RP-050158

INTRODUCTION OF CAUTION++ ARCHITECTURE FOR UTRAN EVOLUTION

Ilkka Talvitie

IST CAUTION++ Consortium

3GPP A GLOBAL INITIATIVE

3GPP RAN WGs on Long Term Evolution meeting

Tokyo, Japan. March 7th-8th, 2005

Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Summary of CAUTION++ project

- Project IST 2001-38229
  - CAUTION++ is an EC-funded R&D project
- Nov 2002 – May 2005
- CAUTION++ consortium:

Summary of CAUTION++ project

- Project objectives:
  - Optimization of wireless systems
  - Efficient use of RANs according to the type of service
  - Location-assisted Radio Resource Management
  - Consider business models for low-cost communication
  - Increased QoS in wireless systems
  - Enable seamless vertical handovers between different network segments
  - Demonstrate the platform in real networking environments

Contents

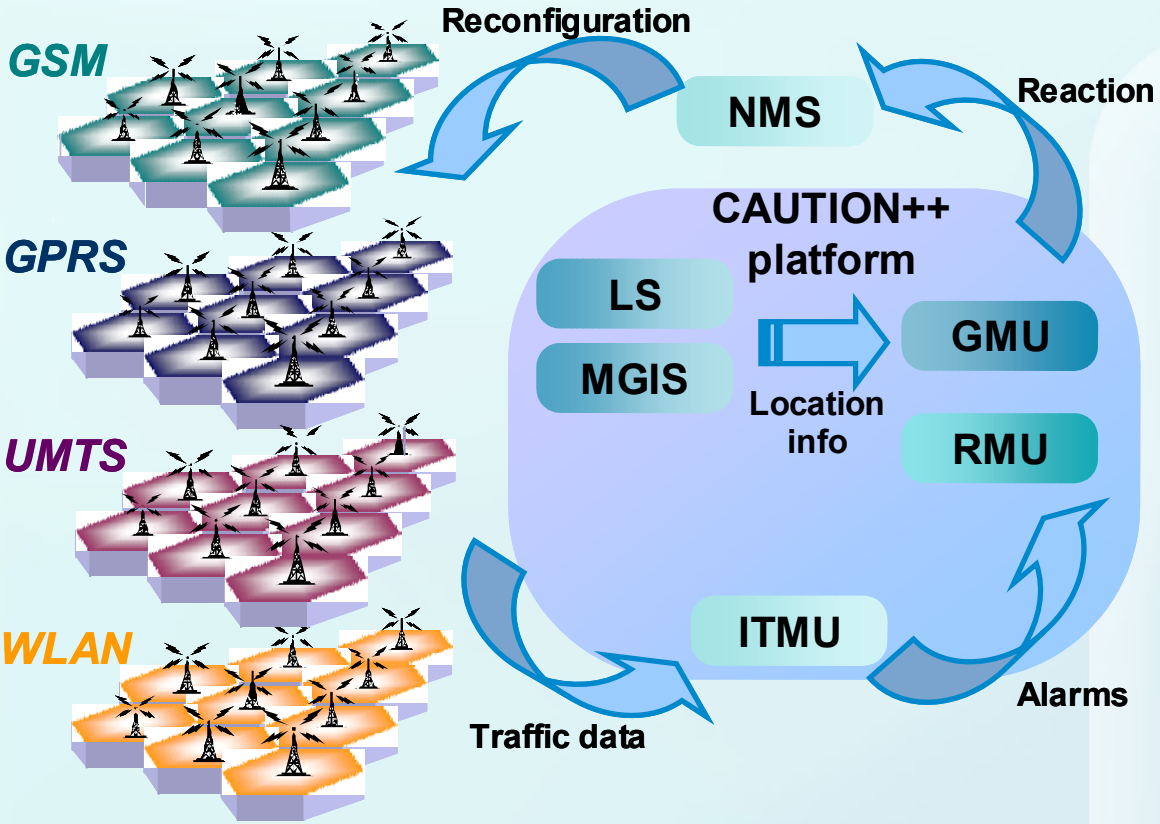
- Summary of CAUTION++ project
- **Overview of CAUTION++ architecture**
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Overview of CAUTION++ architecture

- CAUTION++ platform functionalities:
  - Network monitoring: GSM,GPRS,UMTS,WLAN
  - Detect congestion situations
  - Apply Resource Management Techniques locally to each network
  - Ensure stable transition from the congested state to the normal state.
  - Apply techniques for inter-network resource management when the congestion cannot be effectively handled locally inside a network

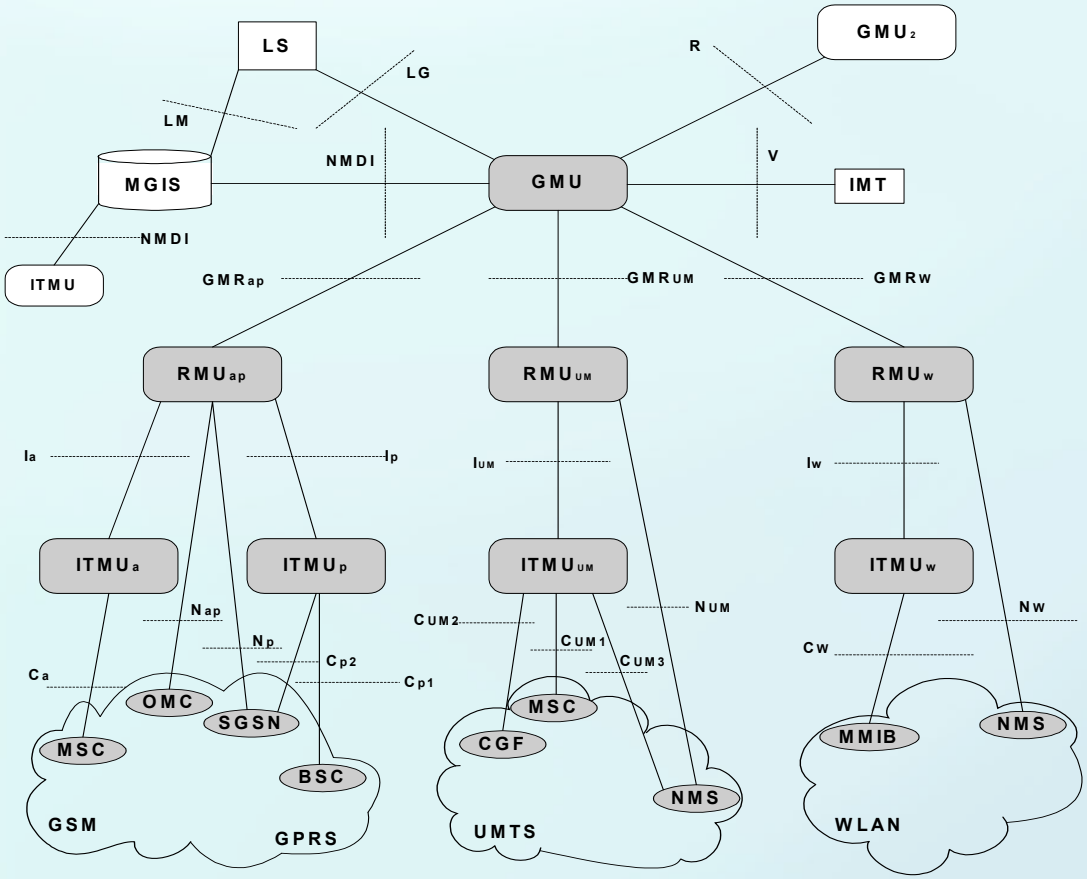
Overview of CAUTION++ architecture

- Scheme of CAUTION++ performance:



Overview of CAUTION++ architecture

- CAUTION++ architecture



Overview of CAUTION++ architecture

- Interface Traffic Monitoring Unit (ITMU)
  - Network Monitoring: KPI collection
  - Congestion detection: alarms
- Resource Management Unit (RMU)
  - Traffic Load Scenario recognition
  - Case-Based Reasoning: Selection of RMTs
  - Monitoring and fine-tuning
  - Scalation
- Global Management Unit (GMU)
  - Inter-RAN resource management
  - Vertical and vertical-vertical handover

Overview of CAUTION++ architecture

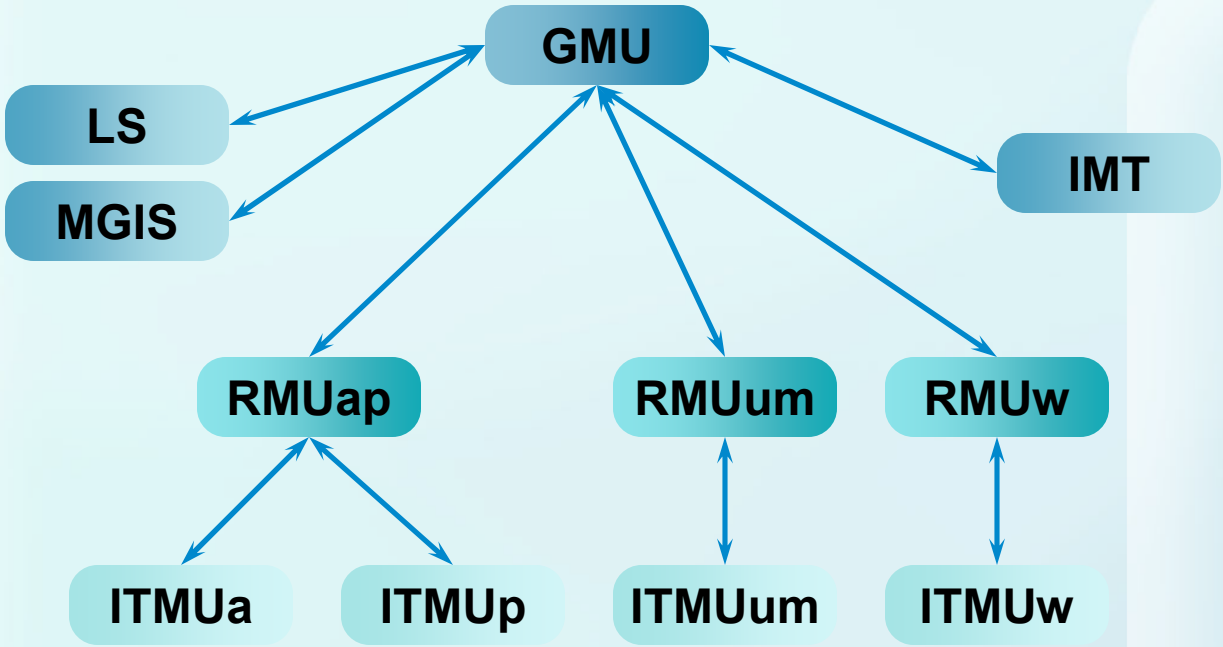
- Location Server (LS)
  - Supports RMU and GMU
  - Provides users' location
    - DCM, Cell ID & Signal Strength techniques
- Mobile network Geographical Information System (MGIS)
  - Network information database
  - Interfaces with ITMU, GMU and LS
- Interactive Mobile Terminal (IMT)
  - CAUTION++ enabled devices
    - Normal User: check availability & costs
    - Super User: network status for maintenance

Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- **CAUTION++ components**
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

CAUTION++ components

- Main components of the platform:



Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - **ITMU**
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Components: ITMU

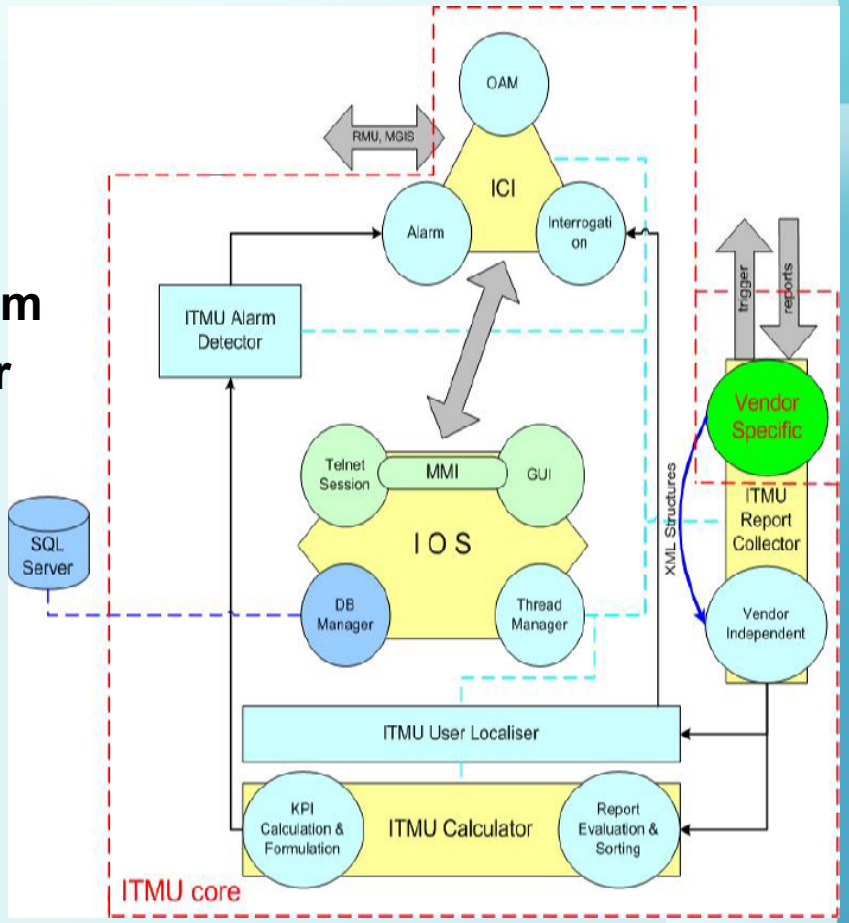
- Four different instances:
  - ITMUa (GSM), ITMUp (GPRS)
  - ITMUum (UMTS), ITMUw (WLAN)
- ITMU functionality:
  - Collection of RTT reports from network
  - Calculation of KPIs
  - Check thresholds
  - Sending alarm to RMU
  - Further conversation with RMU
    - Users' location
    - Neighbourhood traffic data

Components: ITMU

- ITMU core architecture:

- Common
  - Interfaces
  - Operative system
  - Report collector
  - Alarm detector

- Network-Specific
  - Calculator
  - User localiser



Contents

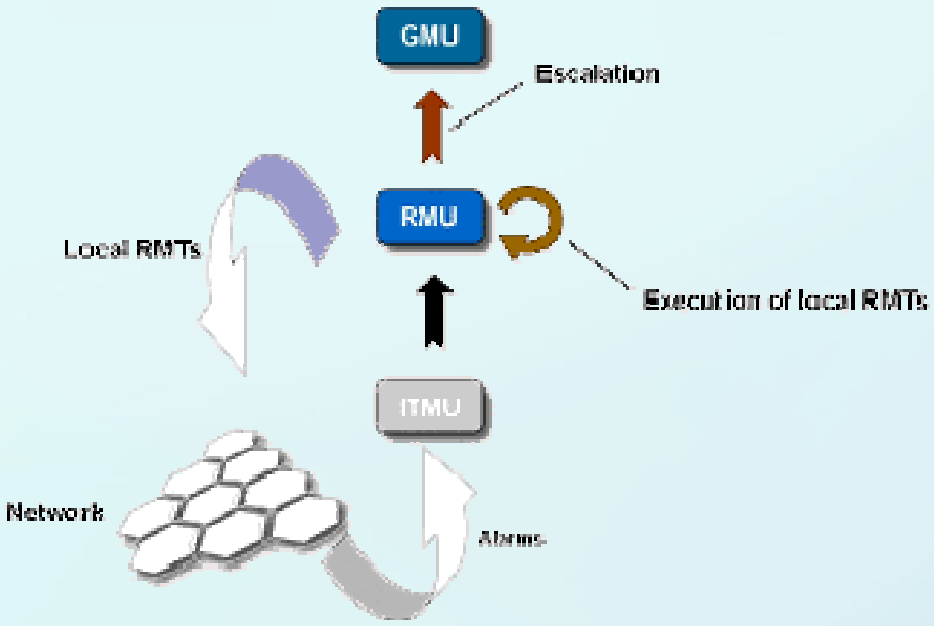
- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - **RMU**
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Components: RMU

- Three different instances:
  - RMUap (GSM and GPRS)
  - RMUum (UMTS), RMUw (WLAN)
- RMU functionality:
  - Alarm reception from ITMU
  - Traffic data gathering
  - Identification of Traffic Load Scenario (TLS)
  - Escalation to GMU
  - Selection of RMT strategy
    - Use of bussiness models
    - Case-based reasoning
  - Send command to NMS
  - Monitor state until alarm is relaxed

Components: RMU

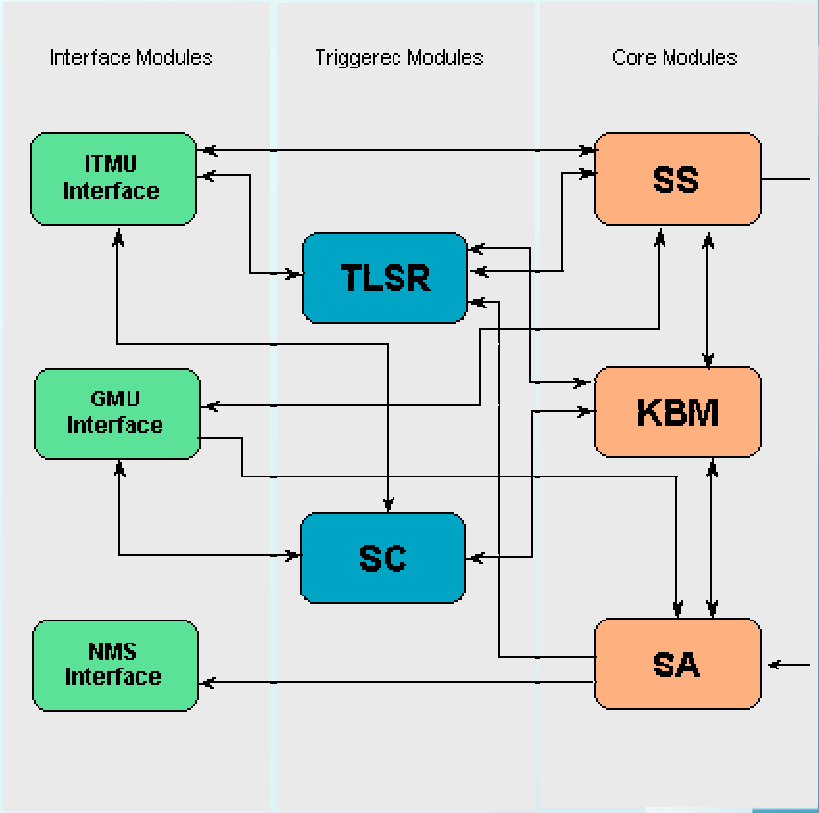
- **RMU functionality:**



Components: RMU

- RMU core architecture:

- Interfaces
- TLS Recogniser
- Status Collector
- Strategy Selector
- Knowledge Base Manager
- Strategy Actuator



Contents

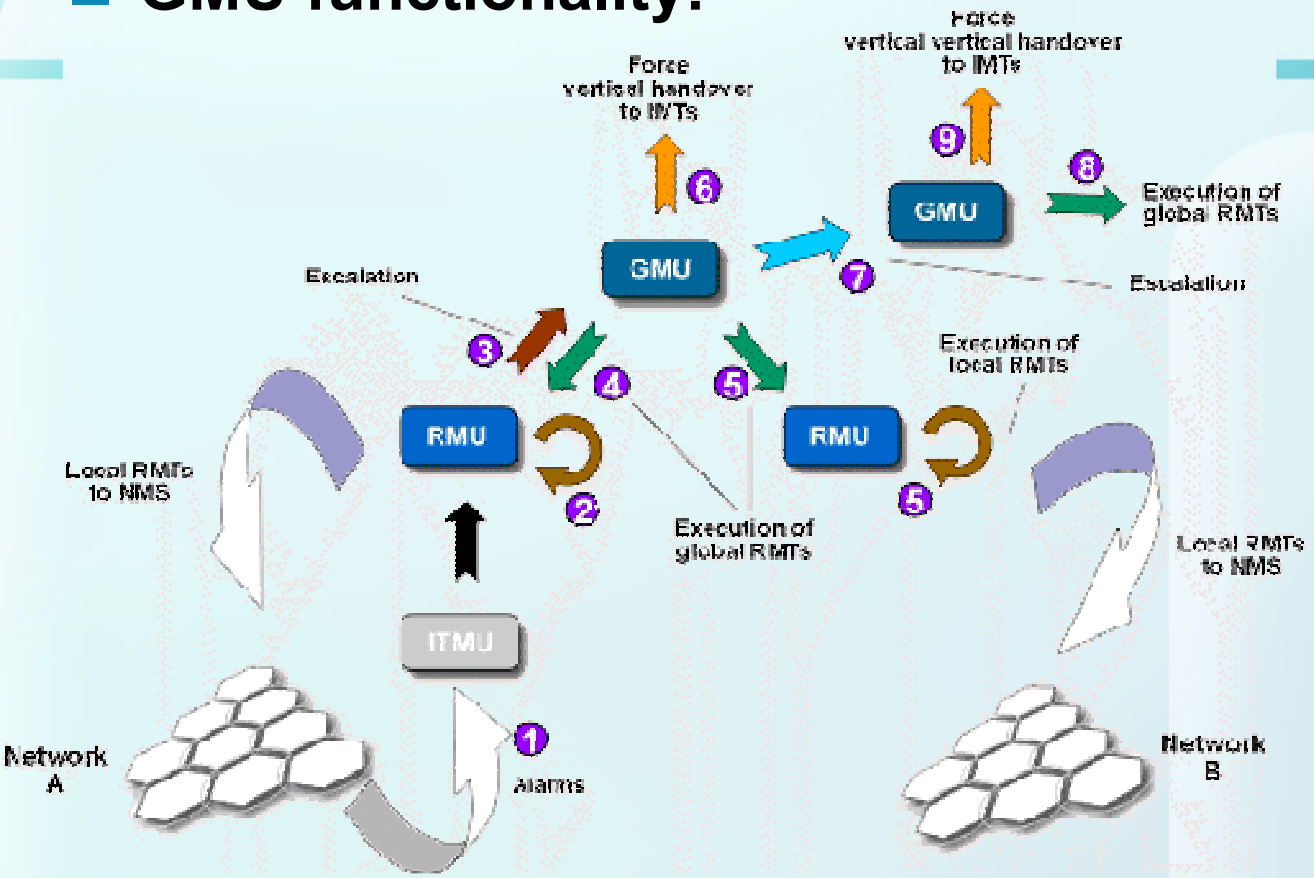
- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - **GMU**
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Components: GMU

- Only one instance by operator
- GMU functionality:
  - Assistance request from RMU
    - Strategy selection
    - Check RMUs availability
    - Escalate traffic to other GMUs
    - Force handovers
  - Assistance request from other GMU
    - Query RMUs to accommodate traffic
    - Negociation with origin GMU
  - Query from IMT
    - Use of LS, MGIS and RMUs info

Components: GMU

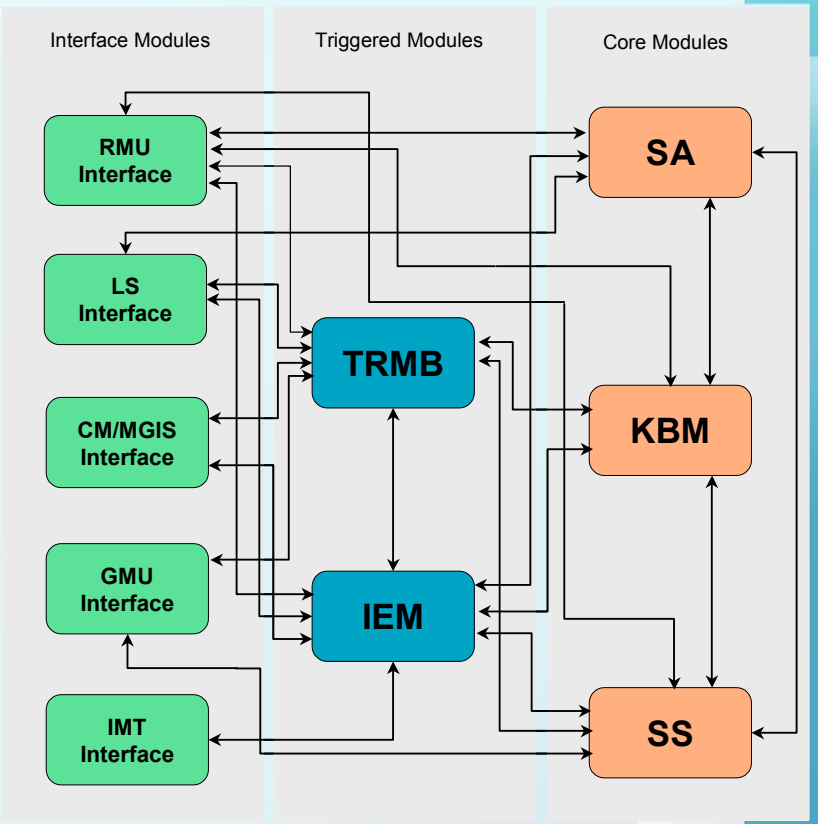
- GMU functionality:



Components: GMU

- GMU core architecture:

- Interfaces
- Traffic Resource Map Builder
- Information Exchange Module
- Strategy Selector
- Knowledge Base Manager
- Strategy Actuator



Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - **LS**
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Components: LS

- Provides users' location information
- LS functionality:
  - Receives requests from GMU
    - RMU and IMT requests via GMU
  - Evaluates user location & accuracy
    - Three techniques available:
      - Cell or AP ID
      - Signal Strenght
      - Database Correlation Method

Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - **MGIS**
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Components: MGIS

- Stores network information
  - Deployment data
  - Network status
  - Coverage measurements
- MGIS functionality:
  - Queries from LS
    - DCM algorithm assistance
  - Queries from ITMU
    - Resource management assistance
  - Queries from GMU
    - Mobility management assistance
  - Network status retrieval
    - Real time data from ITMU

Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - **IMT**
- CAUTION++ interfaces
  - External interfaces
  - Internal interfaces

Components: IMT

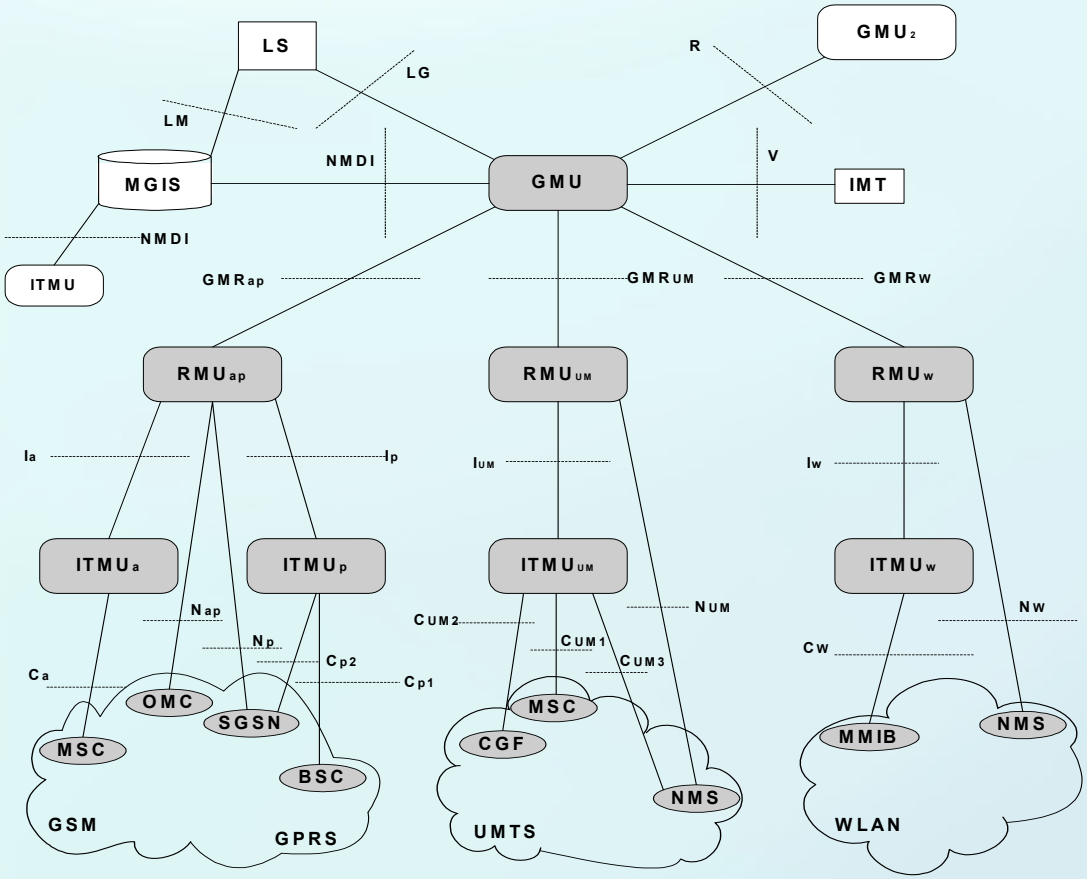
- CAUTION++ enabled devices
- IMT functionality:
  - Normal Users requests:
    - Available networks & services
    - Available UL & DL data rates
    - Pricing info
  - Super Users requests :
    - Available networks & structure
    - Coverage & dominance areas
    - Available cells in location
    - Overlapping cells & blacksopt areas
    - User location & users in cell
    - Network & cell status
    - Command to apply RMT

Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- **CAUTION++ interfaces**
  - External interfaces
  - Internal interfaces

CAUTION++ interfaces

CAUTION++ interfaces

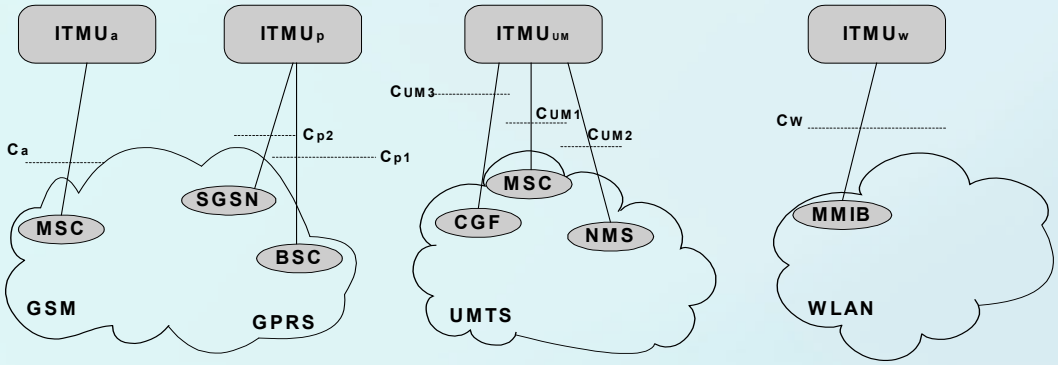


Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - **External interfaces**
  - Internal interfaces

External interfaces

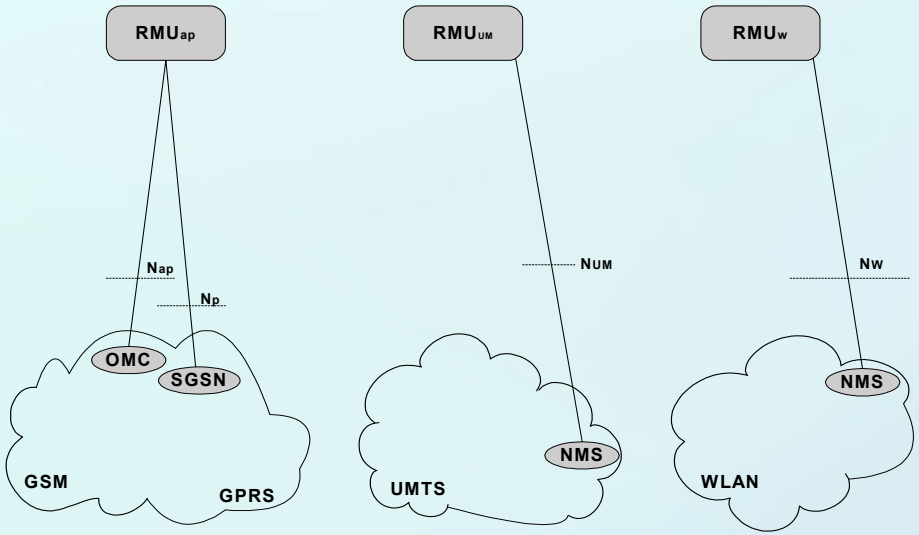
- **Towards networks' RANs:**
  - **Ca:** between ITMUa and MSC
  - **Cp1:** between ITMUp and BSC
  - **Cp2:** between ITMUp and SGSN
  - **Cum1:** between ITMUum and MSC
  - **Cum2:** between ITMUum and CGF
  - **Cum3:** between ITMUum and OMC/NMS
  - **Cw:** between ITMUw and MMIB



CAUTION++

External interfaces

- **Towards networks' NMSs:**
  - **Nap:** between RMUap and OMC
  - **Np:** between RMUap and SGSN
  - **Num:** between RMUum and NMS
  - **Nw:** between RMUw and NMS

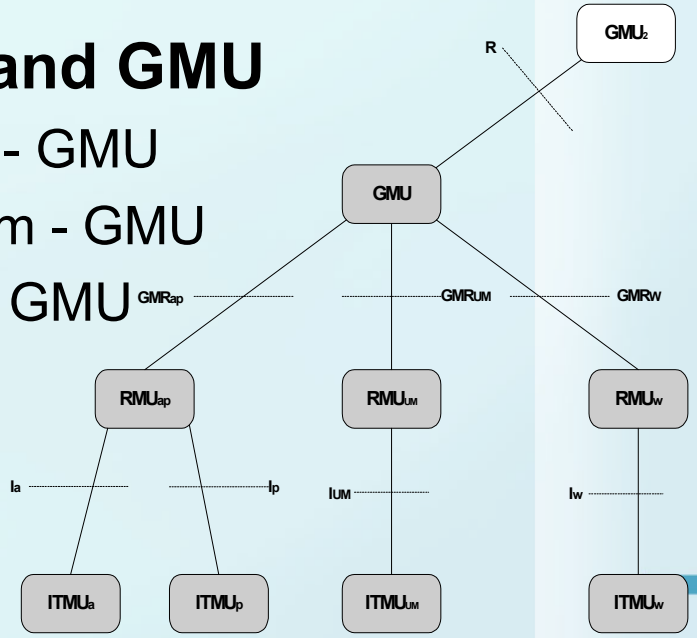


Contents

- Summary of CAUTION++ project
- Overview of CAUTION++ architecture
- CAUTION++ components
  - ITMU
  - RMU
  - GMU
  - LS
  - MGIS
  - IMT
- CAUTION++ interfaces
  - External interfaces
  - **Internal interfaces**

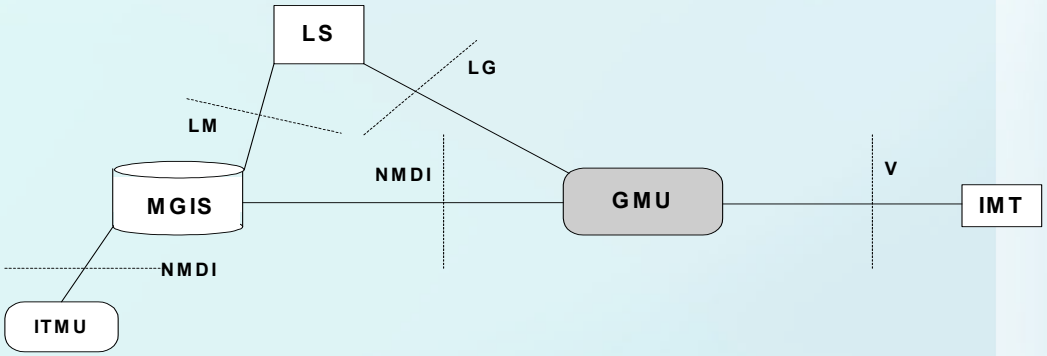
Internal interfaces

- **Between ITMUs and RMUs**
  - **Ia:** ITMUa - RMUap
  - **Ip:** ITMUp - RMUap
  - **Ium:** ITMUum - RMUum
  - **Iw:** ITMUw - RMUw
- **Between RMUs and GMU**
  - **GMRap:** RMUap - GMU
  - **GMRum :** RMUum - GMU
  - **GMRw :** RMUw - GMU
- **Between GMUs**
  - **R:** GMU - GMU



Internal interfaces

- **V:** between GMU and IMT
- **LG:** between GMU and LS
- **LM:** between LS and MGIS
- **NMDI:** between MGIS and ITMU/GMU



Project Number :	**IST-2001-38229**
Project Title :	**Capacity and network management platform for increased utilization of wireless systems of next generation++**

Proposal of standardization of CAUTION++ architecture

Editor :	**Óscar Moreno Jiménez**
Document Name:	**Proposal of standardization of CAUTION++ architecture**
File Name:	**WP6-TEL-I61-Int-005.doc**
Version :	**2.0**
Organization :	**Telefonica I+D**
Date :	**March 1st, 2005**
Distribution :	
Dissemination:	**CO**

The CAUTION++ Consortium consists of:

Participant name	Short name	Country
Institute of Communication and Computer Systems / National Technical University of Athens	ICCS/NTUA	Greece
Technical Research Centre of Finland / Information Technology	VTT	Finland
COSMOTE Mobile Telecommunications S.A.	COSMOTE	Greece
MOTOROLA GSGIT	MOTOROLA GSGIT	Italy
TELEFONICA	TELEFONICA I&D	Spain
ELISA Communications	ELISA	Finland
Istituto di Scienza e Tecnologie dell'Informazione	ISTI	Italy
ERICSSON HELLAS	ERICSSON	Greece
MOTOROLA UK	MOTOROLA UK	United Kingdom
Universitat Politecnica de Catalunya	UPC	Spain

DOCUMENT HISTORY

Date	Version	Status	Comments
04/02/05	1.0	Int	First draft
01/03/05	2.0	Int	Consolidated draft

Table of Contents

List of Figures

List of Tables

TERMS AND ACRONYMS

AP	Access Point
BSC	Base Station Controller
BTS	Base Transceiver System
CGF	Charging Gateway Function
DCM	Database Correlation Method
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IMT	Interactive Mobile Terminal
IP	Internet Protocol
ITMU	Interface Traffic Monitoring Unit
KPI	Key Performance Indicator
LAN	Local Area Network
LS	Location Server
MGIS	Mobile Network Geographic Information System
MMIB	Monitoring Management Information Base
MSC	Mobile Switching Centre
NIC	Network Interface Card
NMS	Network Management System
OMC	Operations and Maintenance Centre
RAN	Radio Access Network
RAT	Radio Access Technology
RMT	Resource Management Technique
RMU	Resource Management Unit
RNC	Radio Network Controller
RTT	Real Time Traffic
SGSN	Serving GPRS Support Node
TCP	Transmission Control Protocol
TLS	Traffic Load Scenario
UMTS	Universal Mobile Telecommunication System
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1 INTRODUCTION

1.1 OBJECTIVES OF THIS DOCUMENT

The goal of this document is to provide a complete description of the architecture of the Resource Management solution envisaged in CAUTION++ project. This description aims to become a firm proposal to get this architecture standardized.

To this end, this document is structured in three sections: the first of them depicts an overview of the proposed system; the second one describes in detail the functionalities of every submodule; and the third one details the interfaces between these submodules.

1.2 SUMMARY OF CAUTION++ PROJECT

CAUTION++ project (Capacity and network management platform for increased utilization of wireless systems of next generation++) is comprised in the 5th Framework Program (IST 2001-38229).

CAUTION++ project began on November 2002 and will end its activities on May 2005. There are ten partners involved:

- NTUA (Greece)
- VTT (Finland)
- COSMOTE (Greece)
- MOTOROLA GSGIT (Italy)
- TELEFONICA I&D (Spain)
- ELISA (Finland)
- ISTI/CNR (Italy)
- ERICSSON (Greece)
- MOTOROLA UK (United Kingdom)
- UPC (Spain)

The main objective of the project is the smooth transition from existing wireless systems to new generation ones. CAUTION++ will exploit knowledge and system platform developed under the framework of CAUTION project and extend this to UMTS and systems beyond.

The main goal of this project is to design and develop a novel, low cost, flexible, highly efficient and scaleable system able to monitor the available resources from a set of wireless access networks, namely GSM, GPRS, UMTS and WLAN, so that they will be able to serve the end user complementary to each other, sharing resources from multiple operators. CAUTION++ platform should be able to monitor all the above access networks, detect any problematic situations where the QoS could be in risk, or eventually reduced, arise alarms and forward them to the upper management levels of the system in order to deal efficiently with the situation and thus ensure the gratification of the end user which is of first priority. In this way each operator would reduce to the minimum the loss of revenues due to traffic conditions and from another point of view could offer to its subscribers new services exploiting the capabilities of his entire network.

1.3 OVERVIEW OF CAUTION++ ARCHITECTURE

1.3.1 Introduction

The context in which CAUTION++ platform will operate is a diversified radio environment in which GSM, GPRS, UMTS and WLAN access technologies coexist and overlap coverage areas. Additionally, multiple network operators may also play a role in this heterogeneous network arena, each of them managing on his own a subset of the mentioned RANs. Subsequently, the objectives of the CAUTION++ project are that of designing and developing a prototype of an enhanced network management system able to:

- Monitor each network (GSM, GPRS, UMTS and WLAN) separately.
- Detect congestion situations that may occur in those networks.
- Apply techniques locally to each network to tune resource management for alleviating or eliminating the effects of overloads.
- Ensure stable transition from the congested state to the normal state.
- Apply techniques for inter-network resource management when the congestion cannot be effectively handled locally inside a network. This includes also roaming between different access networks (GSM, GPRS, UMTS and WLAN), owned by the same network operator, or by different network operators.

1.3.2 System architecture

The system architecture that has been devised to meet the objectives stated above is the one shown in Figure 1.

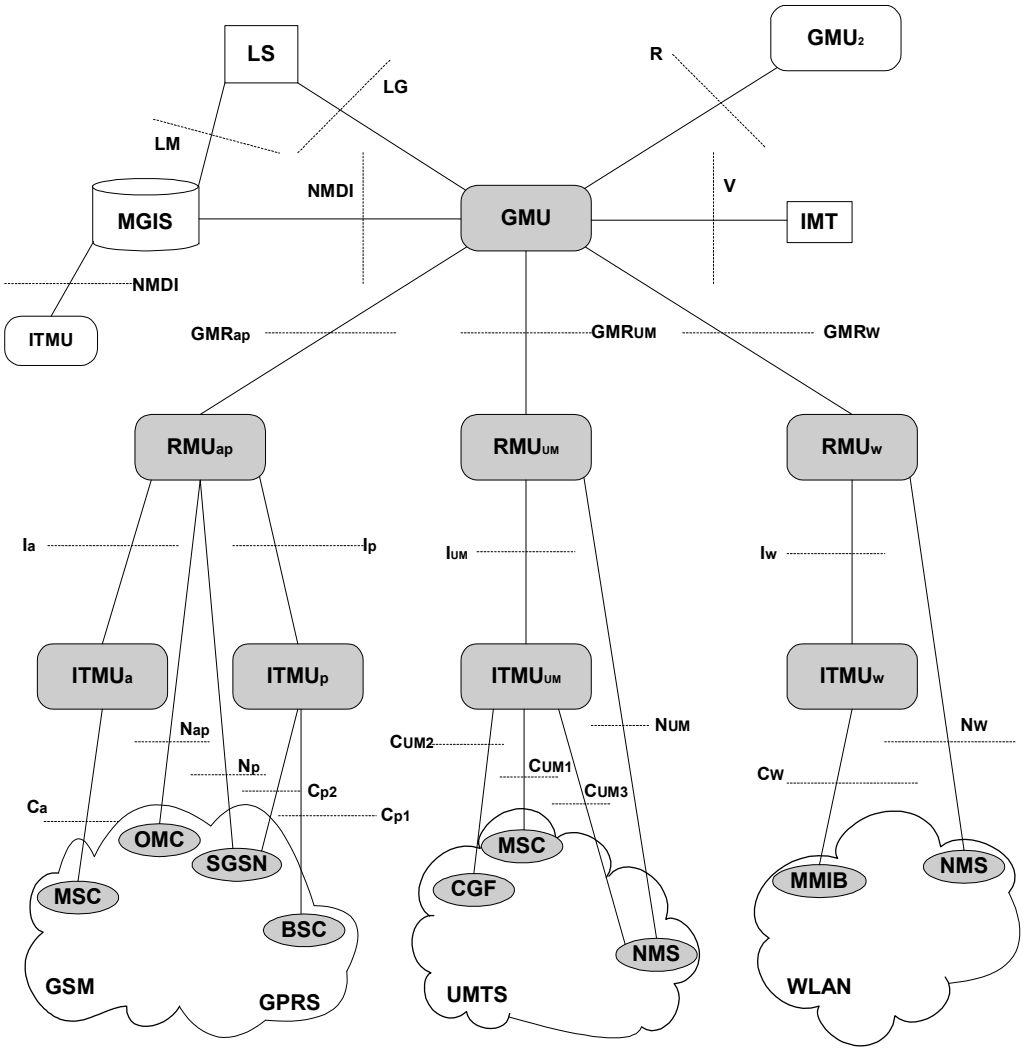


Figure 1. CAUTION++ System Architecture

The first element of the architecture is a real–time network monitoring unit, whose purpose is to monitorise network resource utilization to detect congestion situations. This unit, called Interface Traffic Monitoring Unit (ITMU), is the collector of a set Key Performance Indicators (KPIs), which are used to describe traffic congestion. Each type of RAN of the heterogeneous wireless network environment has its own dedicated ITMUs. The number of ITMUs to be deployed is determined by the number of cells to be monitored. Each ITMU continuously computes the values of the KPIs for each monitored cell by means of the received information from other network nodes (such as MSC, SGSN, BSC or MMIB, depending on the particular RAN).

The output of the real-time monitoring unit is forwarded to a higher-level component, called Resource Management Unit (RMU). RMU is the element in charge of performing the first level of resource management. The information offered by ITMU to RMU provides the values of the calculated KPIs for each congested cell.

RMU processes this information to match it with one in a set of pre-defined Traffic Load Scenarios (TLS), each of them describing a different congestion situation. Then, an appropriate management technique is selected and applied according to the identified TLS. After a reaction has been applied, the RMU and ITMU coordinate with each other to ensure a smooth transition from the congested to the normal state, with on-the-fly adjustments of the technique's parameters. A single RMU may perform resource management for several ITMUs.

Moving upwards in Figure 1, the highest level of resource management in CAUTION++ is implemented by the component called Global Management Unit (GMU), which stands as a centralized component connected with the RMU of each network. In case an RMU cannot satisfactorily manage the congestion detected by its ITMU, it may escalate a support request towards the GMU component. Each GMU watches the resources of a single network operator and enables an inter-RAN resource management through vertical handover between different access networks, e.g. GPRS with WLAN. The support of a Location Server (LS) and of an Mobile network Geographic Monitoring System (MGIS) is available to the GMU to help in the identifications of those networks that are target candidate for the movement of users asking resources in congested areas.

Finally, the Interactive Mobile Terminal (IMT) represents an enabling application for subscribers to access the information available in the CAUTION++ system. Through the interface IMT-GMU, subscribers will be allowed requesting information about the more convenient radio access technology available for the specific service they intend to require to the heterogeneous network. Moreover, the GMU may initiate a communication with the IMT for the execution of vertical and vertical-vertical handovers.

1.3.3 System components

CAUTION++ system is composed by five components connected by means of dedicated wired lines or IP backbone network, as illustrated in Figure 1. The elements are the following ones:

- **ITMU** (several of them in each network. Also, ITMUs of different networks are different)
- **RMU** (total three: one for GSM/GPRS, one for UMTS and one for WLAN)
- **GMU** (one for all access networks)
- **LS/MGIS** (one for all access networks)
- **IMT** (one for each CAUTION++ enabled user)

The number of submodules mentioned above refers to a single network operator. Two different operators can get connected through their own GMUs by means of V interface, as can be seen in Figure 1 and described in section 3.2.4.1.

1.3.3.1 Interface Traffic Monitoring Unit (ITMU) overview

One of the most important topics, in terms of the network consideration, is network monitoring. Generally, monitoring enables the obtaining of useful data about a system, with respect to its state and behaviour. More specifically, network monitoring enables the provision of useful information on resources utilization, blocking rate, response time and interaction between various network units.

The key considerations for a mobile radio network are its resources, the kind and the capacity of channels, the number of cells, the number of network elements (BSCs, MSCs, SGSNs, routers, RNCs) that the network has, etc. Other critical factors throughout monitoring are whether a call request or a packet switched service was established successfully or not, if a call was ended successfully or not, and if network resources are sufficient at emergency instances. In the case of an unsuccessful clearance of a connection, the reasoning and the cause of that problem have to be distinguished and the corresponding solutions to be proposed. This is the main motivation behind the development of a special tool, which will be capable of monitoring the mobile network adequately. This tool in CAUTION++ project is named ITMU sub-network and it is a distributed element comprised of 4 different kinds of ITMUs, each of them specialized in one of the target networks. Thus the following ITMU units constitute the ITMU sub-network:

- **$ITMU_A$** for GSM
- **$ITMU_P$** for GPRS
- **$ITMU_{UM}$** for UMTS
- **$ITMU_W$** for WLAN

The main task of ITMU sub-network is to monitor the network and report congestion situations to RMU sub-network, so that the RMU can identify the traffic load scenario and obtain a high level visualization about the mobile network congestion. Each of the traffic load scenarios will be characterized by a set of parameters (Key Performance Indicators, KPIs), concerning logical channels utilization and congestion characteristics. These parameters are sent to RMUs from the corresponding ITMU. Also, RMUs send queries to the corresponding ITMU about specific KPIs. Finally, ITMU sub-network exchanges data with the MGIS element. The ITMU sub-network performs a real-time monitoring on the network, by collecting information. It receives, from the "report generating elements" of each network type, several different data – reports that are appropriately processed to generate the network congestion parameters (KPIs) of interest in CAUTION++.

The ITMU will extract the information (KPIs) from different nodes, depending on the access network. For example, from GSM using the A standard interface between MSC and ITMU; in the case of GPRS the ITMU will collect the information through the SGSN; in WLAN the information will be extracted from routers. As a common task for all access networks, the ITMU will create a table for all the BTS or Access Points (AP) that is hosting. Internal matrices will be stored, so data will be processed, providing information and alarm messages towards the RMU.

1.3.3.2 Resource Management Unit (RMU) overview

The Resource Management Unit (RMU) is the component of the CAUTION++ system that selects and executes resource management techniques, after a detection of congestion within a specific network type (GSM, GPRS, UMTS, and WLAN) has taken place.

The RMU receives the alarms generated by the ITMU and reacts accordingly to the congestion situations originated in the home network. The RMU is the core resource management element for each network locally. When congestion is being detected, the RMU performs the following procedure:

- Aggregation of the received KPIs so that they will be mapped onto a pre-defined set of Traffic Load Scenarios. The identification of the TLS is the first step in the application of the knowledge base that the RMU manages to drive its decision-making processes.
- Once the TLS has been recognized, the RMU will interact with the ITMU to define the size of the congested area. The output of this activity is a cluster of cells for which the decision making process will have to take a single decision about which management techniques are to be applied.
- When the cluster defining the congestion situation and its surrounding context are available, the RMU launches a Business Model to decide which part of the congestion is to be handled locally, and which part (if any) is to be escalated to the upper level of resource management (GMU). If a part of the congestion is to be moved upwards to the GMU, this communication is managed concurrently with the local treatment. This is likely to result in GMU decision to perform some handover of users form the RMU controlled network to another network. In this case, the RMU will have to actuate some techniques as per request of the GMU.
- To decide which resource management techniques are to be applied for the part of the congestion that the RMU decided to handle locally, a Case-Based Reasoning approach is adopted, which searches an Historical Knowledge Base of successfully treated congestion events, and finds the most similar one. The RMU applies to the current congestion event the resource management techniques that were applied to solve the selected case.
- After application of the resource management techniques, the RMU will enter a monitoring state, within which it will keep the treated area under surveillance, by checking the relevant KPIs that the ITMU sends to the RMU. If significant deviations are expected from the expected KPI behaviour, the RMU will retune its reaction, or it will apply additional management techniques.

- When all the KPIs are back into the nominal values, the RMU stops its congestion treatment actions, by restoring the initial network configuration. Some threshold values and adequate timeouts are used to avoid ping-pong phenomena between congested and non-congested situations. In case the RMU had escalated the congestion to the GMU, then the termination of a congestion situation is also notified to the GMU. Successfully treated events are stored into the Knowledge Base for future reuse.
- In case the monitoring reveals the treatment to be unsuccessful and the congestion persists, the RMU will escalate the congestion to the GMU.

It is worth outlining that while the interface between ITMU and RMU can be specified in a way that it is not dependent from the specific RAN the RMU is deployed, the interfaces between RMU and the network for the actuation of the decided reaction does depend on the specific technology. For GSM the RMU will have to directly send commands to the OMC, whereas for GPRS the interface may include either SGSN or OMC, depending on the management technique selected. For UMTS, the interface ends up at NMS and SGSN (R99), while for WLAN it ends at the router.

1.3.3.3 Global Management Unit (GMU) overview

The Global Management Unit (GMU) is responsible of devising a higher-level global solution to congestion situations. The GMU operates as the top-level component in the resource provision as it is able to achieve a global view upon the entire operator's access networks. This global view is achieved due to the communications channels towards the associated RMUs, which report the status of resource availability to their GMU. Moreover, GMU is also able to communicate with LS and MGIS nodes to locate subscribers and to know, for each of them, which radio access networks can provide the required services.

The information available to GMU enables a combined management of the different associated radio access networks. This management initiation is triggered when the congestion cannot be satisfactorily handled by a single RMU. In this case, a support request is provided to GMU, which starts its operations to obtain a solution for the overload situation that uses all the radio resources available in the congestion affected area. To implement its decision, the GMU will require the associated RMUs to support the execution of some vertical-vertical handovers.

It is important to observe that both GMU and RMU, besides having a different view of the network status, have also different roles in the resource management in terms of the techniques they can employ. Indeed, the GMU is restricted only on the decision for the actuation of vertical and vertical-vertical handover techniques, whereas the RMU may apply a wider set of techniques to accommodate the traffic inside the boundaries of its controlled radio access network. This design choice allows each component to deal only for those scenarios on which the CAUTION++ component can gather the required resource management information, and also avoids different levels of resource management of the system to take contrasting choices.

1.3.3.4 Location Server (LS) overview

The Location Server (LS) is the component in CAUTION++ used to provide users' location information, in case that it is requested by another CAUTION++ component (typically by GMU, or RMU via GMU). After receiving a location request, the Location Server computes an estimate of the user location.

The server supports three techniques, namely

- Cell ID (or Access Point ID)
- Signal Strength
- Database Correlation Method (DCM)

The algorithms use the measurement information obtained as parameters of the location request and the network information obtained by queries from the MGIS database. The LS returns the computed location estimate and an estimate of the location accuracy (in meters) to the requester. In case of an error, if the location cannot be determined, an error report will be given. The obtained location information can be used in resource management or as a supporting factor in mobility management. Based on the knowledge of the user location or geographic distribution of the users in the network, the actions by RMU and GMU can be made more efficient.

1.3.3.5 Mobile network Geographic Information System (MGIS) overview

The Mobile network Geographic Information System (MGIS) database contains information about the network to be used by the CAUTION++ components (ITMU, GMU and LS). The information stored in MGIS may contain:

- Stable long term information from the network
- Data referring to a specific network state
- Measurement results or other system specific information from GPRS/GSM, UMTS or WLAN

The MGIS interfaces with LS, GMU and ITMU so it can answer to queries made by these components. The MGIS may also retrieve real-time information about the status of the networks (from the GMU or ITMU) or information about the user location (from the LS). The MGIS database is structured by tables, which are either system specific or common.

1.3.3.6 Interactive Mobile Terminal (IMT) overview

The CAUTION++ platform is designed to extract network information and control traffic for the access networks of GSM/GPRS, UMTS and WLAN. This information could be available for normal users, in order to improve their experience when trying to access to a network to obtain a certain service; and also for maintenance technician workers of the network operator, so as they can gather useful information about the network's status.

IMTs are devices designed to retrieve information from CAUTION++ system, and its capabilities are directly related with the kind of user:

- Normal users: they are simple users who desire to get a certain service, and so they request some information to GMU to decide which one of the available networks will be more suitable for such service, in terms of cost, data rates, etc.
- Super users: they are technicians in charge of the maintenance of the network who, in their periodic surveillance of the network status, retrieve information from the CAUTION++ nodes.

IMT software has been developed to run over PDA or laptop devices.

2 CAUTION++ COMPONENTS

2.1 ITMU

2.1.1 Introduction

Each ITMU is responsible to monitor one RAN type and to report to the corresponding RMU. So, each ITMU collects the various RTT (Real Time Traffic) reports from each network and calculates the appropriate KPIs for each network type. This knowledge is used to know the system situation at any time (problems, congestion, etc.). The RTT collection is performed through different network nodes in each network type (SGSN, MSC, BSC, Router, etc). RTTs will be collected from a vendor specific interface by means of a special sub-module, which is placed between the ITMU and the appropriate vendor specific interface.

After the report collection, ITMU performs the most critical tasks: report analysis and KPI calculation. The proper calculation of these KPIs is a very important and difficult task. ITMU must evaluate RTTs, extract all the useful information and calculate the KPIs using the best formula for each network type. All calculation formulae result from the pre-study of the operation of the RTTs in each network, and are programmed to avoid delays.

The last task to be performed by ITMU is to report to RMU the status of the network, through predefined alarm messages. Each KPI has a critical threshold, so if the calculated value overcomes it (thus meaning an overloaded resource), then ITMU sends the appropriate alarm message to RMU. The alarm contains information about this congested resource of the congested cell. So, RMU is provided with a snapshot of the overall congestion situation. The alarm is continuously sent (on a periodic basis) until the resource drops back to normal operation (non-congestion situation), and then the alarm is deactivated.

The communication between ITMU and RMU is a two-way communication. This is important in order to allow the exchange of additional information when required. RMU receives the alarm messages, which are submitted asynchronously from the ITMU, but it might not be able to detect the scenario, or perhaps it is recommended to have more information about network traffic, before taking the decision of executing some command. Therefore, RMU may request data regarding neighbour cells, in order to decide about the area that is affected from the traffic overload. In that case, ITMU sends a message to RMU containing information about the requested neighbour cell. The same applies to User Localization message: RMU queries ITMU about the users camped in a specific cell, and ITMU responds with the cell ID of the cell (or AP) in which each user is camped.

2.1.2 Functionality

According to the CAUTION++ architecture, there are 4 different ITMU instances: $ITMU_A$ for GSM network, $ITMU_P$ for GPRS network, $ITMU_{UM}$ for UMTS network and $ITMU_W$ for WLAN. It is obvious that each network (GSM, GPRS, UMTS and WLAN) has its own character and features; thus different KPIs exist for each network type, but also different monitoring and calculation procedures. So, the calculation requirements of each KPI in each network type are different. There are differences in the RTTs that should be monitored, in the data that must be extracted and exploited, and in the calculation procedures and formulae.

ITMU core structure is shown in Figure 2.

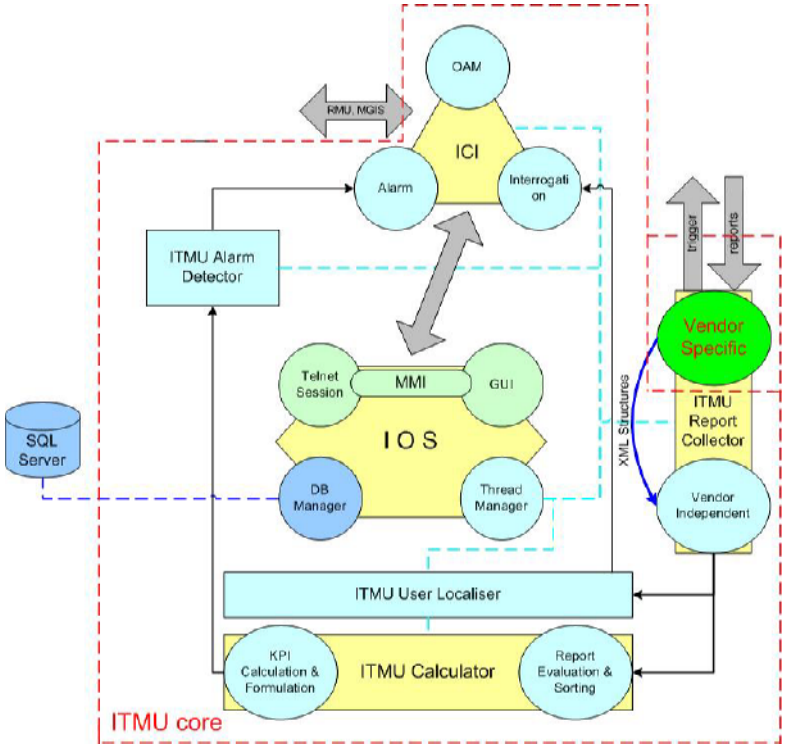


Figure 2. ITMU Core Structure

So, ITMU structure is divided in two main parts: the core structure (that is the same in all ITMU instances) and the specific structure (different for each ITMU instance). The core structure modules are composed by:

- ITMU CAUTION++ Interface
  - Alarm
  - Interrogation
  - Operation & Maintenance
- ITMU Report Collector
- ITMU Alarm Detector
- ITMU Operating System
  - Man – Machine Interface
    - Telnet Session Interface
    - Graphical User Interface
  - Database Manager
  - Thread Manager

The modules that are different for each ITMU instance are the following:

- ITMU Calculator
  - Report Evaluation & Sorting
  - KPI Calculation & Formulation
- ITMU User Localiser

The *ITMU Calculator* module is comprised of two sub-modules: the *Report Evaluation & Sorting* and the *KPI Calculation & Formulation*. The *Report Evaluation & Sorting* sub-module evaluates the received from *Report Collector* reports and analyses and sorts the data in a such way that *KPI Calculation & Formulation* sub-module can exploit them. The *KPI Calculation & Formulation* sub-module contains the KPI calculation algorithms: It calculates KPIs and then formulates the results.

2.1.3 Interfaces

From the cellular network side, ITMU sub-network is connected to the “report generating elements” through vendor-specific interfaces. Each interface is used as a gateway to collect and translate the reports that are delivered to the ITMU, to a standard recognizable format. Each ITMU must have multiple interfaces in order to collect all the necessary info.

From the CAUTION++ system side, ITMU sub-network is connected to RMU sub-network that is the core element of the CAUTION++ system, and to MGIS, concerning the whole CAUTION++ architecture.

On the 4 following figures the different ITMU interfaces are illustrated:

- **NMDI:** ITMUxx – MGIS interface
- **Ixx:** ITMUxx – RMUxx interface
- **Cxxn:** Vendor Specific Interface Element – Network Element interface

  xx: (*A* for GSM, *P* for GPRS, *UM* for UMTS, *W* for WLAN)

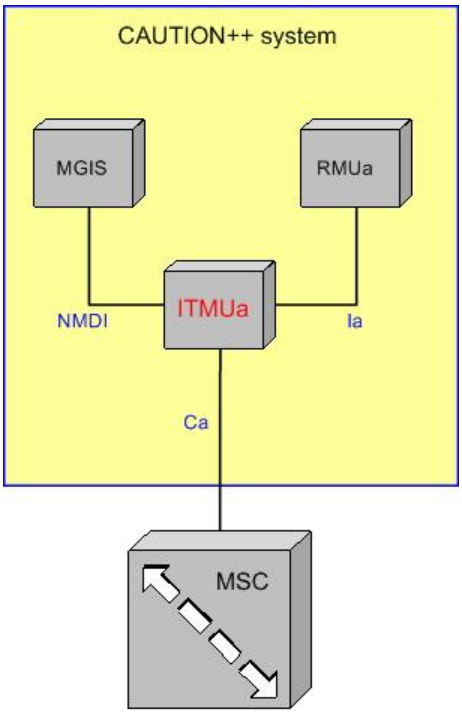


Figure 3. ITMU for GSM

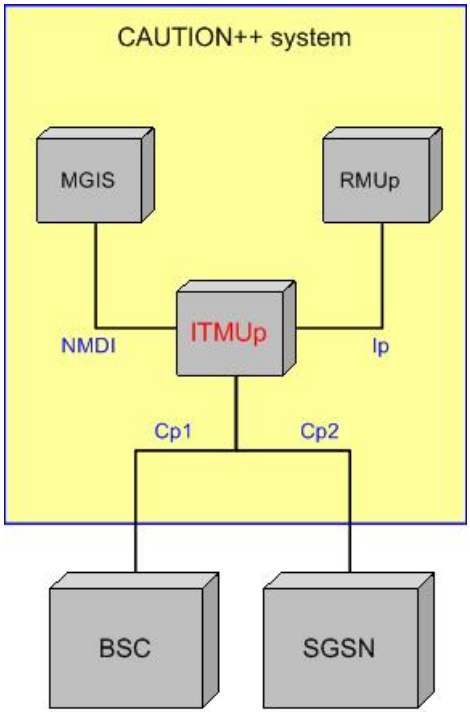


Figure 4. ITMU for GPRS

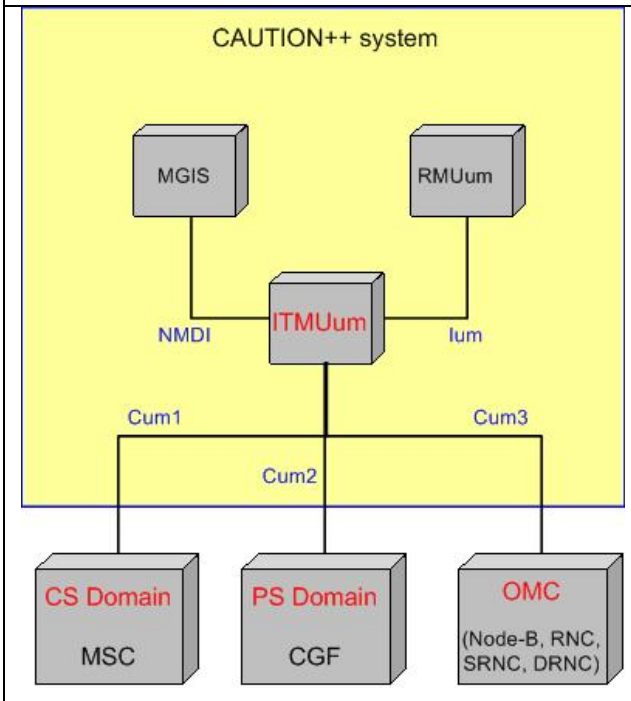


Figure 5. ITMU for UMTS

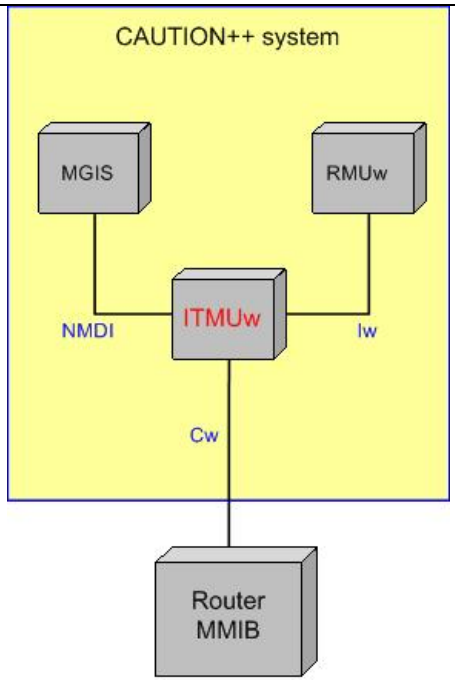


Figure 6. ITMU for WLAN

All the connections between ITMU and other elements are established over an Ethernet (802.3) Local or Wide Area Network (LAN or WAN), depending on the actual location of the elements. The TCP/IP protocol stack is used. In the application layer, the HTTP/1.1 protocol will be used, because it supports persistent connections. This allows issuing more than one request during the same TCP/IP session without having to establish a new connection for each request, thus greatly improving throughput if a large number of messages is sent. The messages exchanged are XML formatted. The protocol hierarchy is shown in the Figure 7.

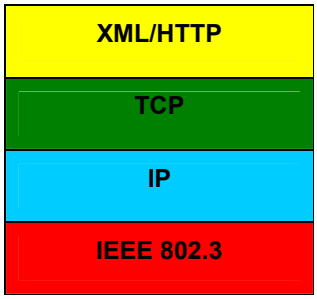


Figure 7. Protocol stack for ITMU communications

A more detailed description of the interfaces can be found in chapter 3.

2.2 RMU

2.2.1 Introduction

The resource Management Unit (RMU) is the component in charge of performing the decision making process that ultimately results in the triggering of the adequate congestion treatment techniques.

The submodules that compose RMU are the following:

- **Traffic Load Scenario Recognizer (TLSR):** is in charge of analysing the alarm messages coming from ITMU and, by inquiring the internal knowledge database, to identify the appropriate traffic load scenario. This module may require more information from the ITMU or from other ITMUs in order to increase the confidentiality about the identified traffic load scenario.
- **Strategy Selector (SS):** is responsible to perform the two steps of decision-making, i.e., first to apply a business model for deciding which part of the offered traffic is to be managed locally and which part is to be escalated to the GMU, and then to select the more appropriate Resource Management technique (RMT) and the suitable RMT parameters to handle the part of the traffic that is to be treated locally.
- **Strategy Actuator (SA):** is responsible for the execution of the resource management techniques selected in the previous stage. To this end, the SA receives from the SS module the information about the selected resource management techniques and translates this into appropriate commands that are transferred and executed at the NMS of the controlled radio access network.
- **Status Collector (SC):** is used for retrieving (through ITMU queries) and communicate to the GMU the information about the availability of resources in given areas of the controlled network.
- **Knowledge Base Manager (KBM):** it supports RMU in storing an retrieving the relevant network configuration information, the description and syntax of the resource management techniques, the CAUTION++ configuration data such as IP addresses of communicating modules, as well as an historical database of cases to support the decisions on which resource management technique is to be applied through a Case-Based Reasoning approach [1].
- **Interface modules:** towards the ITMU, NMS and GMU, which manage the communications towards these external entities.

Figure 8 shows the proposed architecture for the RMU entity

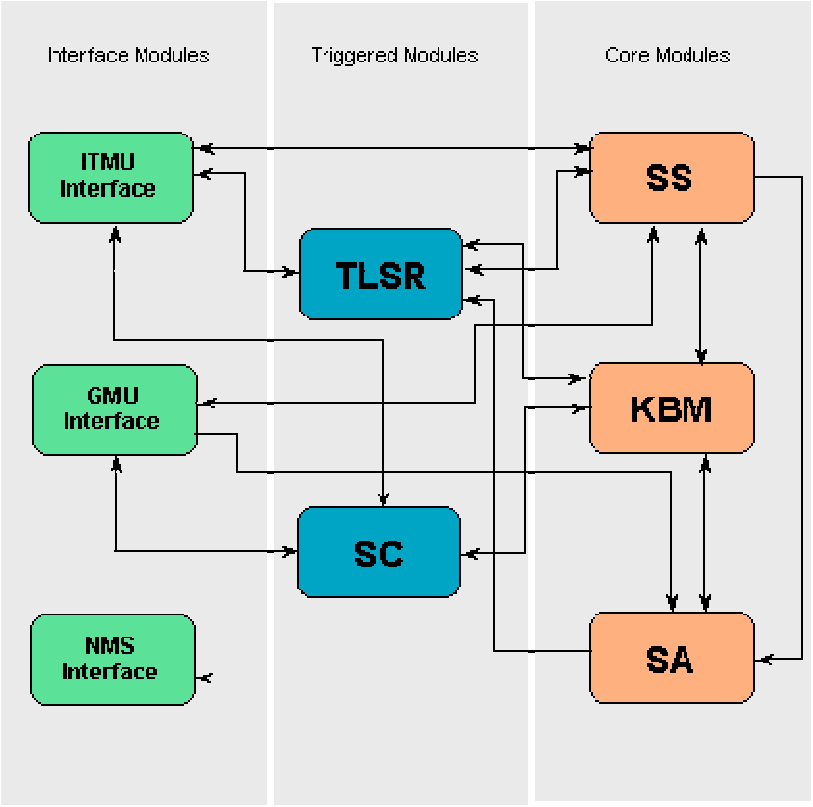


Figure 8. RMU architecture

The design of the RMU has been on purpose made scalable enough to accommodate different radio access network scenarios with minimal changes. Indeed, the internal processing of the RMU does not differ from one technology to the other, and the same algorithms are used in all cases of interest in CAUTION++.

Rather, the impact of the radio access technology is observed in the interfaces of the unit. More specifically, the interface towards the ITMU and that towards the NMS are those affected. These interfaces are described in the following section.

2.2.2 Functionality

The RMU receives from the ITMU the list of alarms that informs about congestion situations, and:

- Determines the Traffic Load Scenario that best suits the current congestion situations, as described by the ITMU congestion notification events.
- Selects the best resource management strategy to cope with the congestion situations. This entails deciding which part of the traffic that is causing the congestion is better to handle locally with the resources of the controlled radio access technology, and which part is better to escalate to the GMU for the sake of an upper level decision-making. This first step of the RMU decision-making is realized through the application of a specific business model, described in CAUTION++ Deliverable D-3.7, [6]. For the part of the traffic that the RMU decides to handle locally, a second decision-making step is applied to decide which resource management techniques are to be applied and also to set parameters for actuation of these resource management techniques. This second decision-making step is described in CAUTION++ Deliverable D-3.4, [5].
- Applies the selected strategies, through the specific NMS of the controlled radio access network.

Besides being activated by an ITMU alarm, each RMU may also be activated by its controlling GMU. Indeed, the GMU may require RMU support for:

- Gathering information about the amount of available resources in same areas of the radio access network controlled by the RMU.
- Executing some resource management techniques that the GMU may have decided or that the CAUTION++ system is commanded to do through the IMT.

2.2.3 Interfaces

The RMU interfaces with three elements of the CAUTION++ architecture. Therefore, among the interfaces defined for every RAT, three new interfaces must be to be considered, namely I, N, GMR

- **I interface:** This interface is specified between the ITMU and RMU mode modules. Via this interface, for every RAT considered, the corresponding ITMU sends the monitoring alarms from the congested cells to the appropriate RMU. The RMU collects and process this monitoring information, requesting if needed additional information to the ITMU for the neighbouring cells.
- **N interface:** This interface is defined between the RMU and the specific NMS modules of each particular RAT. Via this interface the RMU forwards commands to the NMS. These commands carry out the network configuration parameters to be modified to cope with the congestion situation. These parameters have been obtained from the appropriate resource management techniques applied to the corresponding RAT.
- **GMU interface:** This interface is defined between the RMU modules and the GMU module. This is probably the most significant interface into the whole CAUTION++ architecture. Via this interface both alarms from the different ITMU as well as commands from the status of the significant RMU parameters are sent to the GMU. In addition to that the GMU sends commands carrying new traffic profiles and network configuration parameters etc. to be considered for the different RMUs.

Taking into account the mostly of the CAUTION++ elements are connected over Ethernet (802.3) Local or Wide Area Network (LAN or WAN) depending on the actual location of the elements, a TCP/IP protocol is proposed as the appropriate way to transfer information through these interfaces. In particular the messages will be exchanged using a XML format.

A more detailed description of the interfaces can be found in chapter 3.

2.3 GMU

2.3.1 Introduction

The GMU software components designed follows the one of RMU, but with new modules, according to the role of GMU and the four invoked states. The logical architecture is divided into three sections: interface modules, triggered modules and core modules. Each one describes the main functionalities of connectivity, triggering and processing. The CAUTION++ GMU modules are depicted in Figure 9.

The submodules that compose GMU are the following:

- **Traffic Resource Map Builder (TRMB):** is the principal module that triggers a Decision Making Process when an RMU alarm or a help request from another operator are present. This module with the help of two other GMU modules, GMU Interface Module and RMU Interface Module, creates a TRM for the affected area. At the same time, it communicates with the LS interface for user location purposes and with the MGIS Interface module to update the traffic map with coverage info, in order to identify candidate networks belonging to the same operator. The output of the TRMB is a TRM that is fed to the SS Module. Furthermore the TRMB participates in providing the maximum coverage capabilities to IMT users according to his/her preferences.
- **Information Exchange Module (IEM):** serves the requests coming from the IMT interface module. This module manages and delivers information according to the user needs: network information and cell information status; network information structure; resource management techniques execution and performing vertical, vertical-vertical handovers. In order to achieve this, the IEM enables the communication between all coverage and location info provided by the MGIS together with the LS and other network information by direct communication with the TRMB module and RMU interface. Furthermore the exchange module interacts with the KBM to retrieve the list of predefined RMTs. The communication between GMU and IMT is described in detail in CAUTION++ Deliverable D-3.3 ([2]).
- **GMU Strategy Selector Module (SS):** is the Core Module for the Decision Making Process. Based upon the TRM that is provided by the TRMB. The SS module handles the affected area by applying a business model to decide what is to be treated internally and what is to be escalated to other GMUs. The SS remains active to jointly treat other RMU alarms that may arrive for the same area and terminates when the area it is treating is overload-free. The SS is also responsible to support the RMU in order to avoid black spots in a determined area, as a result the SS will reply either accepted or denied permissions for applying a RMT (e.g. cell breathing techniques).
- **GMU Strategy Actuator module (SA):** manages the Vertical, Vertical-Vertical Handover processes in order to actuate the reallocation decision taken by the GMU with the aid of the business model. If needed, this module asks the RMU to apply specific commands (e.g. forced handover, cell breathing) that make easier the handover process. The SA communicates also with the LS through the LS Interface Module to obtain the x-y coordinates needed to locate the users that have to be moved from one RAT to another or from one GMU to another. The location of user is necessary to accomplish in efficient way the Vertical, Vertical-Vertical Handover.
- **Knowledge Base Manager Module (KBM):** stores several kinds of information from all internal processes of GMU, like the list of RMTs that its controlled RMUs are applying, the list of actions that has recently taken, the mapping between RMU alarms and SS identifiers, the RMTs and finally handover events. Some information are only stored for a limited period of time, while other information will remain available to the network operator that can then analyze them in order to improve system configuration.

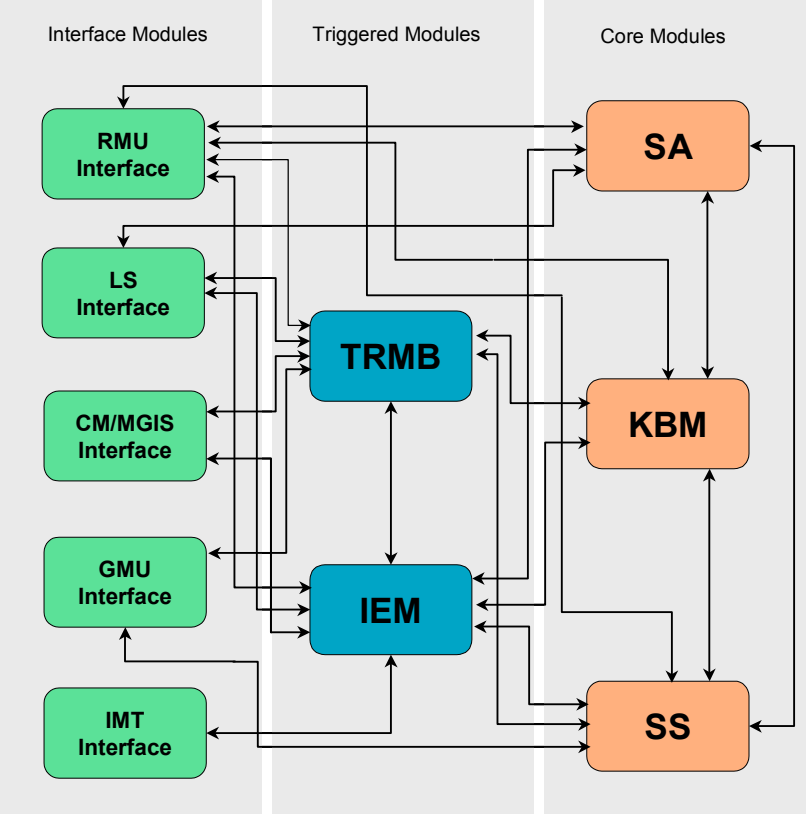


Figure 9. GMU architecture

2.3.2 Functionality

The functionality of the GMU is activated by the requests coming from RMUs, GMUs and from IMTs. In the case the request comes from one if the controlled RMUs, then it may be either one of the two following scenarios:

- The RMU is experiencing a congestion situation that is to be handled through the GMU intervention.
- The RMU is considering the application of some resource management techniques whose actuation might results in black spots area in the heterogeneous network coverage, and is therefore asking GMU permission to proceed with such decision.

In the first case, the GMU will enter a congestion treatment process quite similar to the one followed by the RMU. Indeed, the GMU will perform a first step of decision-making to decide whether it is convenient to entirely handle the congestion event within the boundaries of the available radio access networks, or rather it is convenient to look for the support of other network operators' GMUs.

If a part of the traffic is to be handled locally, then a second decision-making step is performed to decide which technique is to be applied to rearrange traffic across the controlled networks. It is worthwhile remarking that the GMU is enabled to apply only a few resource management techniques, i.e. those that can be used to move users across different networks with vertical and vertical-vertical handover. This split in resource management abilities derives from the division of roles between local and global resource management that RMU and GMU have in CAUTION++.

If a part of the traffic is to be offered to other GMUs, then the GMU will start a process of sequentially enquiry towards the other GMUs that participate in the CAUTION++ system. This process stops when all the traffic to be moved has been accepted by the other GMUs or when no more GMUS are available to take the offered traffic.

If the GMU gets a request from an RMU to assess a potential blackspot condition, it will verify through the MGIS that at least another radio access network is providing coverage in the area in which the RMU is willing to reduce the coverage provided by its controlled radio access network. If such another covering network exists, then the RMU is allowed to continue in its resource management choice, otherwise the RMU decision gets revised by the GMU in a way that the blackspot is not generated. The GMU will reduce the scope of the RMU decision and will take care by itself to solve the congestion by applying some of its available resource management techniques, i.e. a vertical-vertical handover technique.

When the GMU receives a request from another GMU, it is because the requesting GMU wants to offer some traffic it cannot handle within the resources of its controlled networks. On receipt of this request, the GMU will perform the same processing as if the request would have come from one of its controlled RMUs. Solely, as described in CAUTION++ Deliverable D3.7 ([6]), the business model that will be applied in the first step of the decision-making may be different, to take into consideration the fact that the offered traffic is actually traffic that consists of roaming subscribers.

The communications between IMT and GMU may happen as a result of the subscriber wish to gather from the CAUTION++ system the information about the most suitable network to connect to for the specific service he wants to ask the execution. In this case the GMU will perform an enquiry to the radio access networks existing in the area the subscriber is located in, to retrieve information about the availability of resources. This enquiry requires the services of the LS, MGIS and of the RMUs. Other types of GMU interfaces exist towards the IMT. These interfaces are actually deployed to allow the IMT to communicate to other CAUTION++ components via the GMU, which in these cases only acts as a bridge. Specifically, we are referring to the IMT-LS and IMT-RMU communication paths, which are both realized through the GMU data relay.

2.3.3 Interfaces

GMU handles five interfaces towards external components. These components are MGIS, LS and IMT. At the same time the there are also two sets of internal CAUTION++ interfaces, one towards to RMUs and the other towards to other GMUs. The interfaces are shown below with the corresponding name:

Internal CAUTION++ Interfaces:

- To RMU (“GMRx” interface):
  - **GMR_{AP}** (GMU ↔ GSM/GPRS RMU)
  - **GMR_{UM}** (GMU ↔ UMTS RMU)
  - **GMR_{W}** (GMU ↔ WLAN RMU)
- To GMU – “**R**” interface
- To IMT – “**V**” interface
- To LS – “**LG**” interface
- To MGIS – “**NMDI**” interface

A more detailed description of the interfaces can be found in chapter 3.

2.4 LS

2.4.1 Introduction

The role of the Location Server (LS) is to provide location information to other system components in order to enhance the network operation by improving and supporting the resource and mobility management. The server provides location information in several wireless mobile systems including GSM, UMTS and WLAN and supports three techniques, namely Cell or Access Point ID, Signal Strength and DCM, in each specific network. The implemented algorithms use the measurement information obtained as parameters of the location request and the network information obtained by queries from the MGIS database. The provision of the location information is dependent on availability of relevant information (e.g. measurements) in the target access network, which depends e.g. on the network layout and environment.

2.4.2 Functionality

The functionality of the LS is based on the location requests from GMU or RMU and on the available location-related measurement information. The main function of the LS is to provide a location estimate of the mobile terminal to the requester, which in CAUTION++ can be either GMU or IMT via GMU. The LS itself is not involved in any decision making in the CAUTION++ architecture, but the decisions made by the GMU and RMU can be made based on the obtained location estimates of the users in the network.

The LS supports three location algorithms: Cell ID (AP ID in WLAN), Signal Strength and Database Correlation Method (DCM), which are used to provide location estimation in GSM, UMTS and WLAN. The algorithms in GSM and UMTS are all based on usage of standard measurement information made by the base stations or mobile terminals. In WLAN there are no standard based measurements, thus, the WLAN location is implemented based on measurements obtained by a defined WLAN card. The used location algorithm is chosen based on the available measurement information, or also all supported techniques may be used if enough information is available. The measurement information is given as input parameters of the location request and it includes the results of measurements made either by the mobile terminal to be located or by some network component(s), typically base station(s). The actual content of the measurement information is dependent on the specific cellular system. If needed by the location algorithm, the LS retrieves the required network related information or stored measurements from the MGIS database via MGIS server, such as in the DCM algorithm the fingerprint information.

2.4.3 Interfaces

- **LM:** (LS ↔ MGIS)
- **LG:** (LS ↔ GMU)

The LS uses the LM interface to retrieve or make queries of supporting or required information for the user location estimation. The MGIS can also look up the LS in order to retrieve further information about the location of the user ((x,y) coordinates). Via the LG interface the GMU, or RMU via GMU, requests the location information of a defined user or user group. After location estimation is complete, the LS returns the coordinates (x,y) of the mobile terminal through the LG.

2.5 MGIS

2.5.1 Introduction

The Mobile network Geographic Information System (MGIS) database is used to store network specific information used by the location server, coverage manager and by other CAUTION++ components, e.g. ITMU, GMU and RMU via GMU. The MGIS database is structured by tables, which are either system specific or common for all. The information stored in MGIS tables can contain stable long-term information from the network, data referring to a specific network state, measurement results or other system specific information from GPRS/GSM, UMTS or WLAN.

Being only a database, the MGIS requires an interface to enable other programs to efficiently utilize the MGIS.

2.5.2 Functionality

The main function of the Mobile network Geographic Information System (MGIS) server is to answer queries concerning the structure of the network(s) and their coverage areas. The queries can be made either by the LS for location estimation purposes or by the ITMU or GMU to aid in resource and mobility management. The required information is stored in the MGIS database, which is used also as a fingerprint database for the DCM location algorithm. Thus, the database must contain the information about the network structure (sites, cells and locations of those) as well as the information of cell coverage areas (or path losses).

Each query contains certain input parameter e.g. the Cell ID, BTS / Node B / AP, specific access network or a certain area. Depending on the query, the MGIS server may return e.g. the Cell IDs of the other access networks cells covering the area given as input (indicated by Cell ID), the best access networks for certain base station, the list of cells and access networks which cover certain location (x,y).

The MGIS may also itself retrieve real-time information about the status of the networks (from the GMU or ITMU) or information about the user location (from the LS). The information in MGIS is stored in tables, which contain stable long term information from the network, data referring to a specific network state, measurement results or other system specific information from GPRS/GSM, UMTS or WLAN. The tables are either system specific or common for all systems. The communication is done via the interfaces described in the following.

2.5.3 Interfaces

The MGIS server interfaces with three different components, GMU, ITMU and LS, by using the following interfaces:

- **NMDI:** (MGIS $\leftrightarrow$ GMU)
- **NMDI:** (MGIS $\leftrightarrow$ ITMU)

Through the NMDI interface the MGIS communicates with ITMUs, as well as with GMU. The NMDI interface can be used by MGIS (towards ITMU or GMU), in order to collect and store real-time information about the status of the networks. For that reason, the collection of the information is useful to be very frequent. GMU can also send queries to MGIS, in order to be informed about statistical information.

2.6 IMT

2.6.1 Introduction

IMT is the generic name of CAUTION++ enabled devices, which allows users to retrieve useful information from the CAUTION++ platform. This information can be used both for normal users, who need to decide the more suitable network to get a service granted, and for super users, who need to know about network status for maintenance purposes.

IMT software can be deployed on handheld, PDA or laptop devices.

2.6.2 Functionality

The functions of IMT devices are dependant on the kind of user trying to access the network:

- For normal users, IMT functions are related with the request of information about available resources and costs in the target networks.
  - Request for available networks
  - Request for available services
  - Request for uplink and downlink available data rates
  - Request for pricing information
- For super users, IMT functions are related with the retrieval of network status data.
  - Request for available networks and their structure
  - Request for coverage areas and dominance areas
  - Request for available cells in a certain position
  - Request for overlapping cells and blackspot areas
  - Request for user positioning and users attached to a certain cell
  - Request for network status and cell status
  - Command to execute a certain RMT

2.6.3 Interfaces

IMT devices interface only to GMU module, through **V** interface.

3 CAUTION++ INTERFACES

3.1 EXTERNAL INTERFACES

The network elements designed for GSM (ITMU, RMU, LS) in CAUTION++ have increased their number as well as their complexity in the case of CAUTION++ by the addition of an extra component (GMU) as well as the integration of them to a multi-system wireless environment including GSM, GPRS, UMTS and WLAN. In this section the external interfaces of CAUTION++ system will be examined. The following description of the external interfacing needed for traffic monitoring will investigate which network elements are interfaced, as well as which kind of physical links are to be used.

The external interfaces are divided into two categories:

- The interfaces towards the RANs
- The interfaces towards the NMCs.

The external interfaces of CAUTION++ system towards the RANs and the NMCs are segmented to four, with respect to the GSM, GPRS, UMTS and WLAN networks.

3.1.1 Interfaces towards the RANs of the wireless networks

The interfaces towards the RANs realize the goal of each ITMU, which is to perform the real time monitoring for the corresponding network. In order that this goal will be accomplished and a clear overview for the network's state is obtained, the ITMU utilizes all the available reporting mechanisms.

On Figure 10 the external interfaces of CAUTION++ system are illustrated, towards the RANs of the wireless networks.

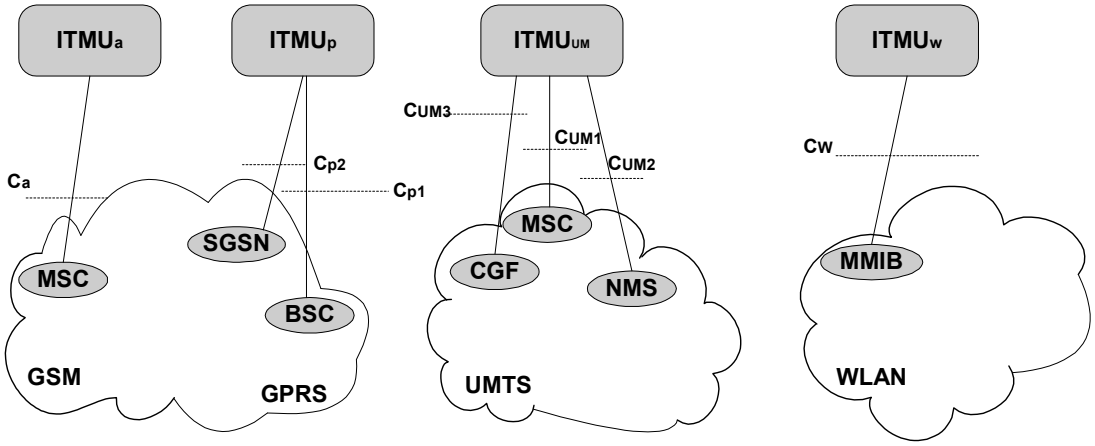


Figure 10. External Interfaces towards the RANs of the wireless networks

The following sections describe in detail each monitoring interface.

3.1.1.1 GSM:

- **Ca**: Interface between ITMUa and MSC

  ITMU collects the reports from one or several MSCs through the Ca interface. These connections run over an Ethernet (802.3) network. The Ca interface format uses the XML structure shown in Table 1, and is propagated in a TCP packet over an IP network:

<?xml version="1.0"?>	
<ICR>	*ITMU Call Report*
<RID>…</RID>	*Report ID*
<CID>…</CID>	*Cell ID*
<NCID>…</NCID>	*New Cell ID*
<EID>…</EID>	*Event ID*
<TS>…</TS>	*Time Stamp*
<ST>…</ST>	*Signalling Time*
<TC>…</TC>	*Termination Code*
</ICR>	

Table 1. ICR format for GSM

ITMU must know the users that are locked in each cell. For that reason a second XML structure-report must exist. This XML structure is shown in Table 2:

<?xml version="1.0"?>	
<ICR2>	*ITMU Call Report 2*
<Cell_ID>…</Cell_ID>	*Cell ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<IMSI> Served IMSI </IMSI>	*Served IMSI*
<MSISDN> Served MSISDN </MSISDN>	*Served MSISDN*
<TOS> Type of Service </TOS>	*Type of Service*
</ICR2>	

Table 2. ICR2 format for GSM

3.1.1.2 GPRS:

- **Cp_1**: Interface between ITMUp and BSC

  The format of GPRS ITMU input interface uses the XML structure showed in Table 3.

<?xml version="1.0"?>	
<ICR>	*ITMU Call Report*
<Cell_ID>…</Cell_ID>	*Cell ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<NRRU>…</NRRU>	*Number of Radio Resources UL_TBF*
<NRRD>…</NRRD>	*Number of Radio Resources DL_TBF*
<URCT>…</URCT>	*UL Release due to CS Traffic*
<DRCT>…</DRCT>	*DL Release due to CS Traffic*
<URNR>…</URNR>	*UL Release due to no response from MT*
<DRNR>…</DRNR>	*DL Release due to no response from MT*
<NTBF>…</NTBF>	*Number TBF*
<TBFT>…</TBFT>	*TBF Total Time*
<AUDT>…</AUDT>	*Actual UL Data Throughput*
<ADDT>…</ADDT>	*Actual DL Data Throughput*
<MNBL>…</MNBL>	*Max Number of Blocks*
<FGAT>…</FGAT>	*Fail GPRS Attach*
<SGAT>…</SGAP>	*Successful GPRS Attach*
</ICR>	

Table 3. ICR1 format for GPRS

- **Cp_2**: Interface between ITMUp and SGSN

  ITMU must know the users that are camped in each cell. For that reason a second XML structure-report must exist. This XML structure is shown in Table 4:

<?xml version="1.0"?>	
<ICR2>	*ITMU Call Report 2*
<Cell_ID>…</Cell_ID>	*Cell ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<IMSI> Served IMSI </IMSI>	*Served IMSI*
<MSISDN> Served MSISDN </MSISDN>	*Served MSISDN*
<TOS> Type of Service </TOS>	*Type of Service*
</ICR2>	

Table 4. ICR2 format for GPRS

3.1.1.3 UMTS:

- **C_{UM1}**: Interface between $ITMU_{UM}$ and MSC (for the circuit-switched part of UMTS)

The XML structure for the input of UMTS ITMU is listed in Table 5.

<?xml version=”1.0”?>	
<ICR>	*ITMU Call Report*
<Cell_ID>…</Cell_ID>	*Cell ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<RTDCP>…</RTDCP>	*RTD_CID_PS*
<TPUMC>…</TPUMC>	*TPUTmax_CID*
<TPUAC>…</TPUAC>	*TPUTavg_CID*
<TPUACO>…</TPUACO>	*TPUTavg_CID_old*
<RABECD>…</RABECD>	*RAB_end_CID_drop*
<RABEC>…</RABEC>	*RAB_end_CID*
<RABRC>…</RABRC>	*RAB_reneg_CID*
<RABC>…</RABC>	*RAB_CID*
<RABNMC>…</RABNMC>	*RAB_n_max_CID*
<RABNNC>…</RABNNC>	*RAB_n_neg_CID*
<RABRQC>…</RABRQC>	*RAB_req_CID*
<BQC>…</BQC>	*BadQuality_CID*
<DURTC>…</DURTC>	*DURtot_CID*
<BLERAC>…</BLERAC>	*BLERavg_CID*
<TPUTTC>…</TPUTTC>	*TPUTtot_CID*
<IC>…</IC>	*I_CID*
<UC>…</UC>	*user_CID*
<PTXC>…</PTXC>	*PTX_CID*
<PTXCM>…</PTXCM>	*PTX_CID_max*
<UC>…</UC>	*user_CID*
<RSCPAC>…</RSCPAC>	*RSCPavg_CID*
<PTXCPC>…</PTXCPC>	*PTX_CPICH_CID*
<TPCSC>…</TPCSC>	*TPC_sum_CID*
<CC>…</CC>	*code_CID*
<DURTC>…</DURTC>	*DURtot_CID*
<USC>…</USC>	*Users_CID*

<LINK>…</LINK>	*link*
<USER>…</USER>	*user*
<LUC>…</LUC>	*locupd_CID*
<CD>…</CD>	*CounterDelay*
</ICR>	

Table 5. ICR1 format for UMTS

- **C_{UM2}**: Interface between $ITMU_{UM}$ and CGF

  Finally UMTS ITMU must know the users that are locked in each cell. For that reason a second XML structure-report must exist. This XML structure is shown in Table 6:

<?xml version=”1.0”?>	
<ICR2>	*ITMU Call Report 2*
<Cell_ID>…</Cell_ID>	*Cell ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<IMSI> Served IMSI </IMSI>	*Served IMSI*
<MSISDN> Served MSISDN </MSISDN>	*Served MSISDN*
<TOS> Type of Service </TOS>	*Type of Service*
</ICR2>	

Table 6. ICR2 format for UMTS

3.1.1.4 WLAN:

- **Cw**: Interface between ITMUw and MMIB.

  The XML structure for the input of WLAN ITMU is listed in Table 7.

<?xml version=”1.0”?>	
<ICR>	*ITMU Call Report*
<Cell_ID>…</Cell_ID>	*Access Point ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<LATPU>…</LATPU>	*Latency per user*
<LAT>…</LAT>	*Latency*
<EULPPU>…</EULPPU>	*Erroneous UL packets per user*
<TULPPU>…</TULPPU>	*Total UL packets per user*
<EDLPPU>…</EDLPPU>	*Erroneous DL packets per user*
<TDLPPU>…</TDLPPU>	*Total DL packets per user*
<EULP>…</EULP>	*Erroneous UL packets*
<TULP>…</TULP>	*Total UL packets*
<EDLP>…</EDLP>	*Erroneous DL packets*
<TDLP>…</TDLP>	*Total DL packets*
<LULPPU>…</LULPPU>	*Lost UL packets per user*
<LDLPPU>…</LDLPPU>	*Lost DL packets per user*
<LULP>…</LULP>	*Lost UL packets*
<LDLP>…</LDLP>	*Lost DL packets*
<PTHPU>…</PTHPU>	*Peak throughput per user*
<ATHPU>…</ATHPU>	*Average throughput per user*
<ULPD>…</ULPD>	*UL payload data (Kbytes)*
<DLPD>…</DLPD>	*DL payload data (Kbytes)*
</ICR>	

Table 7. ICR1 format for WLAN

Finally WLAN ITMU must know the users that are locked in each access point. For that reason a special XML structure-report must exist. This XML structure is shown in Table 7:

<?xml version="1.0"?>	
<ICR2>	*ITMU Call Report 2*
<Cell_ID>…</Cell_ID>	*Access Point ID*
<Time>…</Time>	*Time Stamp*
<Date>…</Date>	*Date Stamp*
<IMSI> Served IMSI </IMSI>	*Served MAC*
<MSISDN> Served MSISDN </MSISDN>	*Served IP*
<TOS> Type of Service </TOS>	*Type of Service*
</ICR2>	

Table 8. ICR2 format for WLAN

3.1.1.5 Procedure:

The first step of the procedure followed is the collection of the Key Performance Indicators (KPIs) via the Cx interfaces. The ITMU will compare each of these parameters with a set of threshold values (stored values), to verify whether the threshold value is reached or not. For each access network the ITMU will extract the KPIs from the counterpart entity.

For example, in GSM case, with the usage of a standard interface (Ca) the ITMU communicates with the MSC and collects the KPIs. The equivalent information for GPRS and for UMTS networks is provided to the ITMU by the SGSN, and for WLAN network the router undertakes this role. The Cx interfaces are Ethernet based (TCP/IP), directly connected from the RANs' entities to the ITMUs of CAUTION++ system. Each ITMU can serve multiple instances of the same network (e.g. $ITMU_{UM}$ can serve multiple SGSNs, RNCs and MSCs of the UMTS network). For each connection, a dedicated Ethernet NIC (Network Interface Card) is needed.

3.1.2 Interfaces towards the NMSs of the wireless networks

The Nx interfaces are based on TCP/IP connections over Ethernet, as well as the Cx interfaces. The RMUs have taken an initial decision about the Resource Management Technique (RMT) or the set of RMTs that has to be applied, in order to achieve decongestion. In other words, Nx are actually the interfaces via which the RMUs are informing the corresponding network entities (OMC and NMS respectively) about this decision. The information about the selected RMT is transferred and executed at the OMC or NMS respectively, via the Nx interfaces. More analytically, the interfaces towards the NMSs of each wireless network are depicted in Figure 11 following below.

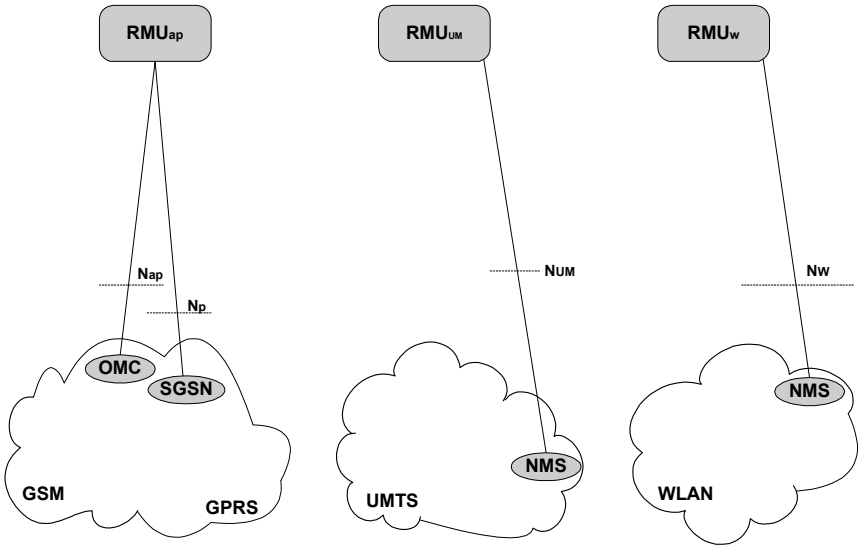


Figure 11. External Interfaces towards the NMSs of the wireless networks

These are respectively:

GSM:

- **Nap:** Interface between RMUa and OMC

GPRS:

- **Nap:** Interface between RMUp and OMC (there is also a 3GPP standardized proposal, defining CORBA interfaces, in which Nap can be based)
- **Np:** Interface between RMUp and SGSN

UMTS:

- **N_{UM}:** Interface between RMUum and NMS of UMTS

WLAN:

- **Nw:** Interface between RMUw and NMS of WLAN

3.2 INTERNAL INTERFACES

The internal interfaces among core CAUTION++ components (ITMUs, RMUs and GMUs), which are shown in Figure 12, will be examined in this section. Other internal interfaces lie between GMU and IMT, LS and MGIS, GMU and LS, LS and MGIS, GMU and MGIS, MGIS and ITMUs of the wireless networks.

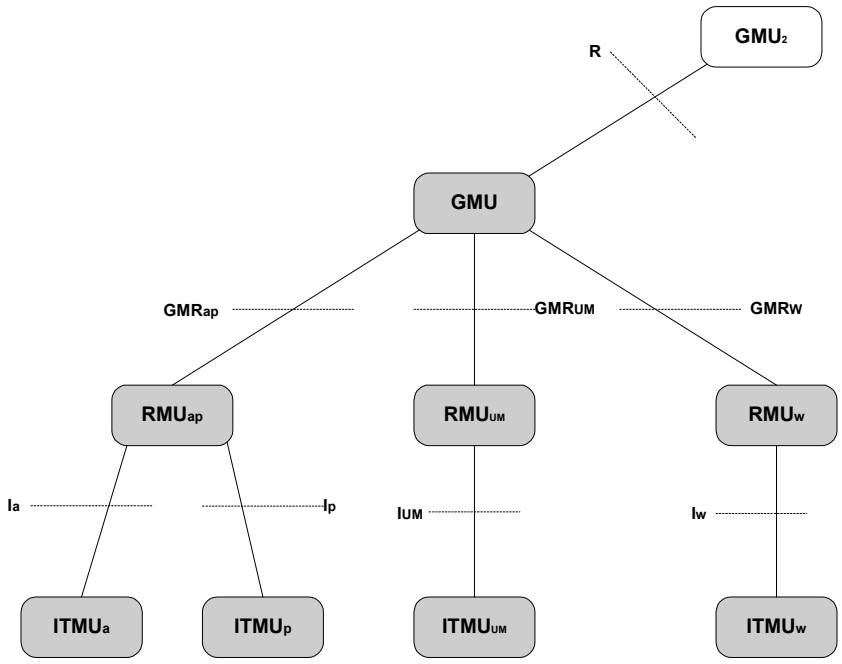


Figure 12. Internal Interfaces in CAUTION++ system

The internal interfaces in CAUTION++ architecture are described below:

3.2.1 Interfaces between ITMUs and RMUs

ITMU, as previously mentioned, is responsible for the real-time monitoring of the networks. When congestion appears, or seems to be appeared (actually, when a combination of some values exceeds a threshold value), ITMUx informs RMUx via Ix interfaces with alarm messages. The communication between RMUx and ITMUx continues during the decongestion period, because adjustments of the technique's parameters may be necessary for the smooth transition of the system to the normal state. This internal communication (Ix interfaces) is based on TCP/IP protocol and the messages that are exchanged are alarms, relaxes, neighbour cell info, and predefined queries from RMUx to ITMUx.

3.2.1.1 **Ia:** Interface between ITMUa and RMUa in GSM network

The XML structures for the messages belonging to interface Ia are listed in the following tables:

When ITMU detects an overloaded resource (a KPI over the threshold), it raises an alarm to RMU. This alarm contains all the data of the congested resource of the congested cell. So RMU is provided with a snapshot of the overall congestion situation. The alarm is periodically sent until the resource drops back to normal operation. The format of the alarm message is showed in the following table:

<?xml version=”1.0”?>	
<alarm>	
<alarm_type> … </alarm_type>	*Values: AL, RX, CLC*
<cell_id> … </cell_id>	*Affected cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<sdcch_utilization> … </sdcch_utilization>	*SDDCH utilization*
<sacch_utilization> … </sacch_utilization>	*SACCH utilization*
<tch_utilization> … </tch_utilization>	*TCH utilization*
<rach_utilization> … </rach_utilization>	*RACH utilization*
<pch_utilization> … </pch_utilization>	*PCH utilization*
<agch_utilization> … </agch_utilization>	*AGCH utilization*
<tch_blocking> … </tch_blocking>	*TCH blocking rate*
<sdcch_blocking> … </sdcch_blocking>	*SDCCH blocking rate*
<emergency_calls> … </emergency_calls>	*Number of emergency calls*
<not-normal_cc> … </not-normal_cc>	*Number of not-normal clear codes*
</alarm>	

Table 9. Alarm message

When RMU receives the alarm, it might not be able to map the information into a particular scenario, or it requires a better view of the system traffic prior the selection of the appropriate command. Therefore, RMU will request the data of neighbour cells, in order to decide about the area that is affected from the traffic overload. This RMU query has the following XML structure:

<?xml version=”1.0”?>	
<neighbour_cell_info>	
<tlsr_in> … </tlsr_in>	*Traffic Load Scenario indicator*
<cell_id> … </cell_id>	*Queried cells IDs*
</neighbour_cell_info>	

Table 10. NCI request message

The ITMU answer to the previous query has the following XML structure:

<?xml version=”1.0”?>	
<message>	
<message_type> … </message_type>	*Value: NCI*
<cell_id> … </cell_id>	*Queried cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<sdcch_utilization> … </sdcch_utilization>	*SDDCH utilization*
<sacch_utilization> … </sacch_utilization>	*SACCH utilization*
<tch_utilization> … </tcch_utilization>	*TCH utilization*
<rach_utilization> … </rach_utilization	*RACH utilization*
<pch_utilization> … </pch_utilization>	*PCH utilization*
<agch_utilization> … </agch_utilization>	*AGCH utilization*
<tch_blocking> … </tch_blocking>	*TCH blocking rate*
<sdcch_blocking> … </sdcch_blocking>	*SDCCH blocking rate*
<emergency_calls> … </emergency_calls>	*Number of emergency calls*
<not-normal_cc> … </not-normal_cc>	*Number of not-normal clear codes*
</message>	

Table 11. NCI response message

In some circumstances, RMU requests from ITMU to change the alarm threshold values. This is achieved by sending a special threshold change command to ITMU. This command has the following structure:

<?xml version=”1.0”?>	
<change_thresholds>	
<cell_id> … </cell_id>	*Affected cells IDs*
<duration> … </duration>	*Duration of change*
<sdcch_threshold> … </sdcch_threshold>	*SDDCH utilization threshold*
<sacch_threshold> … </sacch_threshold>	*SACCH utilization threshold*
<tch_threshold> … </tch_threshold>	*TCH utilization threshold*
<rach_threshold> … </rach_threshold>	*RACH utilization threshold*
<pch_threshold> … </pch_threshold>	*PCH utilization threshold*
<agch_threshold> … </agch_threshold>	*AGCH utilization threshold*

<tch_blocking> … </tch_blocking>	*TCH blocking rate threshold*
<sdcch_blocking> … </sdcch_blocking>	*SDCCH blocking rate threshold*
<emergency_calls> … </emergency_calls>	*Number of emergency calls threshold*
<not-normal_cc> … </not-normal_cc>	*Number of not-normal clear codes threshold*
</change_thresholds>	

Table 12. Change thresholds message

In case that RMU wants to stop ITMU monitoring for a cell, a special command is needed. This command has the following XML structure:

<?xml version=”1.0”?>	
<monitor_indicator>	
<cell_id> … </cell_id>	*Affected cells IDs*
<indicator> … </indicator>	*Values: start, stop*
</monitor_indicator>	

Table 13. Monitor indicator message

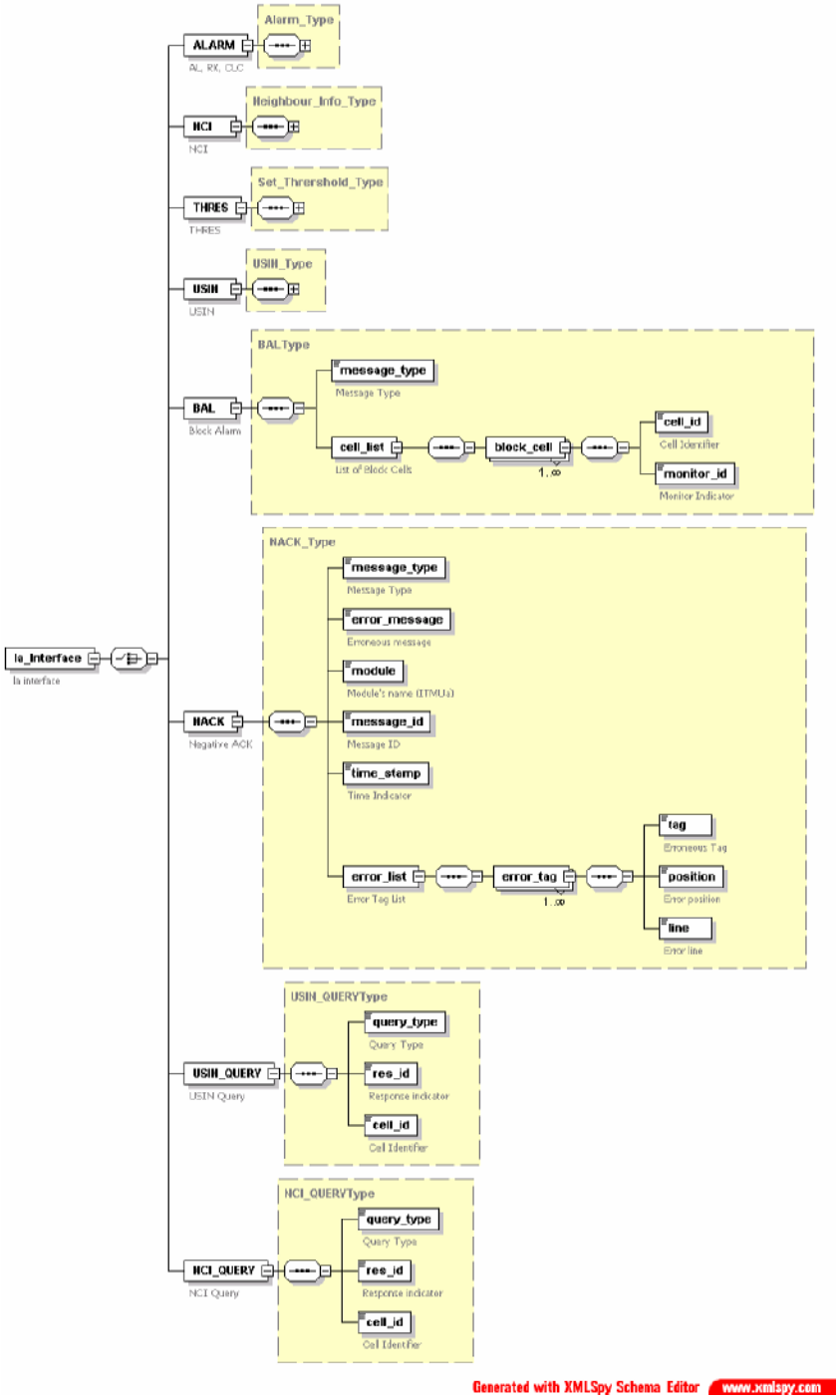


Figure 13. Ia interface

3.2.1.2 **Ip**: Interface between ITMUp and RMUp in GPRS network

The XML generic structure for the messages belonging to interface Ip is listed in the following table

<?xml version="1.0" encoding="UTF-8" ?>	
<Ip_Interface>	
<ALARM> … </ALARM>	*Alarm block*
<NCI> … </NCI>	*NCI block*
<THRES> … </THRES>	*Thresholds block*
<USIN> … </USIN>	*USIN block*
<BAL> … </BAL>	*BAL block*
<NACK> … </NACK>	*NACK block*
<USIN_QUERY> … </USIN_QUERY>	*USIN_QUERY block*
<NCI_QUERY> … </NCI_QUERY>	*NCI_QUERY block*
</Ip_Interface>	

Table 14. Ip generic message

When ITMU detects an overloaded resource (a KPI over the threshold), it raises an alarm to RMU. This alarm contains all the data of the congested resource of the congested cell. So RMU is provided with a snapshot of the overall congestion situation. The alarm is periodically sent until the resource drops back to normal operation. The format of the alarm message is showed in the following table:

<ALARM>	
<alarm_type> … </alarm_type>	*Values: AL, RX, CLC*
<cell_id> … </cell_id>	*Affected cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<KPI> … </KPI>	*KPI block*
</ALARM>	

Table 15. Alarm message

When RMU receives the alarm, it might not be able to map the information into a particular scenario, or it requires a better view of the system traffic prior the selection of the appropriate command. Therefore, RMU will request the data of neighbour cells, in order to decide about the area that is affected from the traffic overload. This RMU query has the following XML structure:

<NCI_QUERY>	
<query_type> … </query_type>	*NCI_QUERY*
<res_id> … </res_id>	*Response indicator*
<cell_id> … </cell_id>	*Queried cells IDs*
</NCI_QUERY>	

Table 16. NCI request message

The ITMU answer to the previous query has the following XML structure:

<NCI>	
<message_type> … </message_type>	*Value: NCI*
<cell_id> … </cell_id>	*Queried cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<res_id> … </res_id>	*Response indicator*
<KPI> … </KPI>	*KPI block*
</NCI>	

Table 17. NCI response message

In some circumstances, RMU requests from ITMU to change the alarm threshold values. This is achieved by sending a special threshold change command to ITMU. This command has the following structure regarding the ITMU and network type.

<THRES>	
<message_type> … </message_type>	*Value: THRES*
<cell_id> … </cell_id>	*Affected cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<DURATION> … </DURATION>	*Duration of change*
<KPI> … </KPI>	*KPI block*
</THRES>	

Table 18. Change thresholds message

RMU can also request ITMU for information about the users attached to a certain cell. This command has the following structure:

<USIN_QUERY>	
<query_type> … </query_type>	*Value: USIN_QUERY*
<res_id> … </res_id>	*Response indicator*
<cell_id> … </cell_id>	*Affected cells IDs*
</USIN_QUERY>	

Table 19. User information request message

ITMU response to the previous command has the following structure:

<USIN>	
<message_type> … </message_type>	*Value: USIN*
<module> … </module>	*Values: ITMUa, ITMUp, ITMUum, ITMUw*
<message_id> … </message_id>	*Message ID*
<cell_id> … </cell_id>	*Affected cells IDs*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<res_id> .. </res_id>	*Response indicator*
<USER_LIST>	*USER_List block*
<USER> ... </USER>	*USER blocks*
</USER_LIST>	
</USIN>	

Table 20. User information response message

In case that RMU wants to stop ITMU monitoring for a cell, a special command is needed. This command has the following XML structure:

<BAL>	
<message_type> … </message_type>	*Value: BAL*
<CELL_LIST>	*Cell_List block*
<block_cell> ... </block_cell>	*Block_cell blocks*
</CELL_LIST>	
</BAL>	

Table 21. Block alarm message

If RMU has to report ITMU about any error concerning the communication protocol, it uses the following message:

<NACK>	
<message_type> … </message_type>	*Value: NACK*
<error_message> … </error_message>	
<module> … </module>	*Values: ITMUa, ITMUp, ITMUum, ITMUw*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<error_list>	*Error_List block*
<error_tag> ... </error_tag>	*Error_tag blocks*
</error_list>	
</NACK>	

Table 22. NACK message

The XML blocks mentioned above are described in the following tables:

- KPI block:

<KPI>	
<DC_SUCC> … </DC_SUCC>	*Data connection success rate*
<SR_SUCC> … </SR_SUCC>	*Session release rate*
<DELAY> … </DELAY>	*Delay*
<PEAK_THR> … </PEAK_THR>	*Peak throughput*
<MEAN_THR> … </MEAN_THR>	*Mean throughput*
<UTIL> … </UTIL>	*GPRS utilization*
<ATT_FR> … </ATT_FR>	*Attach attempts failure ratio*
</KPI>	

Table 23. KPI block

- USER block:

<USER>	
<imsi> ... </imsi>	*IMSI number of user*
<msisdn> … </msisdn>	*MSISDN number of user*
<tos> … </tos>	*Type of service*
</USER>	

Table 24. USER block

- Block_cell block:

<block_cell>	
<cell_id> … </cell_id>	*Affected cells IDs*
<monitor_id> … </monitor_id>	*Monitor indicator*
</block_cell>	

Table 25. Block_cell block

- Error_tag block:

<error_tag>
<tag> … </tag>
<position> … </position>
<line> … </line>
</error_tag>

Table 26. Error_tag block

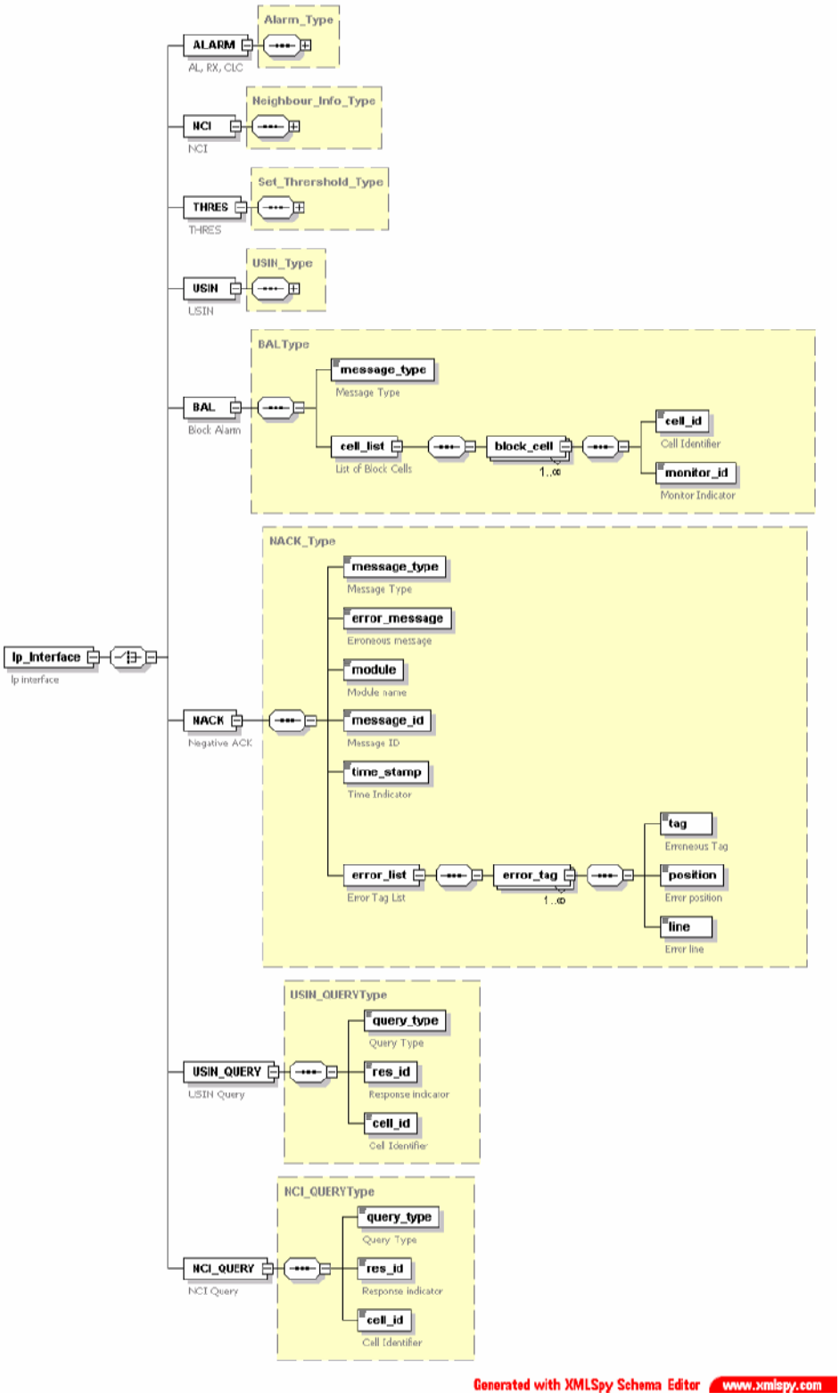


Figure 14. Ip interface

3.2.1.3 I_{UM}: Interface between ITMUum and RMUum in UMTS network

The XML generic structure for the messages belonging to interface Ium is listed in the following table

<?xml version="1.0" encoding="UTF-8" ?>	
<Ium_Interface>	
<ALARM> … </ALARM>	*Alarm block*
<NCI> … </NCI>	*NCI block*
<USIN> … </USIN>	*USIN block*
<NCI_QUERY> … </NCI_QUERY>	*NCI_QUERY block*
<USIN_QUERY> … </USIN_QUERY>	*USIN_QUERY block*
<NACK> … </NACK>	*NACK block*
</Ium_Interface>	

Table 27. Ium generic message

When ITMU detects an overloaded resource (a KPI over the threshold), it raises an alarm to RMU. This alarm contains all the data of the congested resource of the congested cell. So RMU is provided with a snapshot of the overall congestion situation. The alarm is periodically sent until the resource drops back to normal operation. The format of the alarm message is showed in the following table:

<ALARM>	
<alarm_type> … </alarm_type>	*Values: AL, RX, CLC*
<cell_id> … </cell_id>	*Affected cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<KPI> … </KPI>	*KPI block*
</ALARM>	

Table 28. Alarm message

When RMU receives the alarm, it might not be able to map the information into a particular scenario, or it requires a better view of the system traffic prior the selection of the appropriate command. Therefore, RMU will request the data of neighbour cells, in order to decide about the area that is affected from the traffic overload. This RMU query has the following XML structure:

<NCI_QUERY>	
<query_type> … </query_type>	*NCI_QUERY*
<res_id> … </res_id>	*Response indicator*
<cell_id> … </cell_id>	*Queried cells IDs*
</NCI_QUERY>	

Table 29. NCI request message

The ITMU answer to the previous query has the following XML structure:

<NCI>	
<message_type> … </message_type>	*Value: NCI*
<cell_id> … </cell_id>	*Queried cells IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<res_id> … </res_id>	*Response indicator*
<KPI> … </KPI>	*KPI block*
</NCI>	

Table 30. NCI response message

RMU can also request ITMU for information about the users attached to a certain cell. This command has the following structure:

<USIN_QUERY>	
<query_type> … </query_type>	*Value: USIN_QUERY*
<res_id> … </res_id>	*Response indicator*
<cell_id> … </cell_id>	*Affected cells IDs*
</USIN_QUERY>	

Table 31. User information request message

ITMU response to the previous command has the following structure:

<USIN>	
<message_type> … </message_type>	*Value: USIN*
<cell_id> … </cell_id>	*Affected cells IDs*
<message_id> … </message_id>	*Message ID*
<module> … </module>	*Values: ITMUa, ITMUp, ITMUum, ITMUw*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<res_id> .. </res_id>	*Response indicator*
<USER_LIST>	*USER_List block*
<USER> ... </USER>	*USER blocks*
</USER_LIST>	
</USIN>	

Table 32. User information response message

If RMU has to report ITMU about any error concerning the communication protocol, it uses the following message:

<NACK>	
<message_type> … </message_type>	*Value: NACK*
<error_message> … </error_message>	
<module> … </module>	*Values: ITMUa, ITMUp, ITMUum, ITMUw*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<error_list>	*Error_List block*
<error_tag> ... </error_tag>	*Error_tag blocks*
</error_list>	
</NACK>	

Table 33. NACK message

The XML blocks mentioned above are described in the following tables:

- KPI block:

<KPI >	
<DELAY> … </DELAY>	*Delay*
<PEAK_THR> … </PEAK_THR>	*Peak throughput*
<MEAN_THR> … </MEAN_THR>	*Mean throughput*
<CH_M_THR> … </CH_M_THR>	*Change of mean throughput*
<HARD_DR> … </HARD_DR>	*Hard dropping*
<SOFT_DR> … </SOFT_DR>	*Soft dropping*
<HARD_BL> … </HARD_BL>	*Hard blocking*
<SOFT_BL> … </SOFT_BL>	*Soft blocking*
<UNSATIS> … </UNSATIS>	*Unsatisfied*
<BAD_QUAL> … </BAD_QUAL>	*Bad quality time*
<TR_CH_BLER> … </TR_CH_BLER>	*Transport channel BLER*
<T_THR_CELL> … </T_THR_CELL>	*Total throughput per cell*
<T_INTERFER> … </T_INTERFER>	*Total interference at Node-B*
<LOAD_NEIG> … </LOAD_NEIG>	*Load in neighbourhood*
<T_TX_POWER> … </T_TX_POWER>	*Total Tx power in Node-B*
<NUM_US_CELL> … </NUM_US_CELL>	*Number of users served in a cell*
<AVER_LOSS> … </AVER_LOSS>	*Averaged loss*
<UL_TPC_TEN> … </UL_TPC_TEN>	*UL TPC tendencies*
<ALL_CODE> … </ALL_CODE>	*Allocated code*
<SOFT_HO_OH> … </SOFT_HO_OH>	*Soft/softer handover overhead*
<LU_RATE> … </LU_RATE>	*Location update rate*
</KPI >	

Table 34. KPI block

- USER block:

<USER>	
<imsi> … </imsi>	*IMSI number of user*
<ip_add> … </ip_add>	*MSISDN of user*
<tos> … </tos>	*Type of service*
</USER>	

Table 35. USER block

- Error_tag block:

<error_tag>
<tag> … </tag>
<position> … </position>
<line> … </line>
</error_tag>

Table 36. Error_tag block

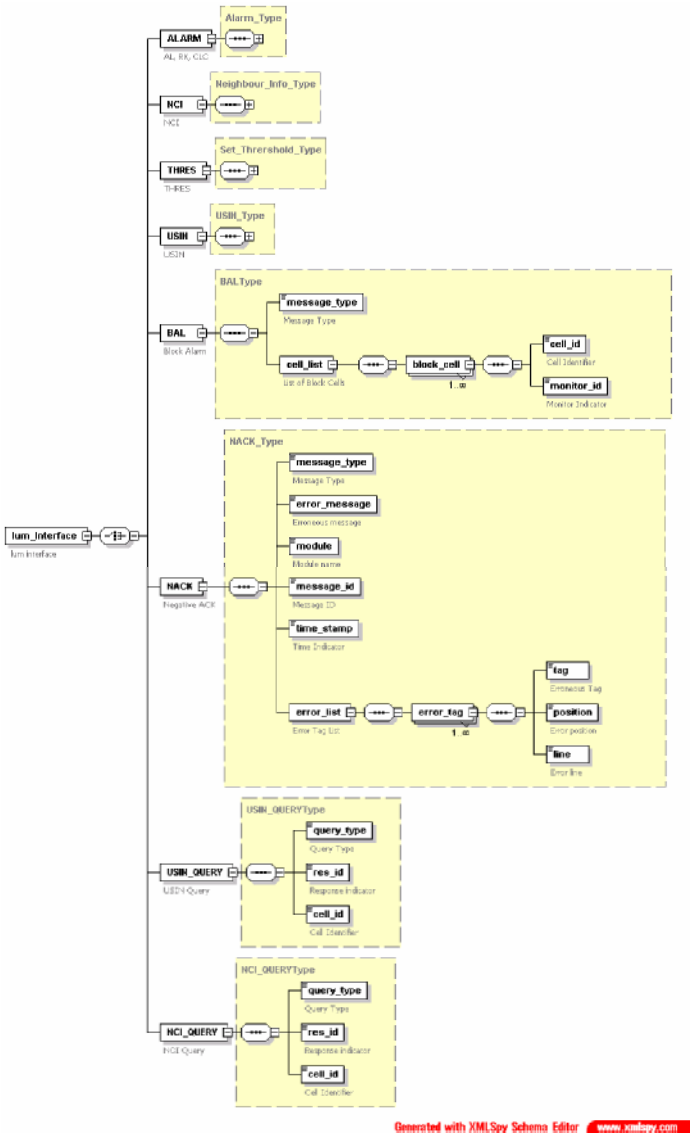


Figure 15. Ium interface

3.2.1.4 **Iw**: Interface between ITMUw and RMUw in WLAN network

The XML generic structure for the messages belonging to interface Ium is listed in the following table

<?xml version="1.0" encoding="UTF-8" ?>	
<Iw_Interface>	
<NCI> … </NCI>	*NCI block*
<ALARM> … </ALARM>	*Alarm block*
<THRES> … </THRES>	*Thresholds block*
<USIN> … </USIN>	*USIN block*
<BAL> … </BAL>	*BAL block*
<NACK> … </NACK>	*NACK block*
<USIN_QUERY> … </USIN_QUERY>	*USIN_QUERY block*
<NCI_QUERY> … </NCI_QUERY>	*NCI_QUERY block*
</Iw_Interface>	

Table 37. Iw generic message

When ITMU detects an overloaded resource (a KPI over the threshold), it raises an alarm to RMU. This alarm contains all the data of the congested resource of the congested cell. So RMU is provided with a snapshot of the overall congestion situation. The alarm is periodically sent until the resource drops back to normal operation. The format of the alarm message is showed in the following table:

<ALARM>	
<alarm_type> … </alarm_type>	*Values: AL, RX, CLC*
<ap_id> … </ap_id>	*Affected AP IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<KPI> … </KPI>	*KPI block*
</ALARM>	

Table 38. Alarm message

When RMU receives the alarm, it might not be able to map the information into a particular scenario, or it requires a better view of the system traffic prior the selection of the appropriate command. Therefore, RMU will request the data of neighbour cells, in order to decide about the area that is affected from the traffic overload. This RMU query has the following XML structure:

<NCI_QUERY>	
<query_type> … </query_type>	*NCI_QUERY*
<res_id> … </res_id>	*Response indicator*
<ap_id> … </ap_id>	*Queried AP IDs*
</NCI_QUERY>	

Table 39. NCI request message

The ITMU answer to the previous query has the following XML structure:

<NCI>	
<message_type> … </message_type>	*Value: NCI*
<ap_id> … </ap_id>	*Queried AP IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<res_id> … </res_id>	*Response indicator*
<KPI> … </KPI>	*KPI block*
</NCI>	

Table 40. NCI response message

In some circumstances, RMU requests from ITMU to change the alarm threshold values. This is achieved by sending a special threshold change command to ITMU. This command has the following structure regarding the ITMU and network type.

<THRES>	
<message_type> … </message_type>	*Value: THRES*
<ap_id> … </ap_id>	*Affected AP IDs*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<DURATION> … </DURATION>	*Duration of change*
<KPI> … </KPI>	*KPI block*
</THRES>	

Table 41. Change thresholds message

RMU can request ITMU for information about the users attached to a certain cell. This command has the following structure:

<USIN_QUERY>	
<query_type> … </query_type>	*Value: USIN_QUERY*
<res_id> … </res_id>	*Response indicator*
<ap_id> … </ap_id>	*Affected AP IDs*
</USIN_QUERY>	

Table 42. User information request message

ITMU response to the previous command has the following structure:

<USIN>	
<message_type> … </message_type>	*Value: USIN*
<ap_id> … </ap_id>	*Affected AP IDs*
<message_id> … </message_id>	*Message ID*
<module> … </module>	*Values: ITMUa, ITMUp, ITMUum, ITMUw*
<res_id> .. </res_id>	*Response indicator*
<time_stamp> … </time_stamp>	*Time stamp*
<date_stamp> … </time_stamp>	*Date stamp*
<USER_LIST>	*USER_List block*
<USER> ... </USER>	*USER blocks*
</USER_LIST>	
</USIN>	

Table 43. User information response message

In case that RMU wants to stop ITMU monitoring for a cell, a special command is needed. This command has the following XML structure:

<BAL>	
<message_type> … </message_type>	*Value: BAL*
<ap_list>	*AP_List block*
<block_ap> ... </block_cell>	*Block_ap blocks*
</ap_list>	
</BAL>	

Table 44. BAL message

If RMU has to report ITMU about any error concerning the communication protocol, it uses the following message:

<NACK>	
<message_type> … </message_type>	*Value: NACK*
<error_message> … </error_message>	
<module> … </module>	*Values: ITMUa, ITMUp, ITMUum, ITMUw*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<error_list>	*Error_List block*
<error_tag> ... </error_tag>	*Error_tag blocks*
</error_list>	
</NACK>	

Table 45. NACK message

The XML blocks mentioned above are described in the following tables:

- KPI block:

<KPI>	
<DELAY> … </DELAY>	*Latency*
<JITTER> … </JITTER>	*Jitter*
<AVAIL> … </AVAIL>	*Availability*
<ERRORS> … </ERRORS>	*Errors*
<P_LOSS> … </P_LOSS>	*Packet loss*
<PEAK_US_THR> … </PEAK_US_THR>	*Peak user throughput*
<MEAN_US_THR> … </MEAN_US_THR>	*Mean user throughput*
</KPI>	

Table 46. KPI block

- USER block:

<USER>	
<mac_add> … </mac_add>	*MAC address of user*
<ip_add> … </ip_add>	*IP address of user*
<tos> … </tos>	*Type of service*
</USER>	

Table 47. USER block

- Block_cell block:

<block_cell>	
<ap_id> … </ap_id>	*Affected AP IDs*
<monitor_id> … </monitor_id>	*Monitor indicator*
</block_cell>	

Table 48. Block_cell block

- Error_tag block:

<error_tag>
<tag> … </tag>
<position> … </position>
<line> … </line>
</error_tag>

Table 49. Error_tag block

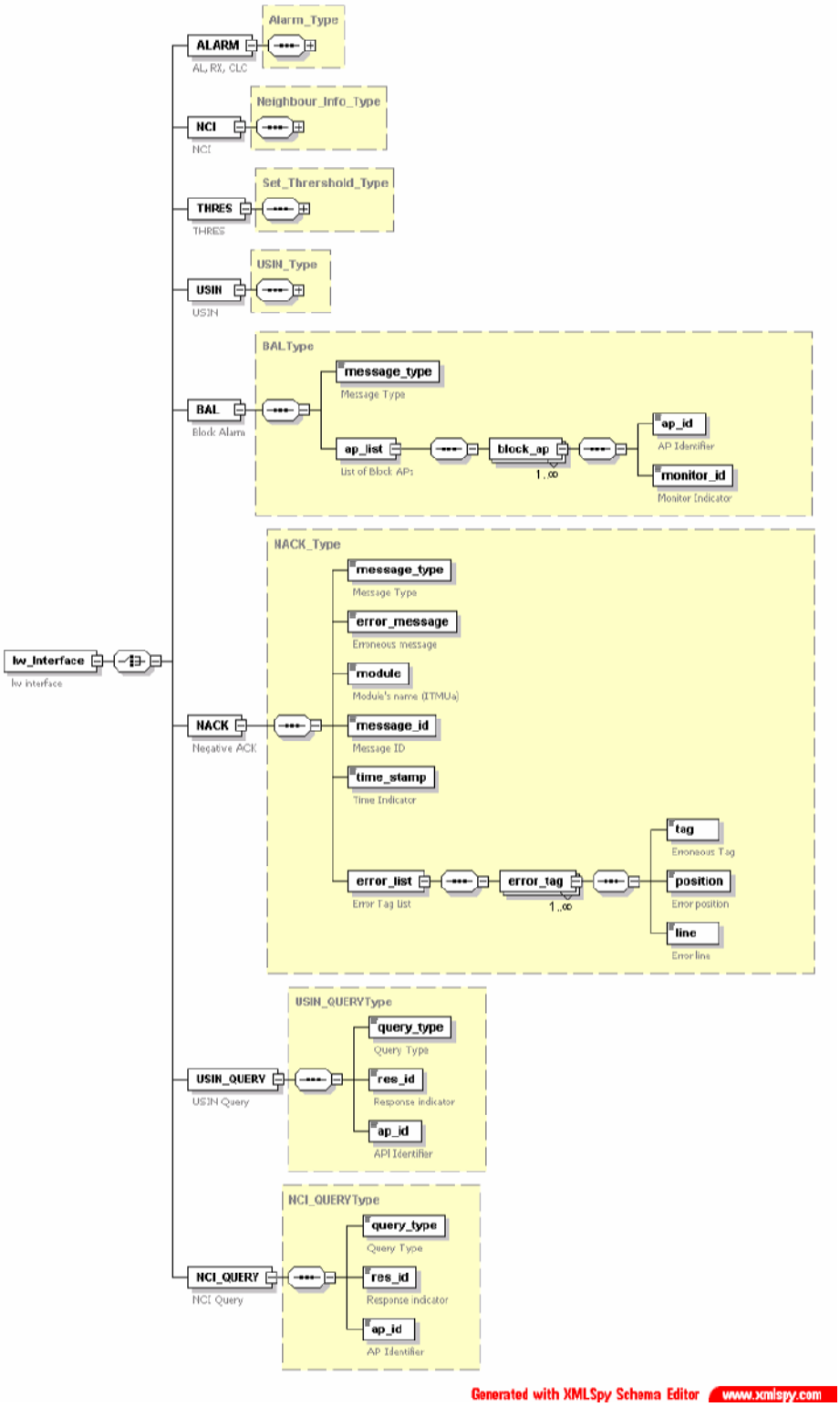


Figure 16. Iw interface

3.2.2 Interfaces between RMUs and GMU

GMRx are the internal interfaces between RMUx nodes and GMU. When a RMU decides that is unable to solve a congestion situation, they report to GMU, via the corresponding GMRx interface, the situation of the underlying network, asking for potential help (mainly, vertical and vertical-vertical handover commands). GMU, which is the highest-level component of CAUTION++ system, has the task of optimizing the behaviour of all monitored networks in congestion situation, and is responsible for vertical handover (i.e. from GPRS to WLAN) and vertical-vertical handover (i.e. from WLAN operator 1 to WLAN operator 2) commands. For that reason, GMU should have a clear view and the superintendence of all RMUs, in order to collect information and details for all access networks. GMU queries RMUs for the congested areas of each network, the network availability (in order to decide for a handover), the kind of the provided service (voice or data), or the available bandwidth. The GMRx interfaces are Ethernet connections, TCP/IP based.

- **GMRap:** Interface between RMUap and GMU in GSM/GPRS network
- **GMRUM:** Interface between RMUum and GMU in UMTS network
- **GMRw:** Interface between RMUw and GMU in WLAN network

The XML generic structure for the messages belonging to interfaces GMRx is listed in the following table:

<?xml version="1.0" encoding="UTF-8" ?>	
<MESSAGE>	
<USIN> … </USIN>	*USIN block*
<USIN_QUERY> … </USIN_QUERY>	*USIN_QUERY block*
<ALARM> … </ALARM>	*Alarm block*
<QUERY_NETP> … </QUERY_NETP>	*QUERY_NETP block*
<QUERY_NETP_RES> … </QUERY_NETP_RES>	*QUERY_NETP_RES block*
<RMT_NTF> … </RMT_NTF>	*RMT_NTF block*
<RMT_NTF_REQ> … </RMT_NTF_REQ>	*RMT_NTF_REQ block*
<RMT_PERM_RES> … </RMT_PERM_RES>	*RMT_PERM_RES block*
<RMT_APPLY> … </RMT_APPLY>	*RMT_APPLY block*
<NACK> … </NACK>	*NACK block*
</MESSAGE>	

Table 50. GMRx generic message

When a RMU evaluates that cannot treat successfully a congestion scenario, then it starts transmitting alarm messages to GMU. These kinds of messages describe the identified Traffic Load Scenario with its related KPIs. When the traffic in the affected areas returns to normal values, a relax alarm is reported to GMU.

The format of these messages is showed in the following table:

<ALARM>	
<TYPE> … </TYPE>	*Values: AL, RX*
<MESSAGE_ID> … </MESSAGE_ID>	*Message ID*
<MODULE> … </MODULE>	*Values: RMUap, RMUum, RMUw*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TLS_ID> … </TLS_ID>	*Traffic Load Scenario ID*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<PER_TRAFF> … </PER_TRAFF>	*Traffic percentage to be moved*
<KPI_UMTS> … </KPI_UMTS>	*KPI_UMTS block*
<KPI_WLAN> … </KPI_WLAN >	*KPI_WLAN block*
<KPI_GSM> … </KPI_GSM >	*KPI_GSM block*
<KPI_GPRS> … </KPI_GPRS >	*KPI_GPRS block*
</ALARM>	

Table 51. Alarm message

After receiving the alarm, GMU requests RMU for information about the active users located in the congestion area. This command has the following structure:

<USIN_QUERY>	
<TYPE> … </TYPE>	*Value: USIN_QUERY*
<USIN_QUERY_ID> … </USIN_QUERY_ID>	*Message ID*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
</USIN_QUERY>	

Table 52. User information request message

RMU response to the previous command has the following structure:

<USIN>	
<TYPE> … </TYPE>	*Value: USIN*
<MESSAGE_ID> … </MESSAGE_ID>	*Message ID*
<MODULE> … </MODULE>	*Values: RMUap, RMUum, RMUw*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<USER_LIST>	*USER_List block*
<USER> ... </USER>	*USER blocks*
</USER_LIST>	
</USIN>	

Table 53. User information response message

GMU identifies which RMUs are attached to the congested area, and then requests them for real-time information about the availability of network resources, and for network parameters needed to feed its own business models.

The format of this request is the following:

<QUERY_NETP>	
<TYPE> … </TYPE>	*Value: QUERY_NETP*
<QUERY_NETP_ID> … </QUERY_NETP_ID>	*Message ID*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
</QUERY_NETP>	

Table 54. Network parameters request message

RMUs responses to the previous command have the following structure:

<QUERY_NETP_RES>	
<TYPE> … </TYPE>	*Value: QUERY_NETP_RES*
<MODULE> … </MODULE>	*Values: RMUap, RMUum, RMUw*
<QUERY_NETP_RES_ID> … </QUERY_NETP_RES_ID>	*Message ID*
<QUERY_NETP_ID> … </QUERY_NETP_ID>	*Request Message ID*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<GSM>	*GSM parameters block*
<RES_BW> … </RES_BW>	*Residual bandwidth*
<COST> … </COST>	*Cost*
<KPI_GSM> … </KPI_GSM >	*KPI_GSM block*
</GSM>	
<GPRS>	*GPRS parameters block*
<RES_BW> … </RES_BW>	*Residual bandwidth*
<COST> … </COST>	*Cost*
<KPI_GPRS> … </KPI_GPRS >	*KPI_GPRS block*
</GPRS>	
<UMTS>	*UMTS parameters block*
<RES_BW> … </RES_BW>	*Residual bandwidth*
<COST> … </COST>	*Cost*
<KPI_UMTS> … </KPI_UMTS >	*KPI_UMTS block*
</UMTS>	
<WLAN>	*WLAN parameters block*
<RES_BW> … </RES_BW>	*Residual bandwidth*
<COST> … </COST>	*Cost*
<KPI_WLAN> … </KPI_WLAN >	*KPI_WLAN block*
</WLAN>	
</QUERY_NETP_RES>	

Table 55. Network parameters response message

RMU should also notify the GMU about the applied RMTs and the last time it was involved with such technique. This notification has the following structure:

<RMT_NTF>	
<TYPE> … </TYPE>	*Value: RMT_NTF*
<MODULE> … </MODULE>	*Values: RMUap, RMUum, RMUw*
<RMT_NTF_ID> … </RMT_NTF_ID>	*Message ID*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TLS_ID> … </TLS_ID>	*Traffic Load Scenario ID*
<RMT_LIST>	*RMT_List block*
<RMT> … </RMT>	*RMT blocks*
</RMT_LIST>	
</RMT_NTF>	

Table 56. Notification message

Some of the resource management techniques affordable by RMU (e.g. cell breathing techniques) may vary the coverage area of a cell or AP and reduce the overlapping areas among RATs. In such cases the RMU must ask permission to the GMU before applying those RMTs.

The format of this request is the following:

<RMT_PERM_REQ>	
<TYPE> … </TYPE>	*Value: RMT_PERM_REQ*
<MODULE> … </MODULE>	*Values: RMUap, RMUum, RMUw*
<RMT_PERM_REQ_ID> … </RMT_PERM_REQ_ID>	*Message ID*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TLS_ID> … </TLS_ID>	*Traffic Load Scenario ID*
<RMT_LIST>	*RMT_List block*
<RMT> … </RMT>	*RMT blocks*
</RMT_LIST>	
</RMT_PERM_REQ>	

Table 57. Permission request message

The response of GMU to such requests is the following:

<RMT_PERM_RES>	
<TYPE> … </TYPE>	*Value: RMT_PERM_RES*
<RMT_PERM_RES_ID> … </RMT_PERM_RES_ID>	*Message ID*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TLS_ID> … </TLS_ID>	*Traffic Load Scenario ID*
<RMT_LIST>	*RMT_List block*
<RMT> … </RMT>	*RMT blocks*
</RMT_LIST>	
</RMT_PERM_RES>	

Table 58. Permission response message

GMU can also command a single RMU to apply specific RMTs that facilitate the handover processes. This command has the following structure:

<RMT_APPLY>	
<TYPE> … </TYPE>	*Value: RMT_APPLY*
<MODULE> … </MODULE>	*Values: RMUap, RMUum, RMUw*
<RMT_APPL_ID> … </RMT_APPL_ID>	*Message ID*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<CELL_ID> … </CELL_ID>	*Affected cells IDs*
<TLS_ID> … </TLS_ID>	*Traffic Load Scenario ID*
<RMT_LIST>	*RMT_List block*
<RMT> … </RMT>	*RMT blocks*
</RMT_LIST>	
</RMT_APPLY>	

Table 59. Application request message

If GMU has to report RMU about any error concerning the communication protocol, it uses the following message:

<NACK>	
<message_type> … </message_type>	*Value: NACK*
<error_message> … </error_message>	
<module> … </module>	*Values: RMUap, RMUum, RMUw*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<error_list>	*Error_List block*
<error_tag> ... </error_tag>	*Error_tag blocks*
</error_list>	
</NACK>	

Table 60. NACK message

The XML blocks mentioned above are described in the following tables:

- USER block:

<USER>	
<USER_ID> … </USER_ID>	*IMSI number of user*
<IP_ADD> … </IP_ADD>	*IP address*
<MAC_ADD> … </MAC_ADD>	*MAC address (only in WLAN)*
<TOS> … </TOS>	*Type of service*
</USER>	

Table 61. USER block

- KPI_UMTS block:

<KPI_UMTS>	
<DELAY> … </DELAY>	*Delay*
<PEAK_THR> … </PEAK_THR>	*Peak throughput*
<MEAN_THR> … </MEAN_THR>	*Mean throughput*
<CH_M_THR> … </CH_M_THR>	*Change of mean throughput*
<HARD_DR> … </HARD_DR>	*Hard dropping*
<SOFT_DR> … </SOFT_DR>	*Soft dropping*
<HARD_BL> … </HARD_BL>	*Hard blocking*
<SOFT_BL> … </SOFT_BL>	*Soft blocking*
<UNSATIS> … </UNSATIS>	*Unsatisfied*
<BAD_QUAL> … </BAD_QUAL>	*Bad quality time*
<TR_CH_BLER> … </TR_CH_BLER>	*Transport channel BLER*
<T_THR_CELL> … </T_THR_CELL>	*Total throughput per cell*
<T_INTERFER> … </T_INTERFER>	*Total interference at Node-B*

<LOAD_NEIG> … </LOAD_NEIG>	*Load in neighbourhood*
<T_TX_POWER> … </T_TX_POWER>	*Total Tx power in Node-B*
<NUM_US_CELL> … </NUM_US_CELL>	*Number of users served in a cell*
<AVER_LOSS> … </AVER_LOSS>	*Averaged loss*
<UL_TPC_TEN> … </UL_TPC_TEN>	*UL TPC tendencies*
<ALL_CODE> … </ALL_CODE>	*Allocated code*
<SOFT_HO_OH> … </SOFT_HO_OH>	*Soft/softer handover overhead*
<LU_RATE> … </LU_RATE>	*Location update rate*
</KPI_UMTS>	

Table 62. KPI_UMTS block

- KPI_WLAN block:

<KPI_WLAN>	
<DELAY> … </DELAY>	*Latency*
<JITTER> … </JITTER>	*Jitter*
<AVAIL> … </AVAIL>	*Availability*
<ERRORS> … </ERRORS>	*Errors*
<P_LOSS> … </P_LOSS>	*Packet loss*
<PEAK_US_THR> … </PEAK_US_THR>	*Peak user throughput*
<MEAN_US_THR> … </MEAN_US_THR>	*Mean user throughput*
</KPI_WLAN>	

Table 63. KPI_WLAN block

- KPI_GSM block:

<KPI_GSM>	
<TCH_UT> … </TCH_UT>	*TCH utilization*
<SDDCH_UT> … </SDDCH_UT>	*SDDCH utilization*
<SACCH_UT> … </SACCH_UT>	*SACCH utilization*
<PCH_UT> … </PCH_UT>	*PCH utilization*
<AGCH_UT> … </AGCH_UT>	*AGCH utilization*
<RACH_UT> … </RACH_UT>	*RACH utilization*
<TCH_BR> … </TCH_BR>	*TCH blocking rate*
<SDCCH_BR> … </SDCCH_BR>	*SDCCH blocking rate*
<EC_NO> … </EC_NO>	*Number of emergency calls*
<CLC_NO> … </CLC_NO>	*Number of not-normal clear codes*
</KPI_GSM>	

Table 64. KPI_GSM block

- KPI_GPRS block:

<KPI_GPRS>	
<DC_SUCC> … </DC_SUCC>	*Data connection success rate*
<SR_SUCC> … </SR_SUCC>	*Session release success rate*
<DELAY> … </DELAY>	*Delay*
<PEAK_THR> … </PEAK_THR>	*Peak throughput*
<MEAN_THR> … </MEAN_THR>	*Mean throughput*
<UTIL> … </UTIL>	*GPRS utilization*
<ATT_FR> … </ATT_FR>	*Attach attempts failure ratio*
</KPI_GPRS>	

Table 65. KPI_GPRS block

- RMT block:

<RMT>	
<RMT_ID> … </RMT_ID>	*RMT ID*
<RMT_PARAM> … </RMT_PARAM>	*RMT parameters*
</RMT>	

Table 66. RMT block

- Error_tag block:

<error_tag>
<tag> … </tag>
<position> … </position>
<line> … </line>
</error_tag>

Table 67. Error_tag block

3.2.3 Interfaces between different GMUs

The interface between GMUs of different operators is named **R** (it stands for ”roaming”). The first objective of R interface is the authentication between different GMUs, in order to be able to communicate and exchange further information. Assuming that authentication is successful and GMU_1 is not able to decongest a congested phenomenon, is sending queries to another authenticated GMU (i.e. GMU_2) providing detailed info with the location of the congestion. GMU_2 answer can be positive or negative both for the coverage of the congested area and for the availability of resources in this area. If both answers are positive, a vertical-vertical handover can take place. R interface is also a TCP/IP connection over Ethernet.

The XML generic structure for the messages belonging to interface R is listed in the following table:

<?xml version="1.0" encoding="UTF-8" ?>	
<MESSAGE>	
<GUSIN> … </GUSIN>	*GUSIN block*
<GUSIN_ACK> … </GUSIN_ACK>	*GUSIN_ACK block*
<HELP_REQ> … </HELP_REQ>	*HELP_REQ block*
<HELP_REQ_ACK> … </HELP_REQ_ACK>	*HELP_REQ_ACK block*
<NACK> … </NACK>	*NACK block*
</MESSAGE>	

Table 68. R generic message

When a GMU is dealing with a congestion situation that cannot be adequately treated with its own resources, it tries to pass some users to other operators. The GMU evaluates the amount and kind of traffic to be moved by applying a business model with the proper value-structure. Then the GMU determines the other GMUs involved in the problematic area and starts offering them, in turn, the exceeding traffic. A GMU will offer traffic to another GMU by sending several HELP_REQUEST messages, one for each service type. An HELP_REQUEST message details the amount of users to be handled by the target GMU, the type of service they are currently using, the type of access network they are attached to, the traffic load scenario, and the congested area. The message structure is described below:

<HELP_REQ>	
<TYPE> … </TYPE>	*Value: HELP_REQ*
<HELP_REQ_ID> … </HELP_REQ_ID>	*Message ID*
<OPERATOR_ID> … </OPERATOR_ID>	*Operator identifier*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<LOCATION> … </LOCATION>	*LOCATION block*
<USER_LIST>	*USER_List block*
<N_USERS> ... </N_USERS>	*N_USERS blocks*
</USER_LIST>	
</HELP_REQ>	

Table 69. Help request message

A target GMU will respond to each the HELP_REQUEST messages by indicating the number of users it accepts to accommodate. A number of users equal to 0 will be returned if the target GMU is rejecting the request for that type of service.

In case the target GMU has accepted all or part of the offered traffic, it will deliver to the offering GMU information the number of accepted users and the mode can be served. Finally the handshaking procedure will start enabling a vertical-vertical handover.

The structure of this response is the following:

<HELP_REQ_ACK>	
<TYPE> … </TYPE>	*Value: HELP_REQ_ACK*
<HELP_REQ_ID> … </HELP_REQ_ID>	*Message ID*
<OPERATOR_ID> … </OPERATOR_ID>	*Operator identifier*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<N_USERS_ACK> … </N_USERS_ACK>	*Number of accepted users*
</HELP_REQ_ACK>	

Table 70. Help request ACK message

After the target GMU accepts the number of users attached to a certain service, the offering GMU starts sending user information messages to its peer GMU in order to authenticate and enable the vertical-vertical handover. This message has the following structure:

<GUSIN>	
<TYPE> … </TYPE>	*Value: GUSIN*
< GUSIN _ID> … </ GUSIN _ID>	*Message ID*
<HELP_REQ_ID> … </HELP_REQ_ID>	*Original message ID*
<OPERATOR_ID> … </OPERATOR_ID>	*Operator identifier*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<USER_LIST>	*USER_List block*
<N_USERS> ... </N_USERS>	*N_USERS blocks*
</USER_LIST>	
</GUSIN>	

Table 71. GMU user information message

The responses of the destination GMU have the following structure:

<GUSIN_ACK>	
<TYPE> … </TYPE>	*Value: GUSIN_ACK*
<GUSIN_ID> … </GUSIN_ID>	*Message ID*
<HELP_REQ_ID> … </HELP_REQ_ID>	*Original message ID*
<OPERATOR_ID> … </OPERATOR_ID>	*Operator identifier*
<TIME_IND> … </TIME_IND>	*Time stamp*
<DATE_IND> … </DATE_IND>	*Date stamp*
<USER_LIST>	*USER_List block*
<N_USERS> ... </N_USERS>	*N_USERS blocks*
</USER_LIST>	
</GUSIN_ACK>	

Table 72. GMU user information ACK message

If one GMU has to report the other about any error concerning the communication protocol, it uses the following message:

<NACK>	
<message_type> … </message_type>	*Value: NACK*
<error_message> … </error_message>	
<module> … </module>	*Values: RMUap, RMUum, RMUw*
<message_id> … </message_id>	*Message ID*
<time_stamp> … </time_stamp>	*Time stamp*
<error_list>	*Error_List block*
<error_tag> ... </error_tag>	*Error_tag blocks*
</error_list>	
</NACK>	

Table 73. NACK message

The XML blocks mentioned above are described in the following tables:

- N_USERS block:

<N_USERS>	
<IP_ADD> … </IP_ADD>	*IP address*
<MAC_ADD> … </MAC_ADD>	*MAC address (WLAN only)*
<TOS> … </TOS>	*Type of service*
</N_USERS>	

Table 74. N_ USER block

- LOCATION block:

<LOCATION>	
<NORTH> … </NORTH>	*North coordinate of user*
<EAST> … </EAST>	*East coordinate of user*
</LOCATION >	

Table 75. LOCATION block

- Error_tag block:

<error_tag>
<tag> … </tag>
<position> … </position>
<line> … </line>
</error_tag>

Table 76. Error_tag block

3.2.4 Other internal interfaces

In this section, any other internal interfaces apart from the previously described are outlined. Figure 17 describes the additional internal Interfaces of CAUTION++ components.

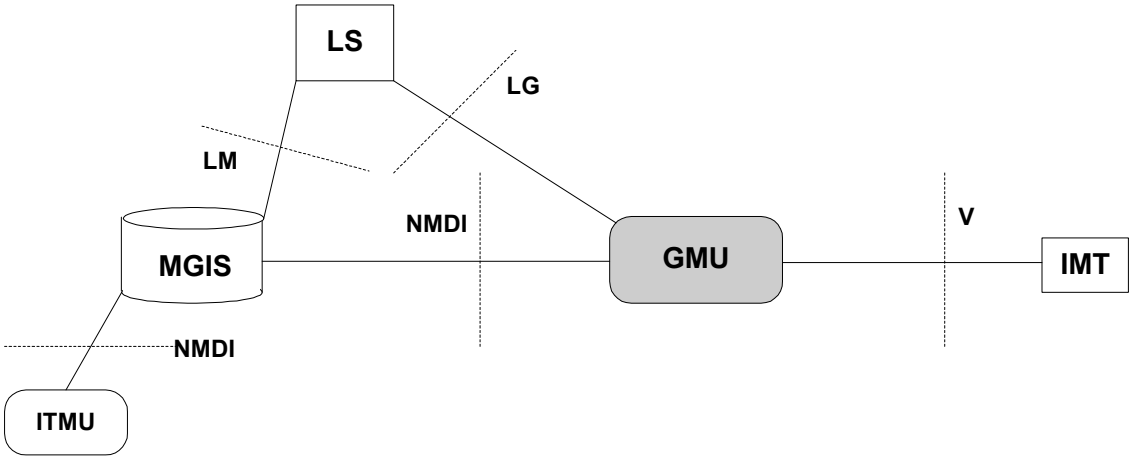


Figure 17. Additional external Interfaces

These interfaces are:

- **V**: ”virtual” interface for the communication between GMU and IMT and is IP based for GPRS, UMTS and WLAN. Communication via SMS is potential in case of GSM network.
- **LG**: interface between GMU and LS. Via LG interface, GMU can retrieve from LS the location of a user.
- **LM**: interface between LS and MGIS. Through it, MGIS can look up LS to retrieve further information about the location of the user.
- **NMDI** interface between MGIS and GMU. NMDI interface can be used by MGIS (towards ITMU or GMU), in order to collect and store real-time information about the status of the networks. GMU can also send queries to MGIS, in order to be informed about statistical information.

3.2.4.1 Interface V:

Interface V is the ”virtual” interface for the communication between GMU and IMT and is IP based for GPRS, UMTS and WLAN. Communication via SMS is potential in case of GSM network.

- Requests from IMT to GMU
  - **Network information:** Both normal users and super users has the capability to request GMU for assistance when trying to establish a communication upon the existing access network. This assistance includes a request for information about resource availability and costs to initiate a certain service. The XML structure of this request is shown in the following table:

<?xml version="1.0" encoding="UTF-8" ?>	
<NET_STATUS>	
<MAC> … </MAC>	*MAC address of user*
<NET> … </NET>	*Target network ID*
<SERVICE> … </SERVICE>	*Desired service*
<D_RATE> … </D_RATE>	*Minimum desired data rate*
<COST> … </COST>	*Maximum desired cost*
<AUTO_ASSIGN> … </AUTO_ASSIGN>	*Auto assign indicator*
</NET_STATUS>	

Table 77. Network Status Request

  - **Cell information:** Only super users may request specific cell status from GMU. The XML structure is as follows:

<?xml version="1.0" encoding="UTF-8" ?>	
<CELL_STATUS>	
<MAC> … </MAC>	*MAC address of user*
<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
</CELL_STATUS>	

Table 78. Cell Status Request

- **RMT execution:** Only super users may request GMU to execute a specific Resource Management Technique over a certain cell. The XML structure is shown in the following table:

<?xml version="1.0" encoding="UTF-8" ?>	
<RMT_EXEC>	
<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<RMT>	*RMT block*
<ID> … </ID>	*RMT identifier*
<PARAMETERS> … </PARAMETERS>	*RMT parameters*
</RMT>	
</RMT_EXEC>	

Table 79. RMT Execution Request

- Responses from GMU to IMT
  - **Network information:** The response from GMU to IMT request has the following format, both for normal users and super users:

<?xml version="1.0" encoding="UTF-8" ?>	
<NET_STATUS>	
<NET>	*Net block*
<NAME> … </NAME>	*Network name*
<SERVICE> … </SERVICE>	*Available service*
<D_RATE> … </D_RATE>	*Available data rate*
</NET>	
<COST> … </COST>	*Service cost*
<AUTO_ASSIGN> … </AUTO_ASSIGN>	*Auto assign indicator*
</NET_STATUS>	

Table 80. Network Status Response

- **Cell information:** The response from GMU to IMT request has the following format (only for super users):
  - *GSM Networks*

<?xml version="1.0" encoding="UTF-8" ?>

<CELL_STATUS>	
<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<TIME> … </TIME>	*Time stamp*
<DATE> … </DATE>	*Date stamp*
<TCH_UT> … </TCH_UT>	*TCH utilization*
<SDCCH_UT> … </SDCCH_UT>	*SDDCH utilization*
<SACCH_UT> … </SACCH_UT>	*SACCH utilization*
<PCH_UT> … </PCH_UT>	*PCH utilization*
<AGCH_UT> … </AGCH_UT>	*AGCH utilization*
<RACH_UT> … </RACH_UT>	*RACH utilization*
<TCH_BR> … </TCH_BR>	*TCH blocking rate*
<SDCCH_BR> … </SDCCH_BR>	*SDCCH blocking rate*
<EC_NO> … </EC_NO>	*Number of emergency calls*
<CLC_NO> … </CLC_NO>	*Number of not-normal clear codes*
</CELL_STATUS>	

Table 81. GSM Cell Status Response

  - *GPRS Networks*

<?xml version="1.0" encoding="UTF-8" ?>

<CELL_STATUS>	
<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<TIME> … </TIME>	*Time stamp*
<DATE> … </DATE>	*Date stamp*
<RES_ID> … </RES_ID>	*Resource identifier*
<DC_SUCC> … </DC_SUCC>	*Data connection success rate*
<SR_SUCC> … </SR_SUCC>	*Session release success rate*
<DELAY> … </DELAY>	*Delay*
<PEAK_THR> … </PEAK_THR>	*Peak throughput*

<MEAN_THR> … </MEAN_THR>	*Mean throughput*
<UTIL> … </UTIL>	*GPRS utilization*
<ATT_FR> … </ATT_FR>	*Attach attempts failure ratio*
</CELL_STATUS>	

Table 82. GPRS Cell Status Response

- *UMTS Networks*

<?xml version="1.0" encoding="UTF-8" ?>

<CELL_STATUS>	
<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<TIME> … </TIME>	*Time stamp*
<DATE> … </DATE>	*Date stamp*
<DELAY> … </DELAY>	*Delay*
<PEAK_THR> … </PEAK_THR>	*Peak throughput*
<MEAN_THR> … </MEAN_THR>	*Mean throughput*
<CH_M_THR> … </CH_M_THR>	*Change of mean throughput*
<HARD_DR> … </HARD_DR>	*Hard dropping*
<SOFT_DR> … </SOFT_DR>	*Soft dropping*
<HARD_BL> … </HARD_BL>	*Hard blocking*
<SOFT_BL> … </SOFT_BL>	*Soft blocking*
<UNSATIS> … </UNSATIS>	*Unsatisfied*
<BAD_QUAL> … </BAD_QUAL>	*Bad quality time*
<TR_CH_BLER> … </TR_CH_BLER>	*Transport channel BLER*
<T_THR_CELL> … </T_THR_CELL>	*Total throughput per cell*
<T_INTERFER> … </T_INTERFER>	*Total interference at Node-B*
<LOAD_NEIG> … </LOAD_NEIG>	*Load in neighbourhood*
<T_TX_POWER> … </T_TX_POWER>	*Total Tx power in Node-B*
<NUM_US_CELL> … </NUM_US_CELL>	*Number of users served in a cell*
<AVER_LOSS> … </AVER_LOSS>	*Averaged loss*
<UL_TPC_TEN> … </UL_TPC_TEN>	*UL TPC tendencies*
<ALL_CODE> … </ALL_CODE>	*Allocated code*
<TIME_UTIL> … </TIME_UTIL>	*Utilisation time*
<SOFT_HO_OH> … </SOFT_HO_OH>	*Soft/softer handover overhead*
<LU_RATE> … </LU_RATE>	*Location update rate*
</CELL_STATUS>	

Table 83. UMTS Cell Status Response

- *WLAN Networks*

<?xml version="1.0" encoding="UTF-8" ?>

<CELL_STATUS>

<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<TIME> … </TIME>	*Time stamp*
<DATE> … </DATE>	*Date stamp*
<DELAY> … </DELAY>	*Latency*
<JITTER> … </JITTER>	*Jitter*
<AVAIL> … </AVAIL>	*Availability*
<ERRORS> … </ERRORS>	*Errors*
<P_LOSS> … </P_LOSS>	*Packet loss*
<PEAK_US_THR> … </PEAK_US_THR>	*Peak user throughput*
<MEAN_US_THR> … </MEAN_US_THR>	*Mean user throughput*

</CELL_STATUS>

Table 84. WLAN AP Status Response

- **RMT execution:** The response from GMU to IMT request has the following format (only for super users):

<?xml version="1.0" encoding="UTF-8" ?>

<RMT_EXEC>

<NET> … </NET>	*Target network ID*
<MSC> … </MSC>	*Target MSC*
<BSC> … </BSC>	*Target BSC*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<RMT>	*RMT block*
<ID> … </ID>	*RMT identifier*
<PARAMETERS> … </PARAMETERS>	*RMT parameters*
<EXECUTED> … </EXECUTED>	*Execution indicator*

</RMT>

</RMT_EXEC>

Table 85. RMT Execution Response

- **Handover command:** GMU can force an IMT (normal and super users) to perform a vertical or a vertical-vertical handover. The format of this command is shown below:

<?xml version="1.0" encoding="UTF-8" ?>	
<VHO>	
<NEW_NET>	*New target network block*
<NAME> … </NAME>	*Network name*
<INFO>	*Network iInformation block*
<CID_APID> … </CID_APID>	*Target Cell or AP ID*
<WEP_KEY> … </WEP_KEY>	*WEP encryption key*
</INFO>	
</NEW_NET>	
</VHO>	

Table 86. Vertical Handover IMT Command

3.2.4.2 Interface LG

The interface between location server and GMU is called LG. This interface is meant to enable GMU to retrieve from LS information related to users' location. The query to LS provides user location and estimated location accuracy as a result.

The detailed specification of the interfacing parameters is shown below.

- Request from GMU to LS
  - **GSM and GPRS Networks:** The parameters needed to request users' location information are shown in the following table:

Operator	*Name of GSM/GPRS operator*
Location method	*DCM, Signal Strength or Cell ID*
Serving Cell parameters	*Parameters block for serving cell*
BSIC	*BSIC code*
Carrier	
Rx Level	
Neighbour Cell parameters	*Parameters block for neighbour cells*
BSIC	*BSIC code*
Carrier	
Rx Level	

Table 87. LS request for GSM/GPRS networks

  - **UMTS Networks:** The parameters needed to request users' location information are shown in the following table:

Operator	*Name of UMTS operator*
Location method	*DCM, Signal Strength or Cell ID*
Cell parameters	*Parameters block for available cells*
Cell type	*Type of cell*
Cell ID	*Cell identity*
Path loss	

Table 88. LS request for UMTS networks

- **WLAN Networks:** The parameters needed to request users' location information are shown in the following table:

Operator	*Name of WLAN operator*
Location method	*DCM, Signal Strength or Cell ID*
Serving Cell parameters	*Parameters block for serving cell*
MAC	*MAC address*
Signal level	
Noise level	
Hearable Cell parameters	*Parameters block for hearable cells*
MAC	*MAC address*
Signal level	
Noise level	

Table 89. LS request for WLAN networks

- Response from LS to GMU

  The parameters sent by LS in the response to GMU are shown in the following table:

Location method	*DCM, Signal Strength or Cell ID*
Coordinate system	*Only WGS84 is supported*
Location parameters	*User geographical coordinates*
Location E	*East-West coordinate (X)*
Location N	*North-South coordinate (Y)*
Estimated accuracy	*Accuracy of location estimation*

Table 90. LS response

3.2.4.3 Interface LM

The interface between location server and MGIS is called LM. This interface is meant to enable MGIS to retrieve from LS information related to users' location. The queries to LS provide user location and estimated location accuracy as a result.

3.2.4.4 Interface NMDI

Interface NMDI is used for the communication between MGIS and ITMUs, as well as between MGIS and GMU. NMDI interface can be used by MGIS (towards ITMU or GMU), in order to collect and store real-time information about the status of the networks. GMU can also send queries to MGIS, in order to be informed about statistical information. NMDI interface is a standardization proposal by 3GPP including technical specifications.

REFERENCES

[1] M. Barbera, C. Barbero, P. Dal Zovo, F. Farinaccio, E. Gkrioustotis, S. Kyriazakos, I. Mura and G. Previti, “An Application of Case-Based Reasoning to the Adaptive Management of Wireless Networks”, European Conference on Case-Based Reasoning, Aberdeen, UK, September 2001

[2] CAUTION++ IST-2001-38229, D-3.1 System architecture definition

[3] CAUTION++ IST-2001-38229, D-3.2 Specifications of traffic monitoring components

[4] CAUTION++ IST-2001-38229, D-3.3 Specifications of resource management techniques

[5] CAUTION++ IST-2001-38229, D-3.4 Decision Making process Specifications

[6] CAUTION++ IST-2001-38229, D-3.7 Specifications of business models

