How to Verify Your LTE Protocol and RF interactions

Introducing 89600 WLA Software

Peter Cain, Agilent Technologies
Overview

• The LTE downlink uses many messages in different layers to manage the operation of the radio link
  ➢ You have to be able to read all of these messages to find out if the system is working correctly

• In many situations outside RF conformance test, the contents of the link are constantly changing
  ➢ You can only understand what’s happening by observing activity over multiple radio frames
  ➢ Which then invalidates test results

• Testing one frame at a time carries the risk of missing important issues in the test signal

• 89600 WLA software provides the most cost effective extension of an existing analysis tool
  ➢ If you’re familiar with 89600 this is a powerful addition
Agenda

• Challenges Addressed
• Finding RF Control Information hidden in LTE Layer 2/3 protocols
• Examining Control Loop Operation
• Agilent Solutions
• Q&A
Challenges Addressed

**eNB Development:** You are building the baseband signal and need to independently verify it

**UE Testing:** You are feeding an unknown base station signal into a UE receiver and want to check the content

**eNB or UE:**
- You have a low level interoperability problem
- You need to find out why throughput results are not as high as you expected

**or:** You need to understand the structure of the signals & operation of the LTE radio system
The LTE Air Interface Protocol Stack

Layer 3
- Radio Resource Control (RRC)

Layer 2
- Radio Link Control (RLC)
- Medium Access Control (MAC)

Layer 1
- Physical Layer (PHY)
- Transceiver
A Refresher: The 5 DL Channels & What They Do

- **Broadcast Channel** sends basic information about the cell using the Master Information Block
- **Control Format Indicator** tells the UE(s) where to look for the control channel (the key to the allocation map)
- **Control Channel** where the eNB tells UEs when to expect their downlink data, and when & how to transmit
- **Shared Channel** has several uses, including sending data to the UEs and broadcasting System Information Blocks
- **HARQ Indicator** is the feedback channel to tell the UE which uplink transport blocks it has to retransmit
Combining Views of the Physical and Detected

Spectrogram – shows what is actually transmitted

Detected Allocations – the logical view

PCFICH

PDCCH

PDSCH

PBCH

S-SS

P-SS

PHICH (if present)

Time

Frequency
89600 VSA Provides Extensive LTE Decoding

- Spectrum & Time views
- Constellation & Error summary
- Detected Allocations
- Decoded Information
- Frame summary
89600 WLA Builds on 89600 VSA Capability
89600 WLA Overview

- Message Log & Frame view
- Individual Message Contents
- PUSCH Allocations
- Uplink configuration parameters
- Analysis with Microsoft® Excel®
EXAMPLE: DCI Scheduling for UE Power Control

<table>
<thead>
<tr>
<th>Allocation Code</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSCH</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TPC Command Field</th>
<th>Accumulated</th>
<th>Absolute change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-1 dB</td>
<td>-4 dB</td>
</tr>
<tr>
<td>1</td>
<td>0 dB</td>
<td>-1 dB</td>
</tr>
<tr>
<td>2</td>
<td>1 dB</td>
<td>1 dB</td>
</tr>
<tr>
<td>3</td>
<td>3 dB</td>
<td>4 dB</td>
</tr>
</tbody>
</table>

Transmit Power Control command
UE Transmit Power Control Loop Operation

Are timing & level change consistent with channel changes?

Frame Number (Time)
The LTE Air Interface Protocol Stack

Layer 3
  - Radio Resource Control (RRC)

Layer 2
  - Radio Link Control (RLC)
  - Medium Access Control (MAC)
    - MAC control headers & elements are added to the front of user payloads

Layer 1
  - Physical Layer (PHY)
  - Transceiver

Used for frequent configuration commands
- Timing Advance
- Power headroom reports
- Buffer status reports
- C-RNTI signalling
- DRX commands
- MBMS dynamic scheduling

Copyright © 2011 Agilent Technologies
The LTE Air Interface Protocol Stack

Layer 3
- Radio Resource Control (RRC)

Layer 2
- Radio Link Control (RLC)
- Medium Access Control (MAC)

Layer 1
- Physical Layer (PHY)
- Transceiver

Used for more persistent configurations of the RF & periodic signalling over longer timescales

Procedures include
- Sending System Information
- Connection Control (set-up, configure & release of bearer services, security associations)
- Measurements (configuration, filtering, triggers and reporting)
- Inter-RAT Mobility (handovers)
LTE Protocol Layers and Channels

**Control Plane**

- **RRC**
  - System Information & Paging
  - RRC Connection establishment
  - RRC dedicated control
  - NAS direct transfer

- **PDCP**

- **RLC**
  - RLC Service Access Points
  - Transparent Mode

- **MAC**
  - Scheduling & Priority Handling
  - Multiplexing and HARQ control

**Logical Channels**
- BCCH
- PCCH
- CCCH
- DCCH1
- DCCH2
- DTCH1
- DTCH2
- DTCH3

**Transport Channels**
- BCH
- PCH
- DLSCH
- DCI
- CFI
- HARQ Indicator

**Physical Layer**

Packet Data Convergence Protocol SAPs

Ref: TS36.300

2011 Greater insight. Greater confidence.
LTE Protocol Layers and Channels

- Network Access Stratum
  - RRC
    - System Information & Paging
    - RRC Connection establish
    - RRC dedicated control
    - NAS direct transfer
  - SRB 0
  - SRB 1
  - SRB 2

- Packet Data Convergence Protocol SAPs

- Physical Layer
  - Transport Channels
    - BCH
    - PCH
    - DLSCH
    - DCI
    - CFI
    - HARQ Indicator

- Logical Channels

- MAC
  - Scheduling & Priority Handling
  - Multiplexing and HARQ control

- RLC Service Access Points
  - Transparent Mode
  - Acknowledge Mode
  - UnAck

- RLC PDU & ARQ

- PDCP
  - Integrity & Ciphering

- User Plane
  - Traffic data including service related signalling
    - Service signalling traffic
    - NRT data traffic
    - RT data traffic

- System Information & Paging

- Ref: TS36.300

Copyright © 2011 Agilent Technologies
The LTE Air Interface Protocol Stack

Layer 3
- Radio Resource Control (RRC)

Layer 2
- Radio Link Control (RLC)
- Medium Access Control (MAC)

Layer 1
- Physical Layer (PHY)
- Transceiver
Layer 2 – Medium Access Control

**Logical Channels**
- BCCH
- PCCH
- CCCH
- DCCH1
- DCCH2
- DTCH1
- DTCH2
- DTCH3

**Transport Channels**
- BCH
- PCH
- DLSCH
- DCI
- CFI
- HARQ Indicator

**Physical Channels**
- PBCH
- DLSCH
- PDCCH
- PCFICH
- PHICH

- **Maps information flows** in logical channels to the physical layer, through transport channels
- **Manages HARQ processes** for each information flow, and the random access process
- **Responsible for channel prioritization and scheduling** of physical resources
MAC Protocol Data Unit Structure (3GPP TS 36.321)

SDU: Service Data Unit (Payload)
EXAMPLE: MAC Control Element Timing Advance

- **Initial Random Access Response, RAR Message**
- **T.A. MAC Control Element**
- **Timing Adjustments**
- **Initial 11-bit Timing Advance Setting**
Tracking Changes to Timing Advance

Timing Advance

Frame Number (Time)

Frame .subframe

Timing Advance

US

0 0.2 0.4 0.6 0.8 1 1.2

945.0 950.0 955.0 960.0 965.0 970.0 975.0 980.0 985.0
Downlink MAC Hybrid-ARQ (Asynchronous)

- Each DL HARQ process may have **variable** timing
- The eNB can transmit as soon as it receives the ACK/NACK from the UE, depending on RB availability

![Diagram of Downlink MAC Hybrid-ARQ](image)

**DL HARQ Process n**

- ACK/NACK from UE on PUCCH or PUSCH

**Next HARQ Process n**

- Variable interval

- Fixed 4 sub-frame interval

- ACK/NACK from UE on PUCCH or PUSCH
Downlink MAC HARQ Redundancy Version

- If data is NACKed, redundancy version is changed
- 89600 WLA can infer successful data transmission using RV and New Data Indicator
Are the downlink HARQ processes limiting data throughput?
DL HARQ: Add Noise Bursts to Channel

Are the downlink HARQ processes limiting data throughput?
Successful HARQ transmission of PDSCH data can be inferred from the presence or absence of retransmissions.

Throughput is represented by the slope of the acknowledged bits.

Immediate re-use of the same HARQ process after 4 successive failures.

RV = 0-2-3-1

The UE has failed to recover the DL signal for 3 consecutive frames; implying an extended problem or a significant issue with the initial transmission.

2011 Greater insight. Greater confidence.
Sample Result

Downlink Data Transmission, by HARQ Process Number

Unexpected: Multiple processes retransmitting

Expected: Single retransmission (delay 8ms)

Unexpected: One process cycles through 4 redundancy versions
HARQ in the Uplink Using PHICH

89600 VSA decodes DL signal, including PHICH
The LTE Air Interface Protocol Stack

Layer 3
- Radio Resource Control (RRC)

Layer 2
- Radio Link Control (RLC)
- Medium Access Control (MAC)

Layer 1
- Physical Layer (PHY)
- Transceiver
# Radio Link Control Protocol – 3 Levels of Service

## Transparent Mode
- **No segmentation** and reassembly of RLC SDUs
- No RLC headers are added
- **No delivery guarantees**
- Limited to system information, paging messages, and the exchange of RRC connection establishment messages associated with CCCH

## Unacknowledged Mode
- **Segmentation** of RLC SDUs into a size requested by the MAC layer
- RLC Headers are added
- **No delivery guarantees**
- Suitable for carrying streaming traffic
- Applied only to the user plane, where it would be utilised for packet traffic flows with low tolerance to delay (e.g. VoIP).

## Acknowledged Mode
- **Segmentation** of RLC SDUs into a size requested by the MAC layer
- RLC Headers are added
- **Reliable in sequence delivery service**
- Provides retransmission of failed RLC PDUs if required
- Suitable for carrying TCP traffic
- Used in the control plane for RRC signalling messages carried in DCCH and for user plane traffic carried in DTCH
The LTE Air Interface Protocol Stack

Layer 3
- Radio Resource Control (RRC)

Layer 2
- Radio Link Control (RLC)
- Medium Access Control (MAC)

Layer 1
- Physical Layer (PHY)
- Transceiver

The RRC is large and complex, covering a number of functional areas:

- **System Information** – the broadcast of system information to all UEs
- **RRC Connection Control** – all procedures related to the establishment, modification and release of an RRC connection (e.g. RNTI assignment), including Data/Signalling Radio Bearers (DRB/SRB) establishment
- **Mobility related functions** – inter-cell, inter-RAT, inter-eNode-B mobility procedures and transfer of context information
- **Measurement configuration and reporting** – for mobility, handovers and configuration of measurement gaps
- **Miscellaneous features** – including, for example, the transfer of dedicated Non-Access-Stratum (NAS) information, and UE radio access capability information
RRC Signalling Radio Bearers (3GPP TS 36.331)

**Control Plane**

- **NAS**
  - System Information & Paging
  - RRC Connection establishment
  - RRC dedicated control
  - NAS direct transfer

- **RRC**
  - SRB 0
  - SRB 1
  - SRB 2

- **Layer 2 Logical Channels**
  - BCCH/PCCH
  - CCCH
  - DCCH

**User Plane**

- Traffic data including service related signalling
  - DRB 0
  - DRB 1
  - DRB n

<table>
<thead>
<tr>
<th>RRC Signalling Radio Bearer</th>
<th>Control Plane signalling</th>
<th>Message contents</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRB 0</td>
<td>CCCH</td>
<td>Non-UE specific</td>
<td>Low</td>
</tr>
<tr>
<td>SRB 1</td>
<td>DCCH</td>
<td>RRC +NAS</td>
<td>High</td>
</tr>
<tr>
<td>SRB 2</td>
<td>DCCH</td>
<td>NAS only</td>
<td>Low</td>
</tr>
</tbody>
</table>

**2011 Greater insight. Greater confidence.**

Copyright © 2011 Agilent Technologies
<table>
<thead>
<tr>
<th>Type</th>
<th>Key Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB</td>
<td>DL Bandwidth, PHICH Configuration, System Frame #</td>
</tr>
<tr>
<td>SIB1</td>
<td>Information relevant when evaluating if a UE is allowed to access a cell and defines the scheduling of other system information blocks</td>
</tr>
<tr>
<td>SIB2</td>
<td>Common and shared channel information</td>
</tr>
<tr>
<td>SIB3</td>
<td>Cell re-selection information, mainly related to the serving cell</td>
</tr>
<tr>
<td>SIB4</td>
<td>Information about the serving frequency and intra-frequency neighbouring cells relevant for cell re-selection (including cell re-selection parameters common for a frequency as well as cell specific re-selection parameters)</td>
</tr>
<tr>
<td>SIB5</td>
<td>Information about other E-UTRA frequencies and inter-frequency neighbouring cells relevant for cell re-selection (including cell re-selection parameters common for a frequency as well as cell specific re-selection parameters)</td>
</tr>
<tr>
<td>SIB6</td>
<td>Contains information about UTRA frequencies and UTRA neighbouring cells relevant for cell re-selection (including cell re-selection parameters common for a frequency as well as cell specific re-selection parameters)</td>
</tr>
<tr>
<td>SIB7</td>
<td>Contains information about GERAN frequencies relevant for cell re-selection (including cell re-selection parameters for each frequency)</td>
</tr>
<tr>
<td>SIB8</td>
<td>Contains information about CDMA2000 frequencies and CDMA2000 neighbouring cells relevant for cell re-selection (including cell re-selection parameters common for a frequency as well as cell specific re-selection parameters)</td>
</tr>
<tr>
<td>SIB9</td>
<td>Contains a home eNB identifier (HNBID)</td>
</tr>
<tr>
<td>SIB10</td>
<td>ETWS (Earthquake and Tsunami Warning System) primary notification</td>
</tr>
<tr>
<td>SIB11</td>
<td>ETWS secondary notification</td>
</tr>
</tbody>
</table>
Radio Resource Control High Level Signalling

RRC Connection Establishment

RRC Connection Reconfiguration
• Establish, modify or release user radio bearers, e.g. during handovers

RRC Connection Re-establishment
• Re-activates security (without algorithm change)
• Only if cell is prepared (maintains context), and security is active
• Used if coverage temporarily lost, e.g. during Handover
UE Attach Message Capture

E6621A PXT (eNodeB emulator)

N9020A MXA Signal Analyzer

Is the UE getting the correct configuration information from the eNodeB?
UE Attach Message Capture

E6621A PXT (eNodeB emulator)  N9020A MXA Signal Analyzer

Voltage depends on power (ZX47 is a negative going detector)

2011 Greater insight. Greater confidence.
### DL Messages & Timing during Connection Setup

<table>
<thead>
<tr>
<th>RFN Hex</th>
<th>RFN Dec</th>
<th>Sub No</th>
<th>Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x26A</td>
<td>618</td>
<td>5</td>
<td>RNTI: 0xFFFF : DL</td>
</tr>
<tr>
<td>0x26A</td>
<td>618</td>
<td>5</td>
<td>System Information</td>
</tr>
<tr>
<td>0x26C</td>
<td>620</td>
<td>5</td>
<td>RNTI: 0xFFFF : DL</td>
</tr>
<tr>
<td>0x26C</td>
<td>620</td>
<td>5</td>
<td>System Information</td>
</tr>
<tr>
<td>0x26D</td>
<td>621</td>
<td>9</td>
<td>RNTI: 0x0004 : DL</td>
</tr>
<tr>
<td>0x26D</td>
<td>621</td>
<td>9</td>
<td>Random Access Pre-ambles</td>
</tr>
<tr>
<td>0x26E</td>
<td>622</td>
<td>5</td>
<td>RNTI: 0xFFFF : DL</td>
</tr>
<tr>
<td>0x26E</td>
<td>622</td>
<td>5</td>
<td>System Information</td>
</tr>
<tr>
<td>0x26F</td>
<td>623</td>
<td>5</td>
<td>RNTI: 0x000C : DL</td>
</tr>
<tr>
<td>0x26F</td>
<td>623</td>
<td>5</td>
<td>UE Contention Re</td>
</tr>
<tr>
<td>0x26F</td>
<td>623</td>
<td>5</td>
<td>DL-CCCH-Messages</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RRCConnectionSetup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SIB-2, SystemInformationBlockType2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DL InformationTransfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SecurityModeCommand</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UE CapabilityEnquiry</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RRCConnectionReconfiguration</td>
</tr>
</tbody>
</table>

**Message Types:**
- DCI 1A: Compact PDSCH codeword
- SIB-1, SystemInformationBlockType1
- MAC RAR Control Message
- MAC Control Message
- RLC Control Message
- DL Information Transfer
- Security Mode Command
- UE Capability Enquiry
- RRC Connection Reconfiguration
**SIB 2 & RRC Connection for PUCCH Config.**

- **INFORMATION:** Number of spare bits: 190

```
<+SIB-2, SystemInformationBlockType2>
  <WLA Decode Results>
  <WLA Decoding Status>
  
  <BCCH-DL-SCH-MessageType>
  <ct>
  <systemInformation>
    <criticalExtensions>
    <systemInformation-r8>
    <sib-TypeAndInfo>
      <sib3>
        <radioResourceConfigCommon>
        <rach-Config>
        <bcch-Config>
        <pch-Config>
        <prach-Config>
        <pdsch-Config>
        <pusch-Config>
    <pucch-Config>
    <soundingRS-UL-Config>
    <uplinkPowerControl>
    <ul-CyclicPrefixLength>
    <srs-TimingAndConfig>
  
  <freqInfo>
  <timeAlignmentTimerCommon>
  <sib3>
  <cellReselectionInfoCommon>
    <q-Hyst>
    <cellReselectionServingFreqInfo>
    <thresholdServingLow>
    <cellReselectionPriority>
    <intraFreqCellReselectionInfo>
      <q-RxLevMin>
      <allowedMissedBandwidth>
      <presenceAntennaPort>
      <neighCellConfig>
      <t-ReselectionEUTRA>
```

**Uplink Power Control**

- DeltaF_pucch(F)
  - Format 1: deltaF0
  - Format 1b: deltaF3
  - Format 2: deltaF0
  - Format 2a: deltaF0
  - Format 2b: deltaF0

**Channel Parameters**

- NRB(2): 8
- Ncs(1): 6
- NPUCCH(1): 0
- Δshift: PUCCH ds2
Downlink / Uplink Capture

Using a 2\textsuperscript{nd} analyzer & 89600 VSA to:

1. Trigger on uplink
2. Capture the uplink
CQI Control Loop Testing

E6621A PXT (eNodeB emulator)

N9020A MXA Signal Analyzer

N5182A MXG Vector Signal Generator

LTE Frame trigger output

Noise Burst

Trig Out

Pulse

Sweep out

Ext Trig 1 In

Does the CQI feedback process act fast enough?

50ms noise bursts added to downlink

Downlink frames

50-250 ms noise bursts
Test CQI Control Loop Using UE Reporting

• eNodeB uses **channel feedback** from the UE to determine MCS allocations

• UE reports HARQ feedback and CQI using PUCCH (or PUSCH)

• Control loop timescale is longer (depends on UE reporting interval)
Test CQI Control Loop Using UE Reporting

- eNodeB uses channel feedback from the UE to determine MCS allocations
- UE reports HARQ feedback and CQI information using PUCCH (or PUSCH)
- Control loop timescale is longer

- Test response by injecting longer periods of AWGN

- HARQ NACKs result in retransmissions
- Uplink CQI reports should result in new MCS
89600 VSA Uplink Synchronization & Analysis

89600 WLA provides UE configuration for UL synch. & demod.

89600 VSA demodulates uplink signal
Uplink PUCCH Decoding

89600 VSA decodes uplink signal contents
PUCCH Reporting: HARQ, CQI, PMI, RI

- **HARQ** Size & Info
- **CQI** Size & Info
- **PMI** (MIMO)
- **RI** (MIMO)

### Analysis Key

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>There is ambiguity in the signal (when using auto-detection)</td>
</tr>
<tr>
<td>F</td>
<td>The pattern has bit errors</td>
</tr>
<tr>
<td><strong>Size</strong>= 0</td>
<td>The signal not present / found</td>
</tr>
<tr>
<td><strong>Info</strong>= 0xF00</td>
<td>Result, front loaded Hex format</td>
</tr>
</tbody>
</table>

![PUCCH Decoder Info](image)
UL HARQ & CQI Changes In Noisy Channel

HARQ goes from 0xC [1100] ACK to 0x0 [0000] NACK

CQI goes from 0xE (very good) to 0x3 (poor)
Agenda

• Challenges Addressed
• Finding RF Control Information hidden in LTE Layer 2/3 protocols
• Examining Control Loop Operation
• Agilent Solutions
• Q&A
89600B VSA Signal Analysis

In-depth analog and demodulated signal analysis

Option BHD FDD, BHE TDD, BHG, BHH LTE Advanced
89600 WLA Software for LTE

89620B: In-depth analysis of the LTE link operation using information from RRC, RLC and MAC protocol layers

www.agilent.com/find/wla
Signal Capture

X series
Analyzers

Infiniium
Oscilloscopes

Modular
N7100A
PXI M9392A

89600 supports all these types of hardware

Choice of RF range, bandwidth, baseband IQ inputs

MIMO or synchronous FDD capture (MXA/EXA)
E6621A (MIMO) Real Time eNB Emulator

N6051A RF parametric test with test mode signaling
N6052A Functional and application test
N6061A Protocol logging and analysis
N6062A Message editor
1: **Information** used to control the LTE RF link **is spread across all the protocol layers**, from System Information Blocks in layer 3 to the DCI content in the PHY.
Summary

1: **Information** used to control the LTE RF link is spread across **all the protocol layers**, from System Information Blocks in layer 3 to the DCI content in the PHY.

2: Being able to recover this information **allows verification** of the signal content, to **ensure the correct configuration** is being used for testing.
1: **Information** used to control the LTE RF link is spread across all the protocol layers, from System Information Blocks in layer 3 to the DCI content in the PHY.

2: Being able to recover this information allows verification of the signal content, to ensure the correct configuration is being used for testing.

3: LTE has at least six control loops running during normal operation, including power, timing & MCS control and DL/UL HARQ retransmissions.
Summary

1: **Information** used to control the LTE RF link is **spread across all the protocol layers**, from System Information Blocks in layer 3 to the DCI content in the PHY.

2: Being able to recover this information **allows verification** of the signal content, to **ensure the correct configuration** is being used for testing.

3: **LTE has at least six control loops** running in normal operation, including power, timing and modulation control and downlink / uplink HARQ retransmissions.

4: **89600 WLA software** provides the messaging information and graphing needed to observe control loop behaviour.
References

1: LTE and The Evolution to 4G Wireless Design and Measurement Challenges Agilent Technologies. Edited by Moray Rumney
www.agilent.com/find/ltebook

2: 3GPP specifications 36.211, 36.212, 36.213, 36.300

3: 89600 Help system (provides further references to the standard)

4: Webcast for more detailed description of uplink, including spectrograms:
http://www.eetimes.com/electrical-engineers/education-training/webinars/4211278/How-To-Verify-the-Data-In-Your-LTE-Uplink-Signal

Acronym list: http://www.home.agilent.com/upload/cmc_upload/All/LTE_Acronyms.pdf

With thanks to colleagues at Agilent Technologies for their help in preparing this presentation
Thanks for your time. We hope this has been helpful