net> ----  @rgoestotheshows

FURTHER READING

FURTHER READING

- Shaik, Altaf, et al. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems." arXiv preprint arXiv:1510.07563 (2015).
- Jover, Roger Piqueras. LTE Security and Protocol Exploits. ShmooCon 2016.
- Jover, Roger Piqueras, Joshua Lackey, and Arvind Raghavan. "Enhancing the security of LTE networks against jamming attacks." EURASIP Journal on Information Security 2014.1 (2014): 1-14.
- Jover, Roger Piqueras. "Security attacks against the availability of LTE mobility networks: Overview and research directions." Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on. IEEE, 2013.
- M. Lichtman, R. Piqueras Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation," Communications Magazine, IEEE, vol. 54, no. 4, 2016.
- Engel, Tobias. "SS7: Locate. Track. Manipulate." FTP: <http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf>. 2014.
- Kumar, Swarun, et al. "LTE radio analytics made easy and accessible." ACM SIGCOMM Computer Communication Review. Vol. 44. No. 4. ACM, 2014.
- Spaar, Dieter. "A practical DoS attack to the GSM network." In DeepSec (2009).
- Kune, Denis Foo, et al. "Location leaks on the GSM Air Interface." ISOC NDSS (Feb 2012) (2012).
- Jermyn, Jill, et al. "Scalability of Machine to Machine systems and the Internet of Things on LTE mobile networks." World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a. IEEE, 2015.
- Lichtman, Marc, et al. "Vulnerability of LTE to hostile interference." Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE. IEEE, 2013.

FURTHER READING

- Golde, Nico, Kévin Redon, and Jean-Pierre Seifert. "Let me answer that for you: Exploiting broadcast information in cellular networks." Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13). 2013.
- Mulliner, Collin, Nico Golde, and Jean-Pierre Seifert. "SMS of Death: From Analyzing to Attacking Mobile Phones on a Large Scale." USENIX Security Symposium. 2011.
- Bhattarai, Sudeep, et al. "On simulation studies of cyber attacks against lte networks." Computer Communication and Networks (ICCCN), 2014 23rd International Conference on. IEEE, 2014.
- Ghavimi, Fayeze, and Hsiao-Hwa Chen. "M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications." Communications Surveys & Tutorials, IEEE 17.2 (2015): 525-549.
- Nakarmi, Prajwol Kumar, Oscar Ohlsson, and Michael Liljenstam. "An Air Interface Signaling Protection Function for Mobile Networks: GSM Experiments and Beyond." Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.
- Khosroshahy, Masood, et al. "Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface." Mobile and Wireless Networking (MoWNeT), 2013 International Conference on Selected Topics in. IEEE, 2013.
- Bailey, D. "War Texting: Weaponizing Machine to Machine." Black-Hat USA (2011).
- Nohl, Karsten, and Sylvain Munaut. "Wideband GSM sniffing." In 27th Chaos Communication Congress. 2010.
- Prasad, Anand. "3GPP SAE-LTE Security." NIKSUN WWSMC (2011).
- Jermyn, Jill, Gabriel Salles-Loustau, and Saman Zonouz. "An analysis of dos attack strategies against the LTE RAN." Journal of Cyber Security 3.2 (2014): 159-180.
- Bailey, Don, and Nick DePetrillo. "The Carmen Sandiego Project." Proc. of BlackHat (Las Vegas, NV, USA, 2010) (2010).

FURTHER READING

- Hussain, Syed Rafiul, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE." In Symposium on Network and Distributed Systems Security (NDSS), pp. 18-21. 2018.
- Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. "Breaking LTE on Layer Two." In Breaking LTE on Layer Two, p. 0. IEEE..
- Hussain, Syed Rafiul, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE." In Symposium on Network and Distributed Systems Security (NDSS), pp. 18-21. 2018..
- Jover, Roger Piqueras, and Vuk Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications." arXiv preprint arXiv:1809.06925 (2018).
- Raza, Muhammad Taqi, Fatima Muhammad Anwar, and Songwu Lu. "Exposing LTE Security Weaknesses at Protocol Inter-Layer, and Inter-Radio Interactions." In International Conference on Security and Privacy in Communication Systems, pp. 312-338. Springer, Cham, 2017.
- Khan, Haibat, Benjamin Dowling, and Keith M. Martin. "Identity Confidentiality in 5G Mobile Telephony Systems." 2018.
- Mjølsnes, Stig F., and Ruxandra F. Olimid. "Easy 4G/LTE IMSI Catchers for Non-Programmers." In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, pp. 235-246. Springer, Cham, 2017.
- Khan, M., Ginzboorg, P., Järvinen, K. and Niemi, V., 2018. Defeating the Downgrade Attack on Identity Privacy in 5G. arXiv preprint arXiv:1811.02293.
- Basin, David, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. "A Formal Analysis of 5G Authentication." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1383-1396. ACM, 2018.