Protocol log analysis with constraint programming
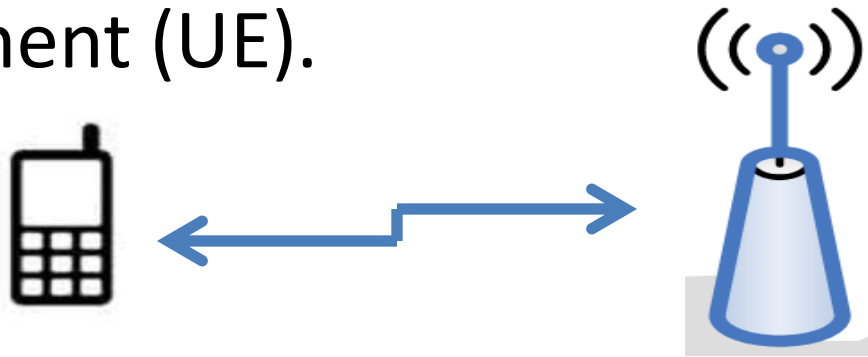
Mats Carlsson   Olga Grinchtein   Justin Pearson

Outline

- Overview
- LTE Radio Access Network
- A case study Public Warning System
- Testing Procedure
- Protocol log generation
- Protocol log analysis
- Ongoing work

Overview

- The LTE Radio Base Station (RBS) is SUT at our department at Ericsson.

- The LTE RBS communicates with the User Equipment (UE).

- The LTE RBS has different functions. Our case study is Public Warning System.

Overview

- Test harness should analyze UE protocol logs

- Protocol logs are sequences of messages with timestamps

- Number of logs with errors should be generated for testing telecommunication test harness

- We use constraint solver for modeling and generation of protocol logs ([DATE'14])

- Constraint solver can also be used for protocol log analysis

LTE Radio Base Station (eNodeB)

LTE Radio Access Network consists of LTE Radio Base Stations (RBS), which support the LTE air interface and performs radio resource management.

An eNB connects to User Equipment (UE) via the air interface.

LTE RBSes are interconnected with each other by means of the X2 interfaces.

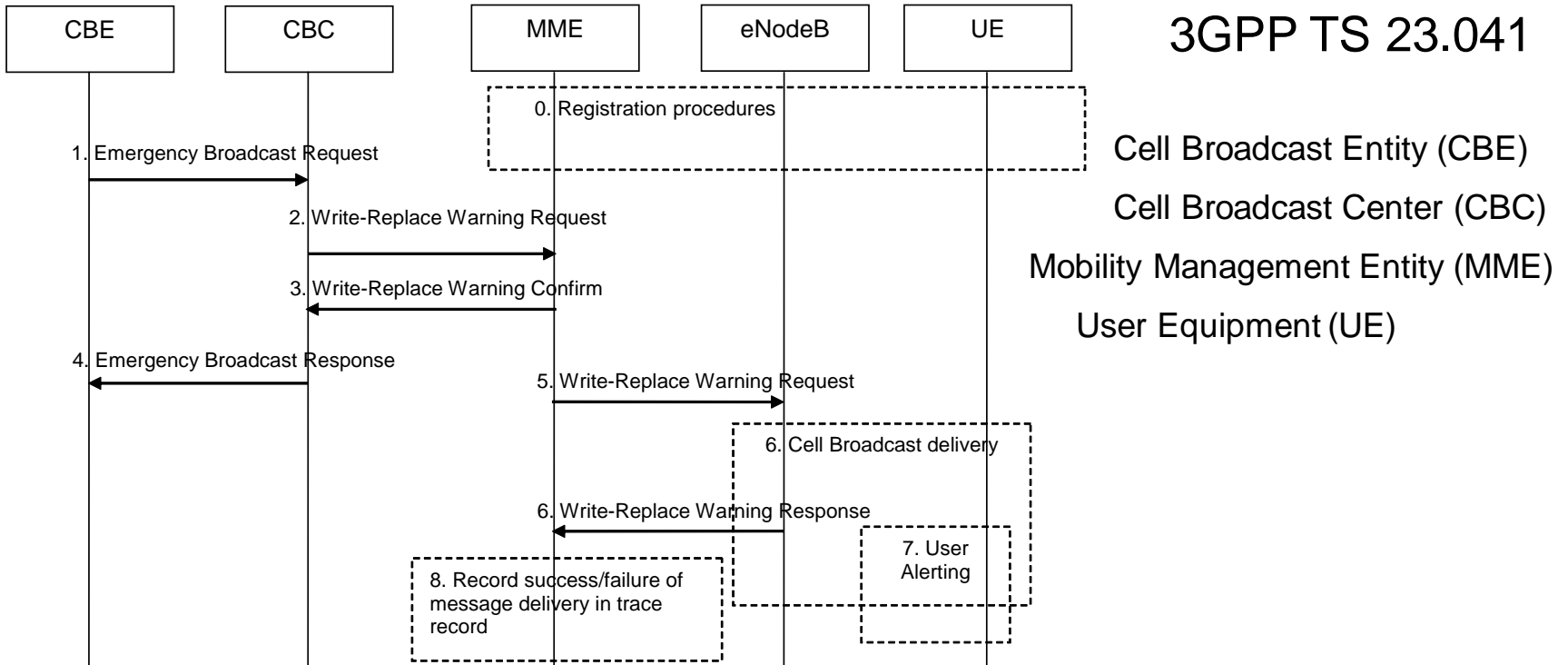LTE RBSes are also connected by means of the S1 interface to the Evolved Packet Core

MME / S-GW

MME / S-GW

S1

S1

S1

S1

X2

X2

X2

eNB

eNB

eNB

E-UTRAN

UE
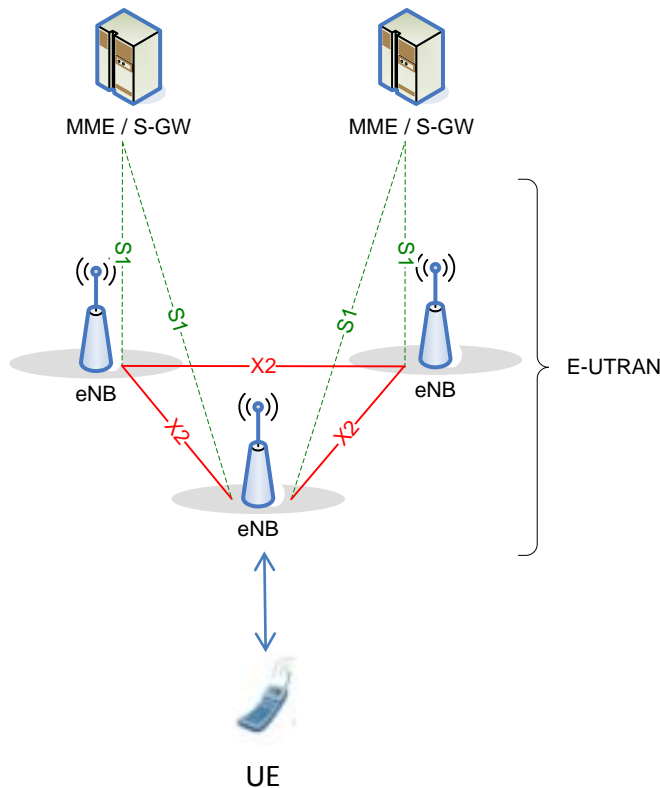
Mobility Management Entity (MME)

Serving Gateway (S-GW)

User Equipment (UE)

3GPP TS 36.300

Public Warning System

3GPP TS 23.041

Cell Broadcast Entity (CBE)
Cell Broadcast Center (CBC)
Mobility Management Entity (MME)
User Equipment (UE)

CBE	CBC	MME	eNodeB	UE

0. Registration procedures

1. Emergency Broadcast Request

2. Write-Replace Warning Request

3. Write-Replace Warning Confirm

4. Emergency Broadcast Response

5. Write-Replace Warning Request

6. Cell Broadcast delivery

6. Write-Replace Warning Response

7. User Alerting

8. Record success/failure of message delivery in trace record

Public Warning System

eNodeB → UE

paging

system information

system information

system information

paging

system information

The eNodeB sends different types of system information messages
- SIB1 (schedulingInfoList)
- SIB10 (primary notification)
- SIB11 (secondary notification)

Secondary notification can come in one or several segments

Testing Procedure

1. Test harness initializes some parameters in eNB.
2. Test harness initiates logging in UE simulator
3. Test harness initiates transmission of messages between MME simulator and eNB
4. Test harness captures and analyses UE protocol log.
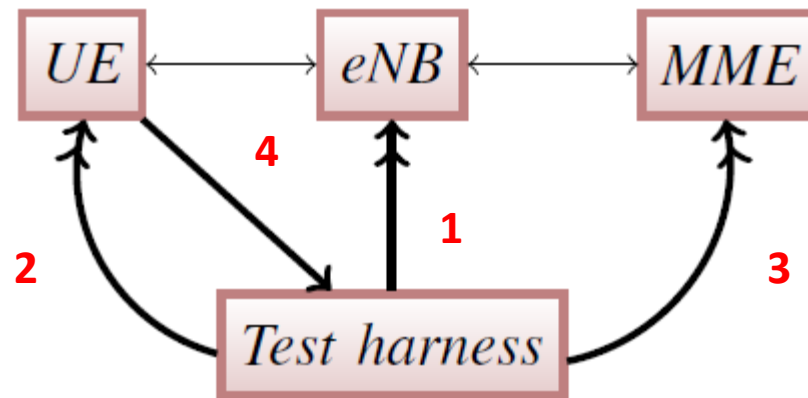
UE protocol log generation ([DATE'14])

- Modelling in Sicstus Prolog
- Model describes how UE acquires primary and secondary notifications sending by eNB after receiving one warning message from MME
- The model is a set of constraints on parameters, which represent timestamps, content of messages or indicate if a message should appear in log.
- Parameters are grouped into lists, that is a Prolog data-structure
- Inject faults into the model
- Based on solutions provided by Sicstus Prolog we generate UE protocol logs
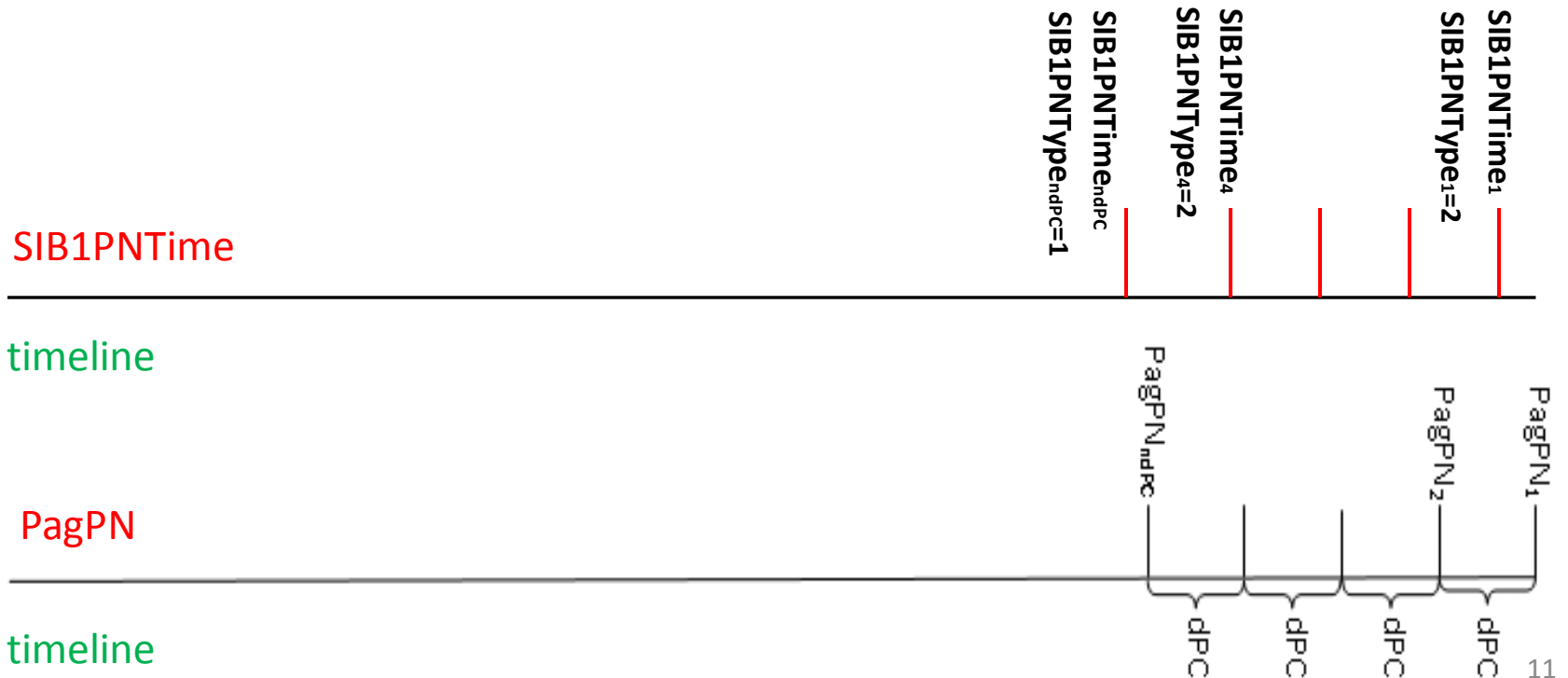
Paging messages

PagPN is array of timestamps of paging messages of primary notification

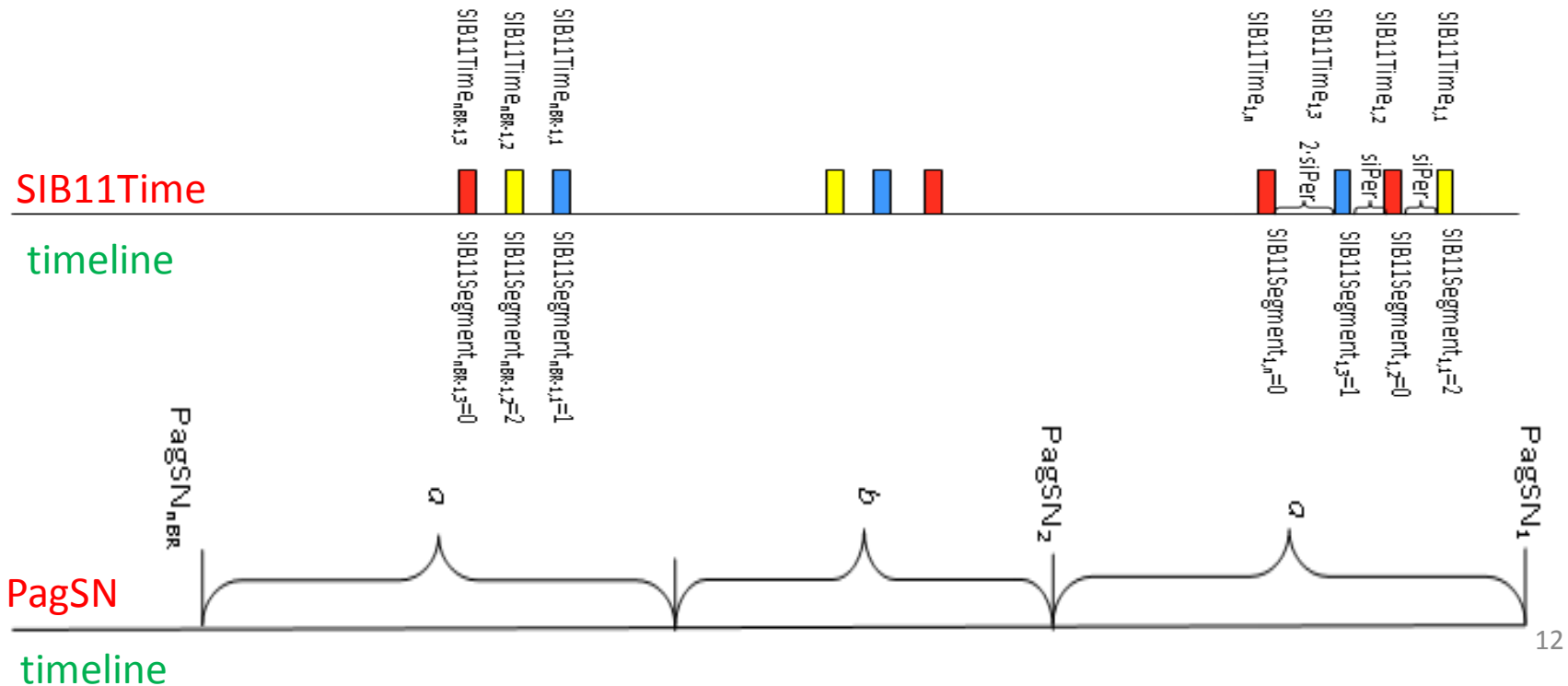PagSN is array of timestamps of paging messages of secondary notification
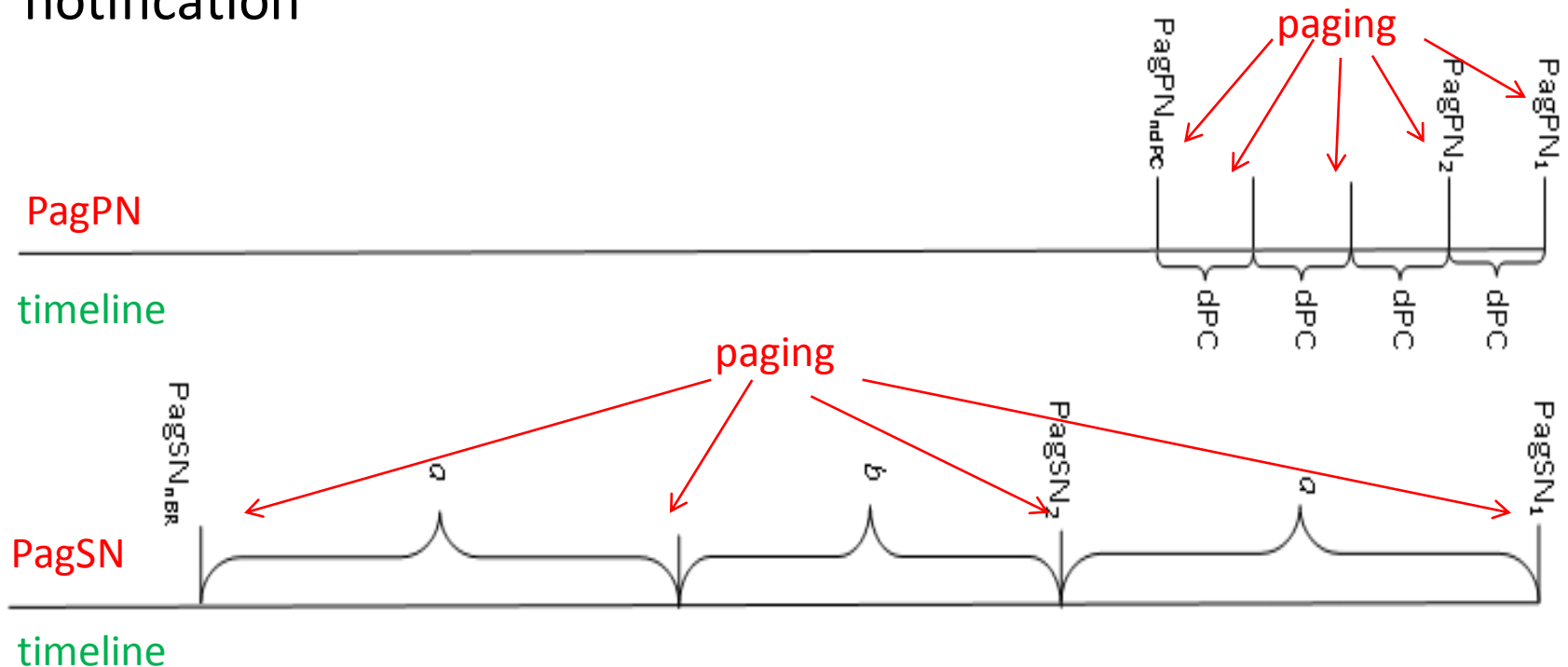
SIB1

- SIB1PNtime is array of timestamps of SIB1 messages after paging messages of primary notification
- SIB1PNtype is array of values from 0 to 3 that indicates whether SIB1 contain schedulingInfoList for SIB10 and/or SIB11

SIB11

- SIB11Time is array of timestamps of SIB11 messages
- SIB11Segment is a array of segment numbers

Protocol log analysis

- Our approach is to implement test harness using constraint solver

- Arrays contain correct timestamps of paging messages

- Arrays contain timestamps and content of messages from the log. First timestamp can be a variable.

- Two stages
  - Check correctness of paging messages
  - Check correctness of SIB1, SIB10 and SIB11 messages

- Boolean parameters indicate errors in logs

- Minimize sum of Boolean parameters

Minizinc

- Constraint specification language
- Solver independent
- Separation data from model
- Model consists of variable declarations and constraint definitions
- Scalar types (Booleans, integers, floats) and compound types (sets, arrays)
- Comparisons, arithmetic operations(+,·,sum), logical operations (\/,/\, forall, exists), set operations, array operations

Model in Minizinc

Boolean variables $SIB11afterpagind$ and $SIB11periodicityind$

SIB11 message after last paging message of secondary notification

- $(\exists\ 1 \leq i \leq numberSIB11log)$
$$\left(SIB11TimeLog_i > PagSN_{numberofbroadcasts}\right)$$
$$\leftrightarrow SIB11afterpagind = 1$$

Periodicity of SIB11 messages

- $(\forall\ 2 \leq i \leq numberSIB11\text{log})$
$$(((SIB11Timelog_i - SIB11Timelog_{i-1})$$
$$mod\ siPerSIB11 = 0)$$
$$\leftrightarrow SIB11periodicityind_i = 0)$$

Ongoing work

- Modelling in Minizinc acquiring by UE primary and secondary notifications sending by eNB after receiving several warning messages from MME

Message 1 SIB10,SIB11		Message 3 SIB11		Message 5 SIB10, SIB11
delay	Message 2 SIB10		Message 4 SIB11	

SIB10	SIB10			SIB10
SIB11		SIB11	SIB11	SIB11