COGEU

FP7 ICT-2009.1.1

COgnitive radio systems for efficient sharing of TV white spaces

in EUropean context

D6.3

Spectrum-aware routing, transport protocols and negotiation protocols between players for secondary spectrum trading; System level simulation tool - Final

Contractual Date of Delivery to the CEC: November 2012

Actual Date of Delivery to the CEC: January 2013

Author(s): Athina Bourdena (AEGEAN), George Kormentzas (AEGEAN), George Mastorakis (AEGEAN), Evangelos Pallis (AEGEAN), Paulo Marques (IT), Jonathan Rodriguez (IT), João Gonçalves (IT), José Cardoso (IT), Damien Lavaux (THALES).

Participant(s): AEGEAN, THALES, IT

Work package: WP6

Est. person months: 20 MM

Security: PU

Nature: Report

Version: 1.0

Total number of pages: 50

Abstract:

This Deliverable reports on the design, implementation and performance evaluation of networking protocols, i.e. signaling, routing and transport layer. More specifically, a signaling protocol was proposed, designed and implemented, facilitating the proper communication between COGEU geo-location database and secondary spectrum users (COGEU broker and WSDs). Furthermore, two spectrum aware routing protocols were designed, simulated and evaluated in the context of a Public Safety mesh networks. Finally, a transport layer protocol was designed, developed, and evaluated aiming at outperforming legacy TCP in terms of throughput, latency and resource consumption in Public Safety cognitive mesh networks.

Keyword list: Signalling protocols, spectrum aware routing protocols, transport layer protocols.

Executive Summary

This deliverable reports the final work performed in Tasks 6.2 “Spectrum-aware routing protocols”, 6.3 “Cognitive transport layer protocols” and 6.4 “Negotiation protocols between players for secondary spectrum trading” of WP6. More specifically, T6.2 elaborates on the design, development and performance evaluation of spectrum-aware routing protocols, capable to efficiently operate, among COGEU secondary users, facilitating the proper deployment of public safety networks over TVWS. The routing protocols proposed in this deliverable enable for the efficient transition of data between secondary users with heterogeneous spectrum availability, taking into account the absence of a Common Control Channel (CCC) and exploiting real TVWS results from Munich area, in Germany. Furthermore, T6.3 elaborates with the design, development and evaluation of a transport layer protocol, adopted in COGEU network architectures, facilitating efficient data transfer between TVWS devices forming a Cognitive Radio Ad-Hoc Network for a Public Safety use-case. Finally, T6.4 elaborates on the design and implementation of a protocol to access the TVWS (PAWS) database, which is able to establish the efficient and safe communication, among COGEU Spectrum Broker and geo-location database, in case of using a Spectrum Broker, or to establish secure communication among geo-location database with master devices, in case of spectrum of commons regime. Following, the key achievements of this deliverable are listed below:

- One of the IETF group is currently working on the definition of a protocol to access white spaces databases – PAWS (“Protocol for Communication between White Space Device and White Space Database”). Ofcom UK has also published a draft document on the definition of a similar protocol, including a detailed list of parameters to be exchanged between WSDs and a database. Ofcom solution is a protocol tailored for the UK scenario, with different requirements than the IETF proposal that is more comprehensive and less specific on details. Therefore, the IETF draft protocol and data model was chosen and considered flexible enough to be adapted for the COGEU model and its requirements.
- A signaling protocol “PAWS” modified for COGEU requirements is developed using a web-based environment. Several programming languages, from MySQL, PHP and JavaScript, were used to develop this implementation of COGEU-PAWS. Three services are defined and implemented on the interface between the geo-location database and WSDs: Registration, Channel List Request and ID Verification.
- To give a glimpse of the protocol implementation to the interested user, with the possibility to test the protocol implementation, a web-based Graphical User Interface (GUI) is developed and public available. All messages presented are XML code that contains all relevant parameters defined from the protocol and data model requirements.
- Routing in CR networks is challenging and different from routing in a conventional wireless network. The secondary usage of spectrum is the key difference, since routing in CR distributed network infrastructures could not be based on a Common Control Channel (CCC).
- Spectrum-aware routing protocols are evaluated in the context of a Public Safety mesh network. Two routing protocols were developed and evaluated, enabling for the reliable data delivery, across regions with different TVWS availability. Real TVWS results were taken into account from Munich area in Germany. In the area of Munich, the available TV channels, based on COGEU geo-location database, varies from 1 to 3 and create inconsistency of spectrum opportunities among secondary nodes.
- A routing simulator was developed, where the AODV protocol was modified and adapted in order to overcome the challenges regarding the absence of a CCC between secondary users in COGEU public safety networks. Performance evaluation results verified the validity of the proposed routing protocols in terms of average End-to-End delay and number of hops.
- Transport layer protocols in Cognitive Radio Ad-Hoc Networks (CRAHNs) were investigated in this WP. A modification of legacy information transport protocols in order to operate in a cognitive radio environment, were designed, developed and evaluated. Integrating services provided by the reference COGEU reference models makes this Hop-By-Hop (HBH) transport protocol a spectrum aware OSI layer 4 protocol.
- A patent has been written and submitted resulting from HBH transport protocol.

Table of Contents

1- Introduction 5

2- COGEU PAWS – Protocol to Access White Space Database 6

2.1- **Introduction** 6

2.2- **COGEU Requirements** 7

2.2.1- *Protocol requirements* 7

2.2.2- *Data model requirements* 8

2.3- **Implementation** 8

2.3.1- *Protocol stack* 8

2.3.2- *Web tools and programming languages* 9

2.3.3- *Database tables* 9

2.3.4- *Supported Services* 10

2.4- **Graphical user web interface** 13

2.4.1- *The registration process* 14

2.4.2- *Channel list request* 15

2.4.3- *Slave WSD ID request* 15

2.4.4- *Download the source code of the COGEU-PAWS draft implementation* 15

3- Spectrum-aware routing protocols for Public Safety Networks over TVWS 17

3.1- **Public Safety scenario exploiting mesh networks over TVWS** 18

3.2- **Design of routing protocols adopted in COGEU** 21

3.3- **Optimization of routing process for COGEU use-cases** 23

3.4- **Simulation scenario and performance evaluation** 23

4- Transport Protocols for Public Safety Networks over TVWS 29

4.1- **Transport Layer Protocols in wireless mesh networks** 30

4.2- **Transport layer protocols in Cognitive Radio Ad-Hoc Networks over TVWS** 31

4.2.1- *Challenges considered for COGEU use-case* 32

4.3- **Hop-by-Hop transport protocol (HBH) for CRAHN over TVWS** 33

4.4- **HBH protocol design for transport over TVWS** 33

4.4.1- *Macroscopic description of HBH* 34

4.4.2- *Hop-by-hop spectrum-aware reliability mechanism* 34

4.4.3- *Hop-by-hop Back-pressure mechanism* 35

4.4.4- *HBH messages structure definition* 36

4.4.5- *Internal HBH variables* 36

4.5- **Design of the HBH implementation** 37

4.5.1- *HBH Design description* 38

4.5.2- *HBH implementation details* 39

4.5.3- *Simulation evaluation of the HBH transport layer results* 41

4.6- **Summary** 44

5- Conclusions 45

References 46

1- Introduction

Successful deployment of Cognitive Radio Networks (CRNs) in the TV white spaces (TVWS) will depend on the development of the appropriate networking protocols at different layers. The main purpose of D6.3 is to design, develop and evaluate the performance of networking protocols in order to overcome challenges of operation in the TVWS.

More specifically, Chapter 2 presents the design and implementation of a Protocol to Access White Spaces Database (PAWS), in order to enable the reliable and secure communication of master white spaces devices (or the COGEU broke)r with the TVWS geo-location database. A detailed implementation compliant with IETF PAWS requirements is reported, using a web-based environment and a graphical user interface.

Chapter 3 discusses routing challenges in a Public Safety CR network with secondary usage of spectrum. Routing in a CR network is challenging and different from routing in a conventional wireless network. A key difference is that routing in CR networks is not based on a Common Control Channel (CCC), since each secondary node cannot obtain the same channel of operation. This chapter investigates multi-hop routing schemes, in order to provide efficient data delivery across regions of heterogeneous spectrum availability, even when the network connectivity is intermittent or when an end-to-end path is temporarily unavailable. In this context, a Public Safety use-case is studied based on a mesh, ad-hoc network architecture, where secondary nodes communicate exploiting novel routing protocols. The proposed routing protocols were designed, implemented and evaluated, in order to validate their efficient exploitation in COGEU use cases.

In Chapter 4 a modification of transport protocols adopting a Distributed Performance Enhancing Proxy scheme in order to operate in a cognitive radio environment, where frequent disruption is a norm and end-to-end paths are hardly available such in some secondary usage scenarios, has been investigated. In cognitive radio networks, many factors such as unpredictable external interference, heterogeneous channel bandwidth availability, or channel mobility/switching can affect the packet loss rate. Similarly, RTT can be affected by the delay due to spectrum sensing and spectrum handoff, for which when the current channel becomes unusable for an unlicensed user, the unlicensed user has to search for a new channel. Therefore, the modified transport layer protocols consider these effects to optimize end-to-end congestion control and to tune reliability accordingly.

Finally, Chapter 5 presents the main conclusions of this deliverable.

2- COGEU PAWS – Protocol to Access White Space Database

2.1- **Introduction**

COGEU reference model supports two different regimes: spectrum commons (unlicensed use) and secondary spectrum trading based on a broker entity (see Figure 1). COGEU also considers a centralized topology with a geo-location Spectrum database dealing directly with TVWS Devices (Spectrum Commons world) or with Spectrum Broker (Secondary Spectrum Market).

Both strategies must be able to communicate with a geo-location spectrum database, to store and retrieve information on the maximum allowed transmitted power of TVWS secondary devices and other technical parameters:

- Spectrum commons: the communication takes place between a geo-location database and a fixed base station, i.e, a master White Space Device (WSD).
- Spectrum broker: the communication is between a geo-location database and the broker entity.

More details on these approaches are provided in COGEU D3.2 of WP3.

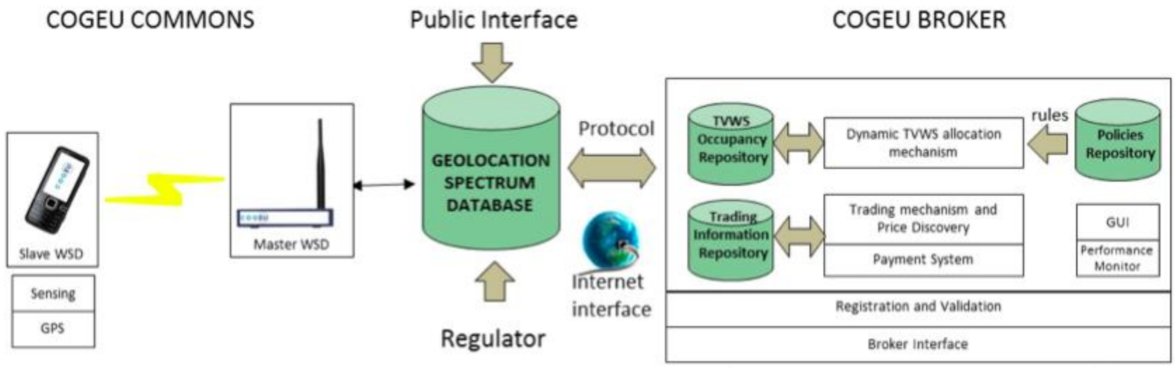


Figure 1: COGEU reference architecture for commons and secondary trading, using a web-based geo-location database access.

The Internet Engineering Task Force (IETF) [1], an organized activity of the Internet Society - ISOC [2], is a group, producing relevant technical documents that influence the way people design, use, and manage the Internet. One of the IETF group is presently working on the definition of a protocol to access white spaces databases – PAWS [3]. Ofcom UK has also published a draft document on the definition of a similar protocol, including a detailed list of parameters to be exchanged between WSDs and a database [4]. Ofcom solution is a protocol tailored for the UK scenario, with different requirements than the IETF proposal that is more comprehensive and less specific on details. Therefore, the IETF draft protocol was chosen and considered flexible enough to be adapted for the COGEU model and its requirements.

The objective of this chapter is to describe the implementation of a reliable and secure communication protocol for master WSDs (spectrum commons) or broker entity (secondary spectrum market) to access geo-location database services over the Internet. The next section presents the proposed solution, followed by a description of COGEU protocol requirements. Then, we describe the protocol implementation, using a web-based environment, and the graphical user interface.

2.1.1- ***Proposed solution exploiting IETF PAWS***

Spectrum Bridge [5] has recently released an IETF Internet-Draft [6], called “Protocol for Communication between White Space Device and White Space Database”. This document is an application protocol for geo-location database services provided to WSDs over the Internet. Several operational requirements are defined to support this primary function, such as device registration, and ID verification. The protocol allows any WSD to gain access to the services of the geo-location database by communicating over commonly used Internet protocols as illustrated in Figure 2.

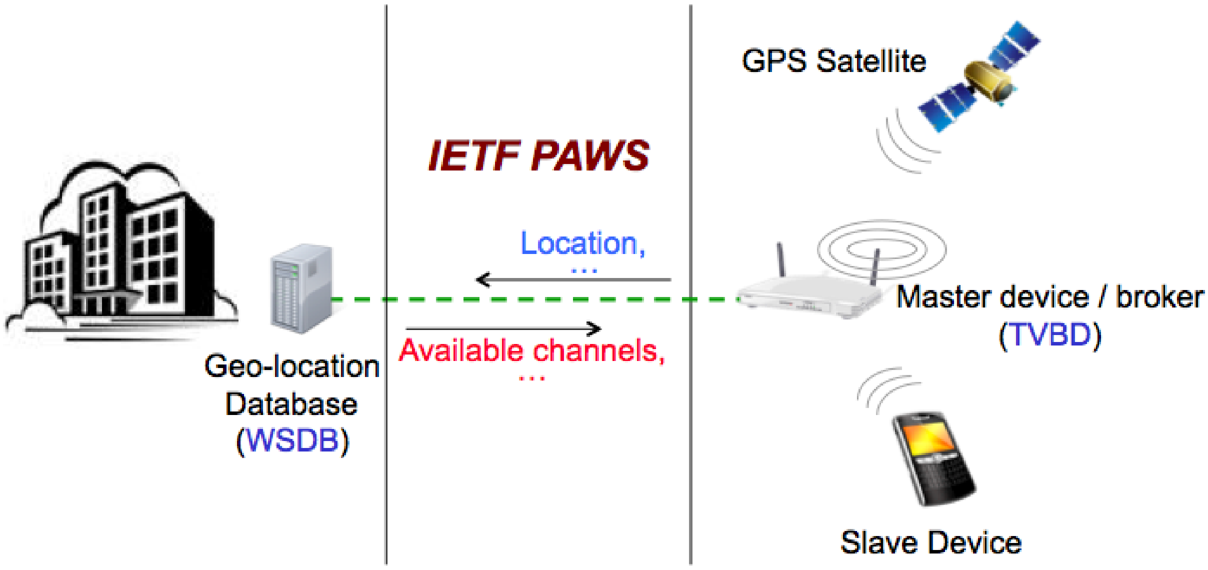


Figure 2: Implemented solution based on IETF PAWS.

Since Spectrum Bridge protocol is compliant with FCC Rules/Requirements [7], we have adapted its contents to satisfy the COGEU system requirements. We adopted Spectrum Bridge proposal as the main reference, so it may continue to comply with requirements defined by IETF PAWS [8].

2.2- COGEU Requirements

This section presents the protocol and data model requirements of COGEU PAWS, and present the main differences with IETF PAWS.

2.2.1- *Protocol requirements*

This section defines the application protocol used between the geo-location database and WSD for all services offered by the geo-location database. The following sections define the services provided by the geo-location database. The services are accessed by the WSD using HTTPS GET and PUT requests over the Internet. Providing available Channel Lists to WSDs is the primary service provided by the geo-location database.

Operations are only initiated by the WSD, with a response from the geo-location database. This eliminates the necessity of the geo-location database to initiate communications with the WSD.

We defined separate requirements for slave WSDs and master WSDs. The protocol must enable a master WSD to complete the following tasks:

- Connect to the database using a well-defined access method.
- Register with the database using a well-defined protocol.
- Provide its geo-location and other data to the database using a well-defined format for querying the database.
- Receive in response to the query a list of currently available white space channels, maximum power and sensing requirements, using a well-defined format for the information.

Moreover, the protocol should enable a slave WSD to complete the following tasks:

- Request to a master WSD, to verify if the slave WSD is valid (enrolled in the database)
- Receive in response to the query, a status code from the master WSD, indicating if the slave WSD is valid or not.

Services not considered in the current implementation, but defined in IETF PAWS, are:

- Database discovery;
- Master or slave WSDs enrolment in the database.

2.2.2- *Data model requirements*

The contents of the queries and response from the protocol need to be specified. A data model is required which enables the WSD to query the database while including all the relevant information such as geo-location, power characteristics, sensing capabilities, etc. which may be country and spectrum and regulatory dependent. The geo-location database is able to interpret the data model and respond to the queries using the same data model that is understood by all WSDs. Partially following IETF proposal [8], but adapted to the COGEU model, the data model requirements are:

- The data model support specifying the location of the WSD and the uncertainty of the GPS receiver, in meters.
- The data model support specifying an ID of the transmitter device. This ID contains the ID of the transmitter device that has been certified by a regulatory body for its regulatory domain. The data model supports a device class:
    - Fixed devices (master WSDs): type 8
    - Mode I devices (Slave WSDs): type 1
- The data model support specifying a manufacturer's serial number for a master device.
- The data model support specifying the antenna related parameters of the subject, such as:
    - antenna height
    - maximum output power, EIRP (dBm)
- The data model support specifying owner and operator contact information for a transmitter. This includes the name of the transmitter owner, name of transmitter operator, postal address, email address and phone number of the transmitter operator.
- The data model support specifying a list of available channels, by channel numbers and maximum power level for each channel in the list. The data model also support specifying sensing necessity for each channel in the list, to detect wireless microphone activity.
- The data model support specifying channel availability information for a single location for a 200x200 m squared area (The resolution of the geo-location database of the Munich area).
- The data model support specifying the frequencies and power levels selected for use by a device in the acknowledgement message.

2.3- Implementation

2.3.1- *Protocol stack*

The Application Protocol utilizes the following protocol stack for communication between the geo-location database and WSD:

- Application Layer: HTTPS
- Presentation Layer: XML
- Session Layer: Undefined
- Transport Layer: TCP
- Network Layer: IP
- Data Link: Undefined
- Physical Layer: Undefined

Many modern applications are successfully utilizing this protocol stack for client-server communications, and most modern network devices already include a TCP/IP stack.

XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services, and has also been employed as the base language for communication protocols [9].

HTTPS is a key component used in this protocol, providing a commonly used request-response protocol for a client-server model, where the geo-location database is the server and the master WSD is the client. Additionally, HTTPS provides security via SSL to satisfy security requirements [6].

2.3.2- *Web tools and programming languages*

Several programming languages, from MySQL, PHP and JavaScript, were used to develop this implementation of COGEU PAWS. All languages are open source software.

MySQL is the world's most used open source relational database management system that runs as a server providing multi-user access to a number of databases. MySQL is the technology used to implement all the requirements for the database. For that case, MySQL is used to store geo-location data, information about all Master WSDs (Registration Process), and the Slave WSDs (serial number only).

PHP is a general-purpose server-side scripting language originally designed for Web development to produce dynamic Web pages. It is one of the first developed server-side scripting languages to be embedded into an HTML source document, rather than calling an external file to process data. Ultimately, a Web server, with a PHP processor module, which generates the resulting Web page, interprets the code. PHP has evolved to include a command-line interface capability and can be used in standalone graphical applications. PHP can be deployed on most Web servers and also as a standalone shell on almost every operating system and platform, free of charge. In the context of COGEU PAWS development, the main objective of PHP is to access a MySQL database, where the TVWS geo-located data is stored.

JavaScript (sometimes abbreviated JS) is a prototype-based dynamic scripting language, weakly typed with first-class functions. JS is a multi-paradigm language, supporting object-oriented, imperative, and functional programming styles. JavaScript is the scripting language of the Web, used in billions of Web pages, to add functionality, validate forms and communicate with the server, among many others functionalities. JavaScript language is used to control the user web interface and the Google maps API.

2.3.3- *Database tables*

Figure 3 shows the connection between all four SQL tables implemented in the database. The “fixed_WSD” table records the list of enrolled devices. This operation generates an ID, and this ID is used in the table “white_spaces_devices_registration”, as a foreign key. This process guarantees that only those devices that are present in the “fixed_WSD” table, may be registered. This way, the registration process is protected right at the beginning of the process, preventing code errors and incrementing security.

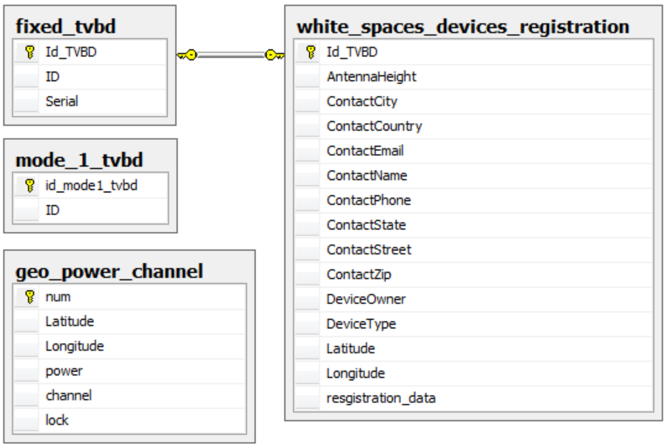


Figure 3: Relational Database Diagram for PAWS

Table “mode_1_WSD”, in a preliminary implementation stage, only saves the ID of Slave WSDs previously enrolled in the database by a regulator or official entity, to guaranty that only registered slave WSDs may have access to the channel lists, sent from the Master WSD.

In the “geo_power_channel” table, we keep a record of geo-location data for every channel, using decimal coordinates. This table is queried each time a Master WSD, registered in the “white_spaces_devices_registration” table, wants to obtain a list of available channels. The Master WSD must inform the database of his location before receiving a channel list.

2.3.4- ***Supported Services***

Three services are defined on the interface between the geo-location database and WSDs:

- Service 1: Registration
- Service 2: Channel List Request
- Service 3: ID Verification

The services are listed in order, representing the steps that a WSD must take to obtain service from the geo-location database.

2.3.4.1 Registration

A fixed WSD must register with the geo-location database prior to operating for the first time, or after changing location, or if any of the registration data changes. Only fixed WSDs register with the geo-location database.

To successfully register, the ID and Serial Number of the WSD must be enrolled at the geo-location database. Device enrollment is an administration function that is not in the scope of this application protocol definition. Geo-location database operators may define their own methods for acquiring and maintaining device enrollment data. See Figure 4 for an example of enrolled devices in the database (for demonstration purposes).

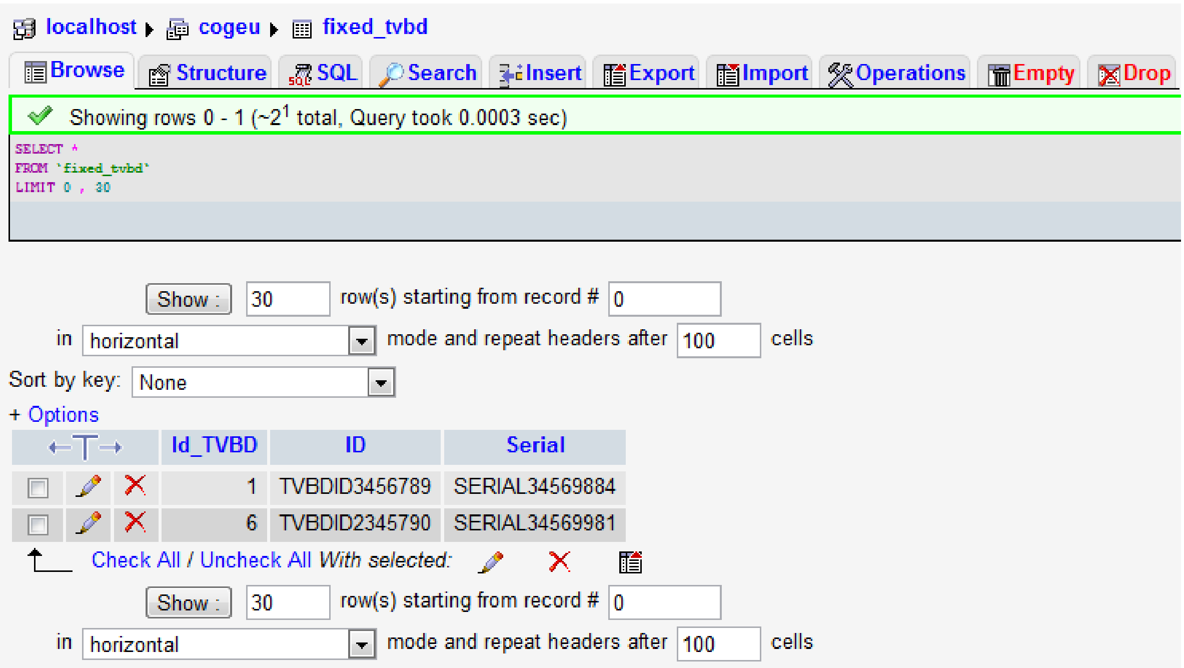


Figure 4: List of enrolled master WSD in the database.

To register with the geo-location database, the WSD must send a “Registration Request” message to the geo-location database.

One of two possible results shall be returned by the geo-location database, represented in Figure 5:

1. Successful Registration. The registration will be valid for a certain period (the timer RVP is described in chapter 2.3.5-) and will be extended by subsequent geo-location database access by the WSD.
2. Unsuccessful Registration. The WSD identifiers (ID and Serial Number) were unrecognized or unsupported by the geo-location database.

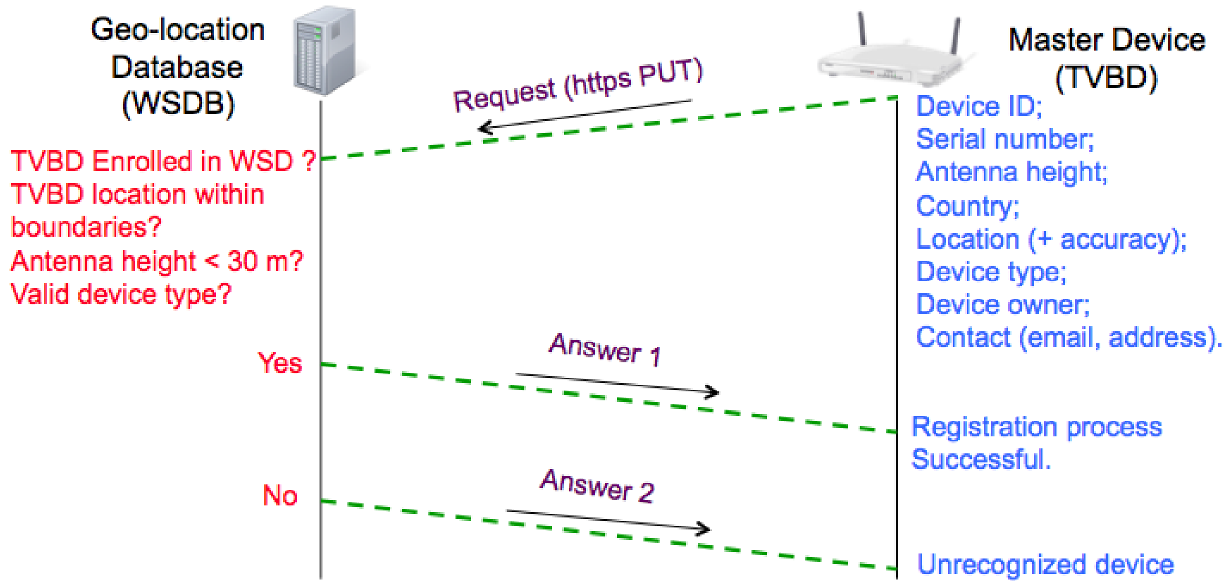


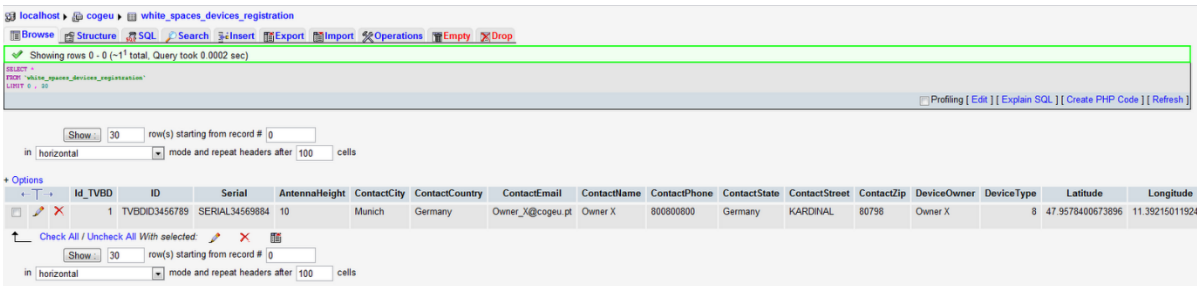
Figure 5: Message exchange, upon registration request from the WSD to the geo-location database.

A successful “Registration Reply” will be returned to the WSD only if all of the following are true:

- The ID and manufacturer's serial number are enrolled at the geo-location database.
- The device location is within the appropriate regulatory boundaries.
- The device type is valid (only Fixed WSDs may register).
- The antenna height is less than or equal to 30 meters.

A successful registration will overwrite any previous registration information for the same WSD, as identified by ID and serial number.

Figure 6 shows an example of a WSD registration stored in the database, i.e., the ID, serial number, location accuracy, and additional XML data.



Id_TVBD	ID	Serial	AntennaHeight	ContactCity	ContactCountry	ContactEmail	ContactName	ContactPhone	ContactState	ContactStreet	ContactZip	DeviceOwner	DeviceType	Latitude	Longitude
1	TVBDID3456789	SERIAL34569884	10	Munich	Germany	Owner_X@cogeu.pt	Owner X	800800800	Germany	KARDINAL	80798	Owner X	8	47.9578400673896	11.39215011924

Figure 6: Recorded data from the WSD in the geo-location database

The database will retain the WSD registration for a fixed period (RVP) with no activity. RVP will be extended by every successful registration, and by any subsequent “Channel List Request” received from the WSD.

Successful registries will timeout, after a period of inactivity from the WSD. More details on timer implementation are described in chapter 2.3.5-.

2.3.4.2 Channel List Request

The geo-location database will provide, upon request, the available TV channels at the WSD's location, the channel list is also combined with information of the TV channels that needs sensing, the power available for each channel and the time to refresh all the information.

There are three possible outcomes to a “Channel Request”:

1. Successful, with channel List;
2. Successful, with no channels available;
3. Unsuccessful.

To successfully receive a channel list, the ID and Serial Number of the WSD must be enrolled and registered at the geo-location database.

A successful “Channel List Response” will be returned to the WSD only if all of the following are true:

- The identifier and manufacturer's serial number are enrolled at the geo-location database.
- The device location is within the appropriate regulatory boundaries.
- The device type is valid.
- For a fixed WSD, the device is registered and the location matches the values previously registered.

Figure 7 shows a representation of the messages exchanged between the geo-location database and the WSD for a “Channel List Request”.

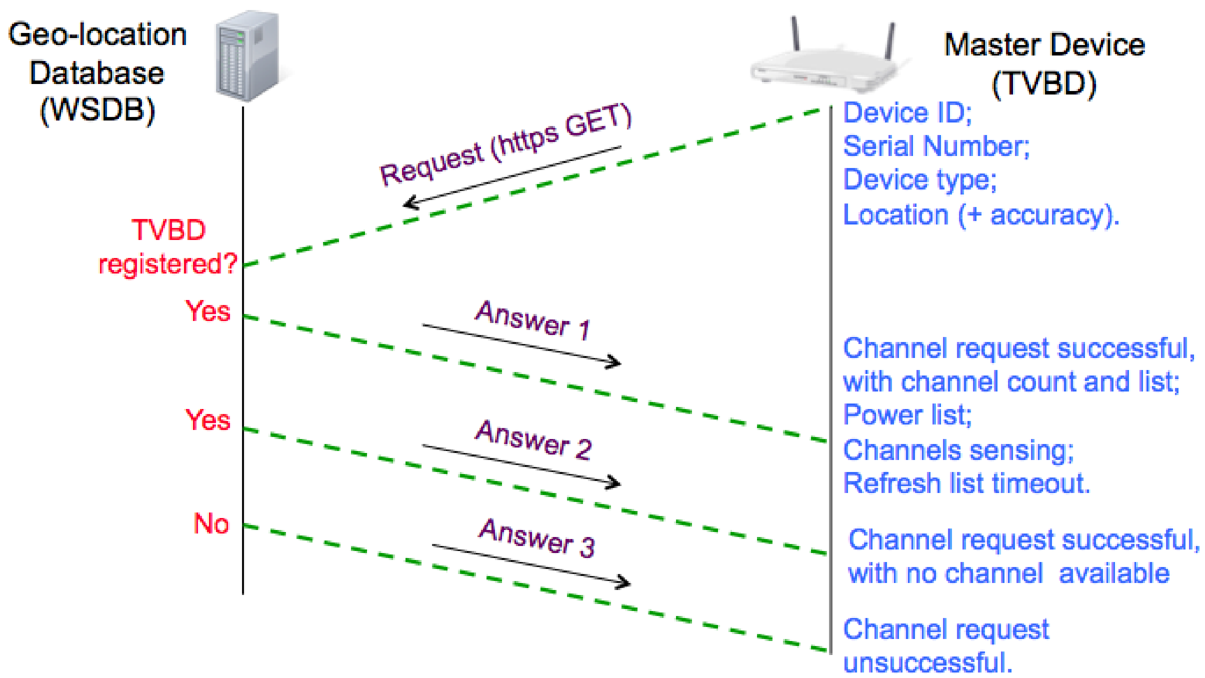


Figure 7: Message exchange for a channel list request from the WSD to the geo-location database. All possible answers are represented, but only one is sent at each request.

2.3.4.3 ID Verification

The “ID Verification Request” provides a method for WSDs to verify the validity of Slave WSDs (Mode I) that are dependent upon a master WSD for channel lists. The geo-location database will respond whether a requested ID is valid or not, i.e., an “ID Verification Response” will always be returned.

The status returned in the geo-location database response is based on whether the ID is found in the authorized list of IDs.

The following sequence of events describes the use of this request (Figure 8):

1. A Master WSD needs to verify if a slave WSD is valid, and sends an “ID Verification Request Message” to the geo-location database.

2. The geo-location database checks the ID against the authorized IDs and returns a reason code of success (0) only if found, otherwise unknown (not 0) will be returned. As long as the message is decodable, an "ID Verification Response" will always be returned.

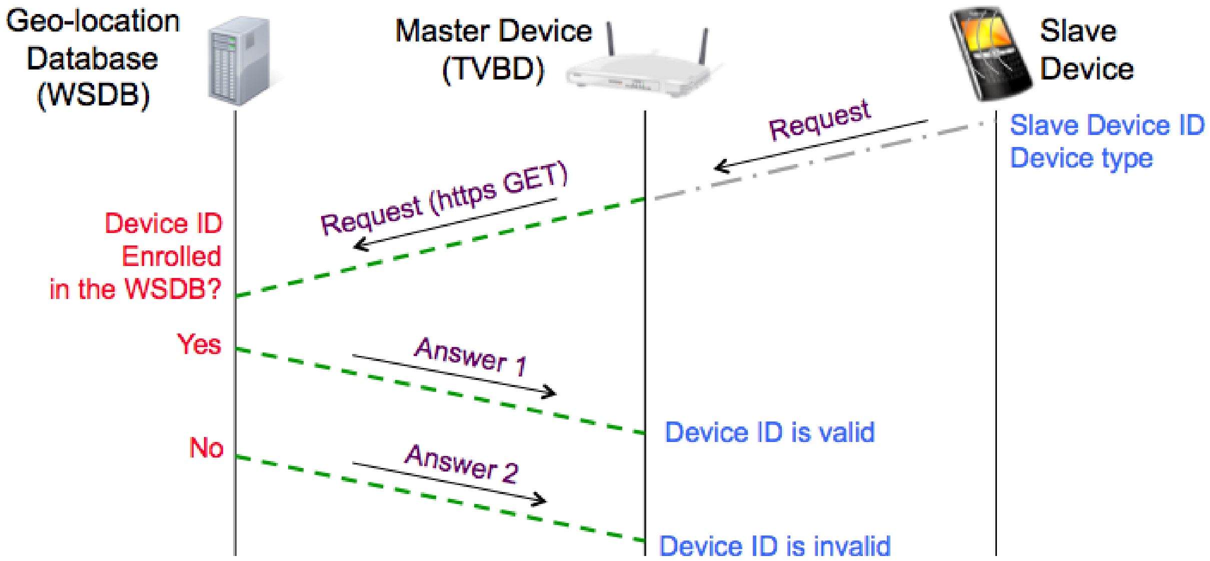


Figure 8: Slave ID request message exchange.

2.3.5- *Timers*

Several timers are implemented and used by the protocol, during operation:

- CLRP (1440 minutes): Channel List Refresh Period. The channel list must be refreshed at least once per day.
- CRT (5 seconds): Channel list Request Timer.
- VRT (5 seconds): ID Verification Request Timer.
- RVP (90 days): Registration Valid Period. This period was reduced to 60 seconds for demonstration purposes.

2.4- Graphical user web interface

To give a glimpse of the protocol implementation to the interested user, with the possibility to test the protocol implementation, we decide to create a web-based Graphical User Interface (GUI).

The GUI is a single webpage, divided into three vertical panes, as shown in Figure 9. In the leftmost pane, the user has access to the parameters definition and may select which kind of device is used to communicate with the geo-location database. In the blue area, we have master WSD (Type 8) parameters and in the red area we have slave WSD (Type 1) parameters. The location of the master WSD may be defined writing the appropriate coordinates, or clicking on the "Show Map" checkbox to open Google Maps to point the desired location. On the same map, the boundaries of the geo-location database are also available. Additionally, a grid with 200 x 200 m resolution may be turned visible, after clicking on the "Show grid" checkbox. For demonstration purposes, a set of master and slave WSD IDs and serial numbers are already enrolled in the database and may be selected from the dropdown menus.

The second and third panes from the left shows the messages sent from WSDs, and the answers from the geo-location database, respectively. A visible log of all messages and answer is kept on the interface, and sequentially numbered. Old messages are greyed, to avoid confusion with the most recent messages.

All messages presented are XML code that contains all relevant parameters defined from the protocol and data model requirements.

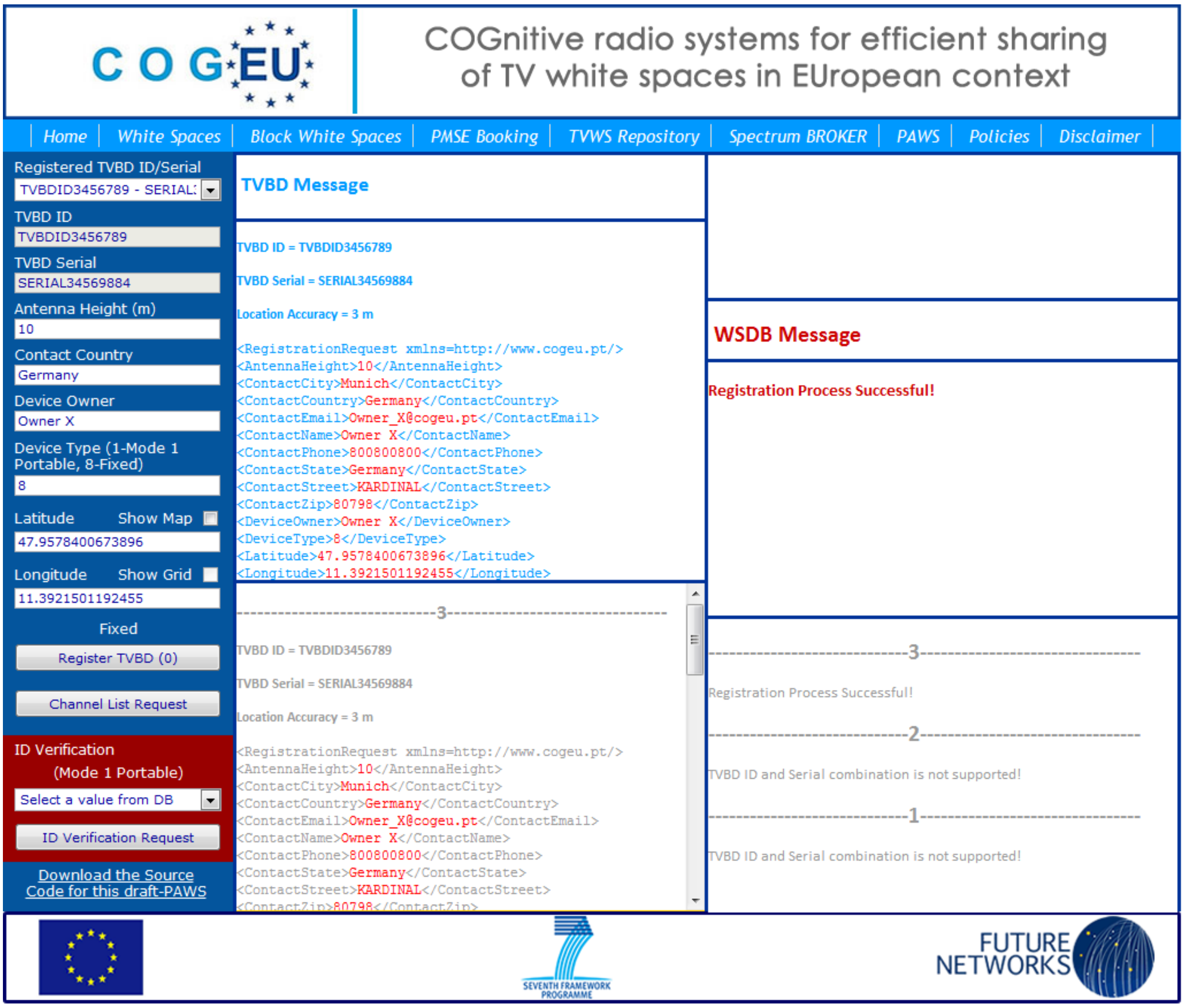


Figure 9: Graphical web interface to demonstrate COGEU PAWS between a geo-location database and a WSD (fixed or Mode 1 Portable)

The next example shows how the message is sent to the geo-location database, and in this case, the acceptance of the data and the recorded data.

2.4.1- *The registration process*

An example of the XML message, from the master WSD to the database, is:


```
WSD ID = WSDID23457900

WSD Serial = SERIAL34569980

Location Accuracy = 3 m

<RegistrationRequest
xmlns=http://www.cogeu.pt/>
<AntennaHeight>10</AntennaHeight>
<ContactCity>Munich</ContactCity>
<ContactCountry>Germany</ContactCountry>
<ContactEmail>Owner X@cogeu.pt</ContactEmail>
<ContactName>Owner X</ContactName>
<ContactPhone>800800800</ContactPhone>
<ContactState>Germany</ContactState>
<ContactStreet>KARDINAL</ContactStreet>
<ContactZip>80798</ContactZip>
<DeviceOwner>Owner X</DeviceOwner>
<DeviceType>8</DeviceType>
<Latitude>47.9578400673896</Latitude>
<Longitude>11.3921501192455</Longitude>
</RegistrationRequest>
```

2.4.2- *Channel list request*

An example of the XML message of a “Channel List Request” from a master WSD is:

```
WSD ID = WSDID23457900
WSD Serial = SERIAL34569980
Device Type = 8
Latitude = 47.9578400673896
Longitude = 11.3921501192455
Location Accuracy = 3 m
```

An example of the XML code from the geo-location database answer is:

```
HTTP/1.1 200 OK Cache-Control: private

Content-Length: 214

Content-Type:    application/xml;    charset=utf-8 \geo-
location database-Version: 1

geo-location database-Status: 0

Date: Mon, 11 Jun 12 22:21:05 +0100

<ChannelResponse xmlns="http://www.cogeu.pt/">
<ChannelCount>2</ChannelCount>
<ChannelList>59,60</ChannelList>
<ChannelSensing>59,60</ChannelSensing>\
<Power>12.7,17.2</Power>
<RefreshIn>60</RefreshIn>
</ChannelResponse>
```

2.4.3- *Slave WSD ID request*

If the serial of the slave WSD is enrolled in the database and the Device Type is 1 (mode I Portable), the message received is “Verification Successful”, in the “database Message”. Otherwise, If the slave ID is not enrolled in the database, the message is “Verification Unsuccessful”.

WSD Slave message:

```
SLAVE ID = ID_MODE_1_4589787

Device Type = 1
```

Master WSD message (after querying the database):

```
HTTP/1.1 200 OK

Cache-Control: private

geo-location database-Version: 1
geo-location database-Status: 0
Date: Mon, 11 Jun 12 22:24:30 +0100
Content-Length: 1
Verification Successful
```

2.4.4- *Download the source code of the COGEU-PAWS draft implementation*

In order to disseminate COGEU-PAWS implementation the source code is online available for download here: http://projectos.est.ipcb.pt/cogeu2/PAWS_index.php
The software works with a geo-location database populated with random data (for illustrative proposes). The installation and configuration guidelines are listed below:

1. Install and configure the zend Server Software (ZendServer-CE-php-5.3.9-5.6.0-SP1-Windows_x86.exe).

2. Go to your browser, to the zend Server local Page, usually: “http://localhost:10081/ZendServer/”

3. Go to tab "Monitor"->"Dashboard", select click "Open phpMyAdmin" and type the username and password previously configured.

4. In the phpMyAdmin, create the new database named "cogeu", and go to the tab "import" and click in browse.

5. Select the script file named "cogeu.sql" and click Execute. Please note, that this operarion will take some time.

6. Repeat the previously step and select the files "Store procedure returnChannelList.txt" and "Store procedure TVBD_Resgistration.txt".

7. Go to the installation path of the Zend Server and select the folder "htdocs"(Ex: "C:\Program Files\Zend\Apache2\htdocs").

8. Copy the folder "PAWS" to the folder "htdocs".

9. Edit the file "connection.php", and type the password to your MySql Data Base.

10. Test all, go to your browser (note: this web page is optimized for Google Chrome), and type http://localhost/PAWS/

3- Spectrum-aware routing protocols for Public Safety Networks over TVWS

The flexibility of cognitive radio, ad-hoc (distributed) networks capabilities, appears to have the potential to enhance Public Safety operations. Cognitive radio networks, operating over TVWS can facilitate multi-organisational (e.g. fire-brigade and police) interventions at operational level, which would not be based on the need for dedicated and harmonised spectrum assignment to Public Safety systems at the European level. Future systems could collectively use possible TVWS spectrum that is available in an open access manner. More details regarding initial specifications, on this use-case scenario, are provided in COGEU D3.3 of WP3. Moreover, cognitive radio technologies have the potential to address interoperability issues of emergency communications systems, through two different means. A TVWS gateway could be used to link two different radio communications systems on different frequencies or the cognitive radio system could be used to minimize mutual interference between two communications systems deployed in the same operational crisis site.

However, the flexibility in the spectrum access phase, by CR network infrastructures caused new challenges along with increased complexity in the design of communication protocols at different layers. More specifically, the design of effective routing protocols for ad-hoc CR networks is a major challenge in cognitive radio networking paradigm. Ad-hoc CR networks are characterized by completely self-configuring architectures [10], where routing is challenging and different from routing in a conventional wireless network. A key difference is that spectrum availability in an ad-hoc CR network highly depends on the primary users' presence, thus, it is difficult a Common Control Channel (CCC) to be used, in order to establish and maintain a fixed routing path between secondary users. Another major challenge that faces reliable operation in the white spaces is interference among peer TV band devices given the unlicensed nature of operation in this band. Managing interference between nodes in the same network is generally a difficult problem, and this becomes more challenging when devices belong to heterogeneous networks, using different air interfaces.

In a general context, multi-hop, ad-hoc networks are collections of network nodes connected together over a wireless medium. These nodes can freely and dynamically self-organize into arbitrary and temporary ad-hoc network topologies, allowing users and devices to seamlessly internetwork in specific geographical areas. Traditionally, tactical networks have been the only communication networking application that followed the ad-hoc paradigm. Recently, the introduction of low-cost wireless technologies (e.g. IEEE 802.11), together with the standardization efforts of the Internet Engineering Task Force (IETF) MANET Working Group, have been generating renewed and growing interest in research and development of ad-hoc networks for several applications. Most of the ongoing research on ad-hoc networks is driven by either military requirements (large-scale military applications with thousands of ad-hoc nodes) or specialized civilian applications (disaster recovery, planetary exploration, etc). Military organizations generated a research agenda and requirements that are far from real users' requirements. Military and specialized civilian applications require lack of infrastructure and instant deployment. They are tailored to very specialized missions, and their cost is typically not a main issue.

On the other hand, from the users' standpoint, scenarios consisting of a limited number of users requesting to form an ad-hoc network for sharing information are much more interesting. In this case, users are looking for multi-purpose networking platforms, in which cost is an issue and Internet access is essential. To turn ad-hoc networks into a commodity some changes to the original definition would seem to be required. By relaxing one of the main constraints of ad-hoc networks, “the network is made of users' devices only and no infrastructure exists” we move to a more pragmatic “opportunistic ad-hoc networking”, in which multi-hop, ad-hoc networks are not isolate self-configured networks, but rather emerge as a flexible and low-cost extension of wired infrastructure networks, coexisting with them. Therefore, a new class of networks is emerging from this view; mesh networks [10]. Mesh networks are built on a mix of fixed and mobile nodes interconnected via wireless links to form a multi-hop, ad-hoc network. Users dynamically join the network, acting as both user terminals and routers for other devices, consequently further extending network coverage. Mesh networks thus inherit many results but have civilian applications as the main target.

Furthermore, while the mesh networks development approach was mainly simulation-based, from the beginning mesh networks have been associated with real test-beds. By designing/implementing “good enough” solutions, it has been possible to verify the suitability of this technology for civilian applications and stimulate users' interest in adopting it. Even though mesh networks are quite recent, they have already shown great potential in the wireless market. Indeed, we can subdivide mesh networks into two main classes: off-the-shelf and proprietary solutions. An example of the first class are so-called community networks built (mainly) on 802.11 technology and aimed at providing Internet access to a community of users that can share the same Internet access link. On the other hand, several companies are now selling interesting solutions that exploit the mesh network potential for indoor and/or outdoor applications (e.g., Mesh Networks, Tropos Networks, Radiant Networks, Firetide, BelAir Networks, Strix Systems). For example, indoor mesh networks can be set up by wireless interconnected access points that, by exploiting routing algorithms developed for MANETs, can create extended WLANs without a wired infrastructure. Outside buildings, mesh networks can be used to provide wireless access across wide geographic areas by minimizing the number of wired ingress/egress points toward the Internet. Outdoor networks might be used, for example, by municipalities to extend their wired networks wirelessly.

This promising networking technology recently received a further boost when IEEE 802 creating Task Group 802.11s aimed at defining medium access control (MAC) and PHY layers for mesh networks to improve wireless LAN (WLAN) coverage with no single point of failure. In such networks, 802.11 access points relay information from one to another, hop by hop, in router-like fashion. As users and access points are added, capacity is added. In addition to 802.11s, other IEEE Working Groups are currently working to provide mesh networking extensions to their standards (e.g., 802.15.5, 802.16a, and 802.20).

In this context, the basic research target of this chapter is to present the design, development and evaluation of novel spectrum aware routing protocols, operating over a distributed, mesh based, CR networking infrastructure, facilitating the efficient communication between secondary users for public safety COGEU use-cases as defined in D3.3. Additionally, this chapter introduces a general architecture for mesh networks, highlighting the benefits of this radically new networking paradigm as presented above. In a general context, several emerging and commercially interesting applications for commodity networks based on wireless mesh network architecture have been deployed recently. To identify all possible applications exploiting the mesh networking paradigm would be too ambitious for the scope of this deliverable. Consequently, in this section we focus on providing use-cases that benefit from wireless mesh networks, operating over TVWS based on real spectrum availability from Munich area in Germany.

3.1- Public Safety scenario exploiting mesh networks over TVWS

The transmission of secondary nodes in an ad-hoc, CR network is based on spectrum opportunity. Therefore, routing in such a network has to take into account the availability of spectrum in specific geographical locations at local level. Spectrum awareness, route quality and route maintenance issues have to be investigated for different routing schemes, in order to enable for the proper data delivery, across regions of heterogeneous spectrum availability, even when the network connectivity is limited or when an end-to-end path is temporarily unavailable.

Figure 10 illustrates the proposed public safety use-case scenario, where secondary nodes operate opportunistically, by utilizing the remaining (from primary systems) available channels in each geographical area (i.e. TVWS in Figure 10). Ad-hoc network is ideally to be used in emergency situations like natural disasters, military conflicts, emergency medical situations etc. Moreover, an ad-hoc network is required to support increasing demand for multimedia communications. Maintaining real-time media traffic, such as audio and video in presence of dynamic network topology is particularly challenging due to high data rate requirements and stringent delay constraint, especially when wireless nodes have generally limited network resources.

It has to be noted here that a CCC does not exist between secondary public safety nodes, which are located in neighboring geographical areas (i.e. Area A, B and C in Figure 10). In such a case, secondary users that are located outside Areas A, B and C, (i.e. Areas with higher spectrum availability in the region) may act as intermediate bridge/relay nodes or gateways, able to switch among multiple channels, towards enabling for an ad-hoc connection between secondary users pairs with different spectrum availability. In this use-case scenario, links on each path have to be established using different channels, according to the TVWS availability in a specific geographical area and time period.

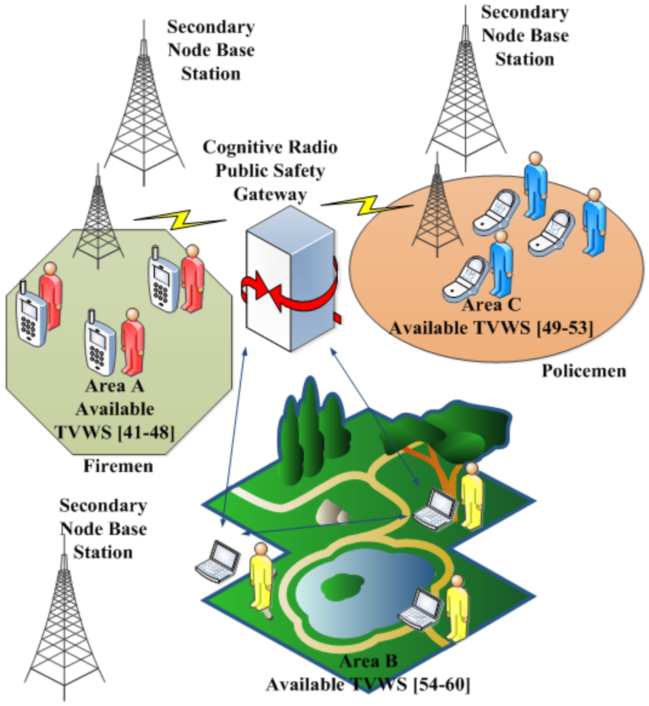


Figure 10: Communication across Public Safety workers operating over heterogeneous TVWS

In such application scenario, the challenge regarding routing protocols stems from the need to maintain reliable routes with QoS assurance, minimum control overhead and energy consumption from such maintenance. Another goal of routing in such networks is to provide persistent, high throughput communication by optimally selecting the appropriate path between secondary nodes. Thus, multi-hop connections must be set up between secondary nodes pairs with different spectrum availability and routing protocols have to be designed and adopted, enabling for route discovery capabilities, taking into account spectrum heterogeneity in different geographical locations. Route quality issues have also to be investigated since the actual topology of such multi-hop CR networks is highly influenced by primary users behaviors, and classical ways of measuring/assessing the quality of end-to-end routes (nominal bandwidth, throughput, delay, energy efficiency and fairness) should be coupled with novel measures on path stability. Furthermore, route maintenance is a vital challenge, considering the above mentioned use-case scenario. The unpredictable appearance of a primary node at a specific time period is possible to make a given channel unusable at local level, thus resulting in unpredictable route failures, which may require frequent path rerouting, either in terms of nodes or used channels. In a general context, routing in a TVWS based ad-hoc CR network constitutes a rather important but yet unexplored problem, especially when multi-hop network architecture is considered. The design of new routing protocols is therefore required, towards overcoming challenges defined above and establishing/maintaining optimal routing paths between secondary users with heterogeneous TVWS availability.

Moreover, public safety secondary nodes in such use-case, communicate utilizing a mesh network infrastructure, which is a fully wireless network that employs multi-hop communications to forward traffic. Mesh based infrastructures are self-configuring and self-healing networks, thus the link failures are limited, as each device has a connection to every other device in its immediate neighborhood. Also, in order to increase capacity and reduce interference, mesh nodes can communicate using multiple radios. Figure 11 illustrates the mesh network architecture, highlighting the different components and system layers.

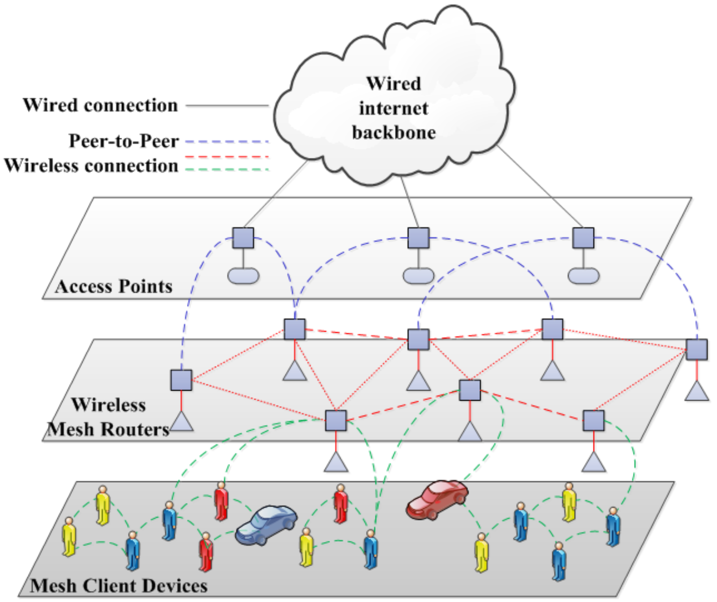


Figure 11: Mesh network architecture for Public Safety use-cases

More specifically, the ad-hoc extension to the backbone or infrastructure devices consists of clients/users with mesh devices. The mesh client devices can be static or mobile and they interact with the backbone or infrastructure devices, namely wireless mesh routers. The mesh routers are communicating among each other and providing wireless transport services to data traveling from mesh clients/users to either other clients or access points, which are special wireless routers with a high-bandwidth wired connection to the Internet backbone. The network of wireless mesh routers consists of a wireless backbone, which provides multi-hop connectivity between mesh clients and wired gateways, thus can save cost by having only a few high bandwidth wired links to the gateways instead of every router having a wired connection.

Meshing among wireless routers and access points creates a wireless backhaul communication system, which provides each mobile user with a low-cost, high-bandwidth, and seamless multi-hop interconnection service with a limited number of Internet entry points and with other wireless mobile users. Backhaul is used to indicate the service of forwarding traffic from the originator node to an access point from which it can be distributed over an external network. The mesh network architecture addresses the emerging market requirements for building wireless networks that are highly scalable and cost effective, offering a solution for the easy deployment of high-speed ubiquitous wireless network infrastructure. The following is not necessarily an exhaustive list of all the possible benefits, but represents an extensive discussion on the motivations behind the mesh networking vision.

- **Reduction of installation costs.** Currently, one of the major efforts to provide wireless networking infrastructures beyond the boundaries of indoor WLANs is through the deployment of Wi-Fi hot spots. Basically, a hot spot is an area that is served by a single WLAN or a network of WLANs, where wireless clients access the Internet through an 802.11-based access point. To ensure almost ubiquitous coverage in a metroscale area, it is necessary to deploy a large number of access points due to the limited distance covered by the 802.11 signal. The downside of this solution is an unacceptable increase in the infrastructure costs because a cabled connection to the wired backbone is needed for every access point. Installing the necessary cabling infra- structure not only slows down hot spot implementation, but also significantly increases installation costs. As a consequence, the hot spot architecture is costly, unscalable, and slow to deploy. On the other hand, building a mesh wireless backbone enormously reduces the infrastructural costs because the mesh network needs only a few points of connection to the wired backbone.
- **Large-scale deployment.** In recently standardized WLAN technologies (i.e. 802.11a and 802.11g), increased data rates have been achieved by using more spectrally efficient modulation schemes. However, for a specific transmit power, shifting toward more efficient modulation techniques reduces coverage (i.e., the further from the access point, the lower the data rate available). Moreover, for a fixed total coverage area, more access points should be installed to cover small-size (e.g. pico) cells. Obviously, this picocellularization of WLANs further hinders the scalability of this technology,

especially in outdoor environments. On the other hand, multi-hop communications offers long distance communications via hopping through intermediate nodes. Since intermediate links are short, these transmissions could be at high data rates, resulting in increased throughput compared to direct communications. Moreover, the wireless backbone can take advantage of non-mobile powered wireless routers to implement more sophisticated and resource-demanding transmission techniques than those implemented in user devices. Consequently, the wireless backbone can realize a high degree of spatial reuse and wireless links covering longer distance at higher speed than conventional WLAN technologies.

- **Reliability.** The wireless backbone provides redundant paths between each pair of endpoints, significantly increasing communications reliability, eliminating single points of failure and potential bottleneck links within the mesh. Network resilience and robustness against potential problems (e.g. node failures, and path failures due to temporary obstacles or external radio interference) is also ensured by the existence of multiple possible destinations (i.e. any of the egress points toward the wired Internet) and alternative routes to these destinations.
- **Self-management.** The adoption of peer-to-peer networking to build a wireless distribution system provides all the advantages of ad hoc networking, such as self-configuration and self-healingness. Consequently, network setup is automatic and transparent to users. For instance, when adding additional nodes in the mesh, these nodes use their meshing functionalities to automatically discover all possible wireless routers and determine the optimal paths to the wired network. In addition, the existing wireless routers reorganize, taking into account the new available routes. Thus, the network can easily be expanded, because the network self-reconfigures to assimilate the new elements.

3.2- Design of routing protocols adopted in COGEU

Towards enabling for an efficient data transition between source and destination Public Safety secondary users in the above mentioned use case, novel routing protocols were designed, implemented and evaluated under controlled simulation conditions. The routing protocols are based on the exchange of AODV-style messages [12] between secondary users, including two major steps (route discovery and route reply). During the route discovery step, a RREQ (route request) message, including TVWS availability of nodes is sent by the source user to acquire a possible route up to the destination user. Once the destination user receives the RREQ message, it is fully aware about the spectrum availability along the route from the source user. The destination user then chooses the optimum routing path, according to a number of performance metrics (e.g. backoff delay, switching delay, queuing delay, number of hops, throughput) and assigns a channel to each secondary user along the route. It has to be noted here, that the evaluation of performance metrics is conducted, by each intermediate node during the routing path of the RREQ message. In the next step, destination user sends back a RREP (route reply) message to the source user that includes information regarding channel assignment so that each node along the route can adjust the channel allocation accordingly. Once this RREP is received by the source user, it initiates useful data transmission.

Figure 12 presents the detailed process of the proposed routing protocol for handling both RREQ and RREP messages. The source user initiates a flow (i.e. New Flow in Figure 12), transmitting a RREQ message to an intermediate node located in a neighboring location. The intermediate node is updated by the geo-location database about TVWS availability of its neighboring nodes and determines if it is capable or not to accommodate the incoming flow from source user. If it is capable, it then evaluates the performance metrics, accommodates it and finally forwards it to the next hop or to the destination user, by forwarding the RREQ message. Once the destination user receives RREQ message, it is fully aware of channel availability along the route from the source node. Destination user sends then back a RREP message to the source user. This message contains information regarding channel assignment so that secondary users along the route can adjust the channel allocation accordingly. Once the source user receives the RREP, the routing path has been established and useful data transmission is initiated.

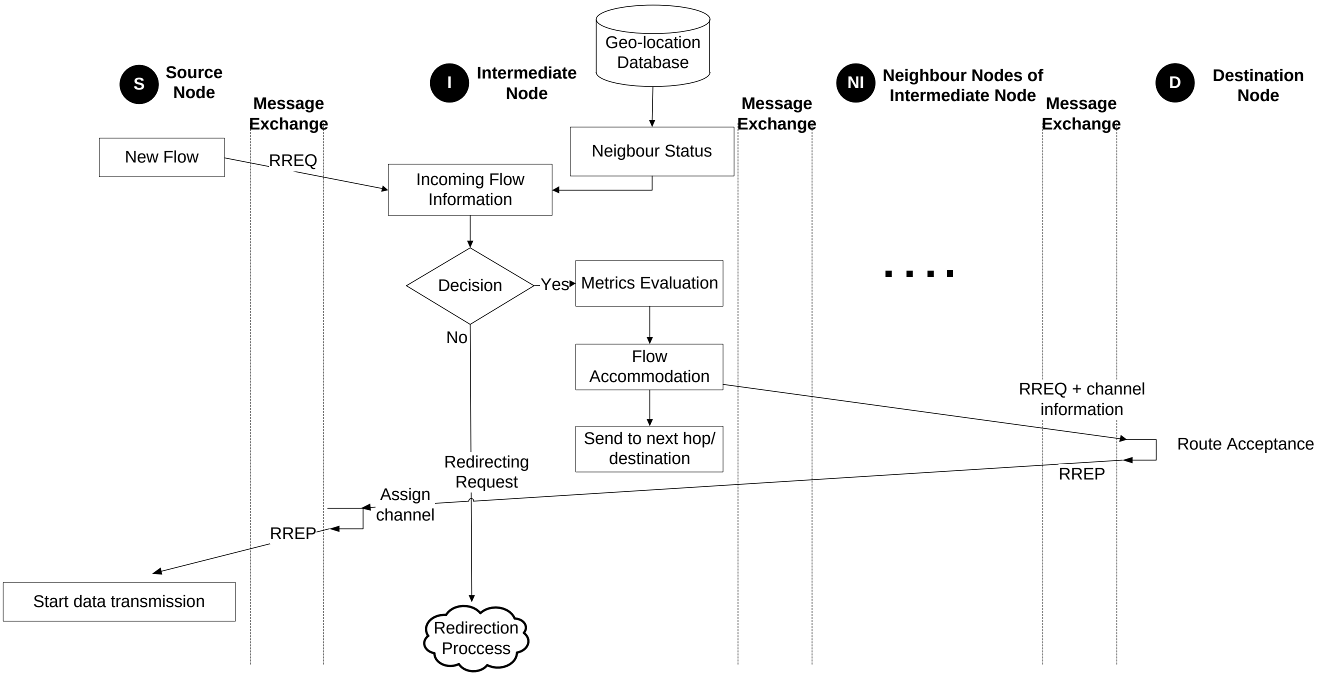


Figure 12: Message exchange process of COGEU routing protocol

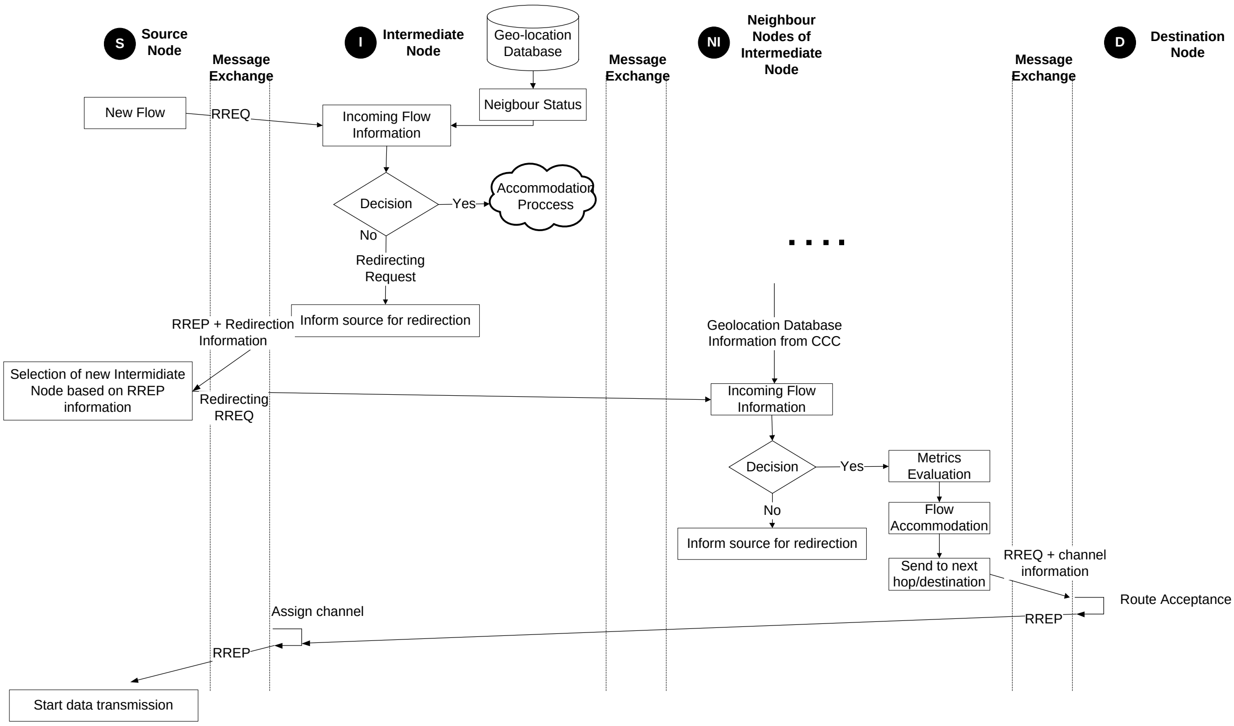


Figure 13: Message exchange process, including redirection

In the case when the intermediate node is not capable to accommodate the incoming flow (i.e. New Flow in Figure 13), an assigning mechanism (redirection process in Figure 13) is in charge of informing the source user, about the neighboring node, which could possibly act as an alternative intermediate node. In such a case, the intermediate node sends a RREP message to the source user, including redirection information. As soon as the source user receives this message, it broadcasts a redirecting RREQ message to the next possible intermediate node, which is then in charge to decide if it is feasible to accommodate the data flow, evaluate the performance metrics and forward it to the next hop. The proposed routing protocol determines a route only when a source user wishes to send a data flow to a destination user. Routes are maintained as long as they are needed by the source user and the exploitation of sequence numbers in the exchange messages guarantee a loop-free routing process.

Furthermore, the proposed routing protocol as a reactive one, creates and maintains routes only if it is necessary, on a demand basis. The routes are maintained in routing tables, where each entry contains information, regarding destination user, next hop, number of hops, destination sequence number, active neighboring nodes for this route and expiration time of the flow. The number of RREQ messages that a source user can send per second is limited, while each RREQ message carries a time to live (TTL) value that specifies the number of times this message should be re-broadcasted. This value is set to a predefined value at the first transmission and increased during retransmissions, which occur if no replies are received.

3.3- Optimization of routing process for COGEU use-cases

The research work that is presented in section 3.2- (see Figure 12, Figure 13) was firstly introduced in deliverable D6.2, while Figure 14 presents an enhancement of the proposed COGEU routing protocol. More specifically, the assigning mechanism aims to alleviate the service load of intermediate nodes, so it is adapted to every intermediate node, which is further able to determine if a neighbor node performs better in the routing path. For this scope, the message exchange process of COGEU routing protocol has been modified, in order to consider the new feature of the assigning mechanism. When a source node initializes a new flow by sending a RREQ, the intermediate node is informed regarding the neighborhood status from the geo-location database through the CCC. Then, the intermediate node evaluates the new flow (i.e. performance metrics) and encapsulates the evaluation result in a message that it is forwarded to all neighboring nodes. This message is the redirecting request signal in Figure 14. Once the neighboring nodes receive a redirecting request, they check its validity with the corresponding flow, ensuring that they are not the source/destination nodes or next-hop nodes of that flow. Then the neighboring nodes initiate a process, in order to evaluate the flow and they send to the intermediate node the result of the evaluation through a redirecting replay message. Once the intermediate node receives the redirecting reply from several of its neighboring nodes it then selects the optimum one, in order to serve/accommodate the incoming flow. Finally, the intermediate node generates a RREP message, in order to inform the source node regarding the new candidate intermediate node, while it also sends a confirmation message to the new intermediate node informing that it is chosen to handle the flow. On the side of the source node, once receiving the RREP, it changes the next-hop node and starts data transmission.

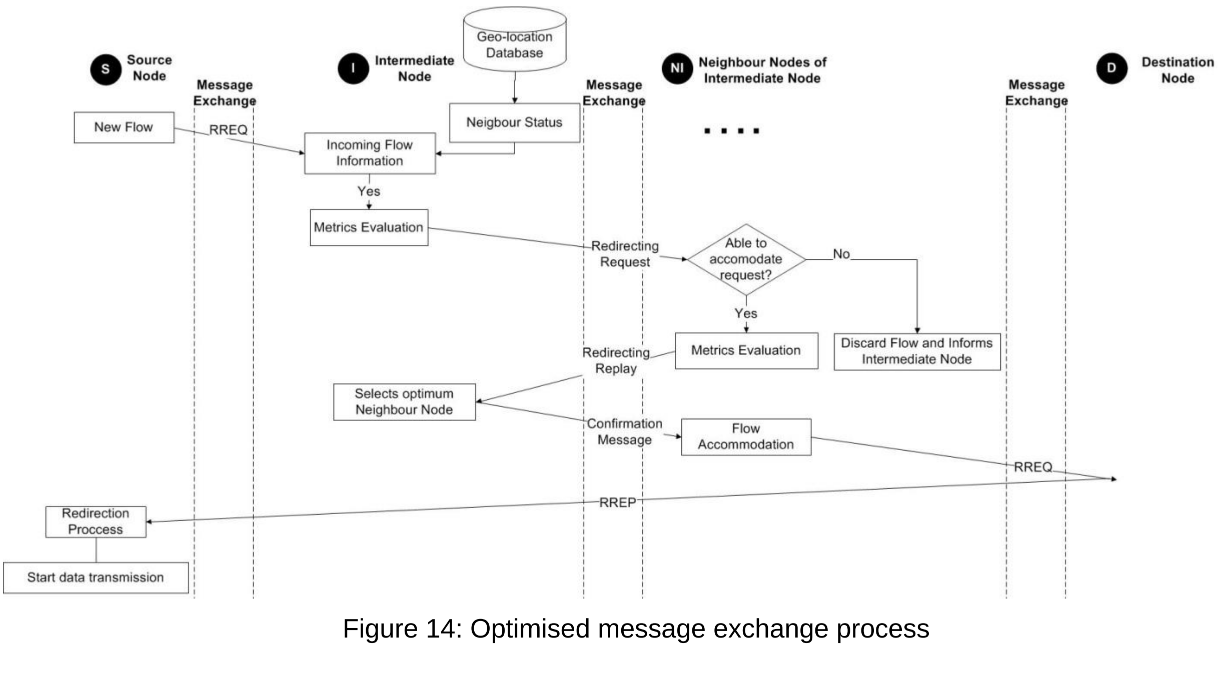


Figure 14: Optimised message exchange process

3.4- Simulation scenario and performance evaluation

Figure 15 depicts the area of Munich in Urban simulation scenario (2.2Km x 2.2Km) used for the final COGEU demonstrator (see D7.3), where secondary public safety network nodes are scattered over geo pixels with different TVWS availability (available through the COGEU geo-location database [13]). Secondary public safety nodes located in this geographical area opportunistically operate using the vacant TV channels available in this Munich area. In this simulation scenario, all secondary nodes (i.e. wireless mesh routers) are possible to act as intermediate secondary nodes in Figure 15. These mesh network nodes are enhanced with an assigning mechanism that enables to determine routing paths between secondary nodes with different TVWS availability in this specific area. Assigning mesh nodes have sensing capabilities and are connected with a geo-location database that includes TVWS availability for all geographical locations. The geo-location database also provides to intermediate communication mesh nodes, data regarding the maximum allowable transmission power that can be used so that no causing interference to primary systems. For this reason an initial study was conducted, in order to compute the transmission power limitations of communications nodes for each TVWS channel. Such an investigation was finalized in the framework of D6.2 for the region of Bavaria in Germany. The main challenge in such an ad-hoc CR network architecture is the spectrum heterogeneity of the available TVWS between neighboring areas, prohibiting secondary nodes to communicate continually, since the spectrum is opportunistic. In such a case, assigning nodes act as intermediate/bridge nodes between source and destination secondary nodes, coordinating data flows and deciding the most optimum routing path that has to be followed.

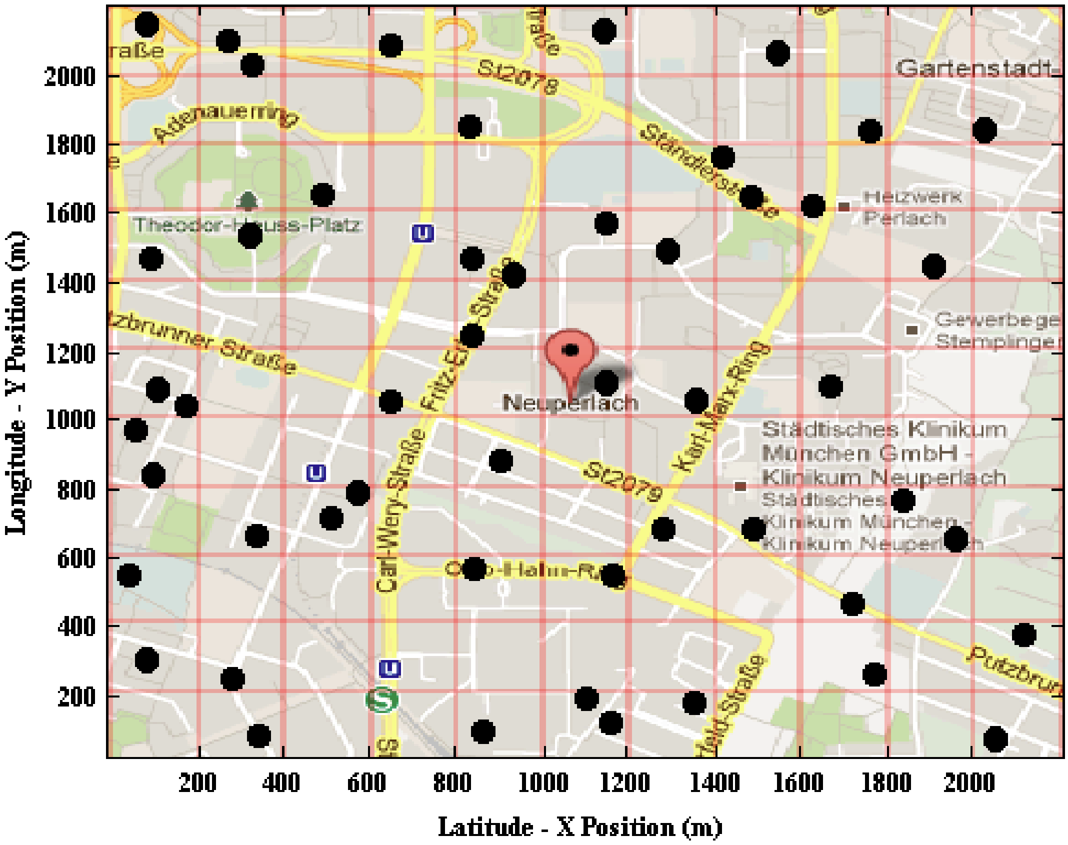


Figure 15: Munich urban-area with public safety network nodes operating over TVWS

Towards verifying the validity of the proposed routing protocol, tests were conducted, under controlled conditions (i.e. simulations). More specifically, in such use-case scenario intermediate nodes are receiving concurrent data flows, stemming from other secondary users, resulting to increased delays. According to this simulation scenario, a number of data flows are contending to pass through the same intermediate node, thus evaluation of delays is crucial regarding the efficient performance of the proposed routing protocol. In this context, a number of delay metrics [15]-[21] that were defined in D6.2 [14] are evaluated, such as switching delay, medium access delay and queuing delay. More specifically, the simulation results below compare the performance of the routing protocol proposed in D6.2 [14], with the enhanced one, by implementing an assigning mechanism that mitigate the service load of intermediate nodes, resulting a routing path that performs better compared to other paths. The delays of the protocols compared based on the number of active flows in the simulation area, the activation probability of an idle Primary System, as well as the distance of the CR source and destination nodes that wish to communicate.

In the area of Munich, the available TV channels, based on COGEU geo-location database [13], varies from 1 to 3 and create inconsistency of spectrum opportunities among secondary nodes. More specifically the available TV channels in this area are 57, 59 and 60 with EIRP from 20 dBm and over. Also, in this area there are more vacant TVWS, but the EIRP/transmission power is too low to operate a secondary system. Simulations were conducted to quantify the performance of both the proposed routing protocols. Up to 50 secondary nodes are randomly distributed over a 2200 m by 2200 m area. The evaluation topology is shown in Figure 16, where the source nodes are on the top and the destination is on bottom. Pairs nodes from S1 − D1 to S10 – D10 represents the flows that are initiated in this simulation scenario, in order to evaluate the protocol under a heavy load. The simulations are contacted in case of the proposed routing protocol, as well as in case of the enhanced routing with the assigning mechanism.

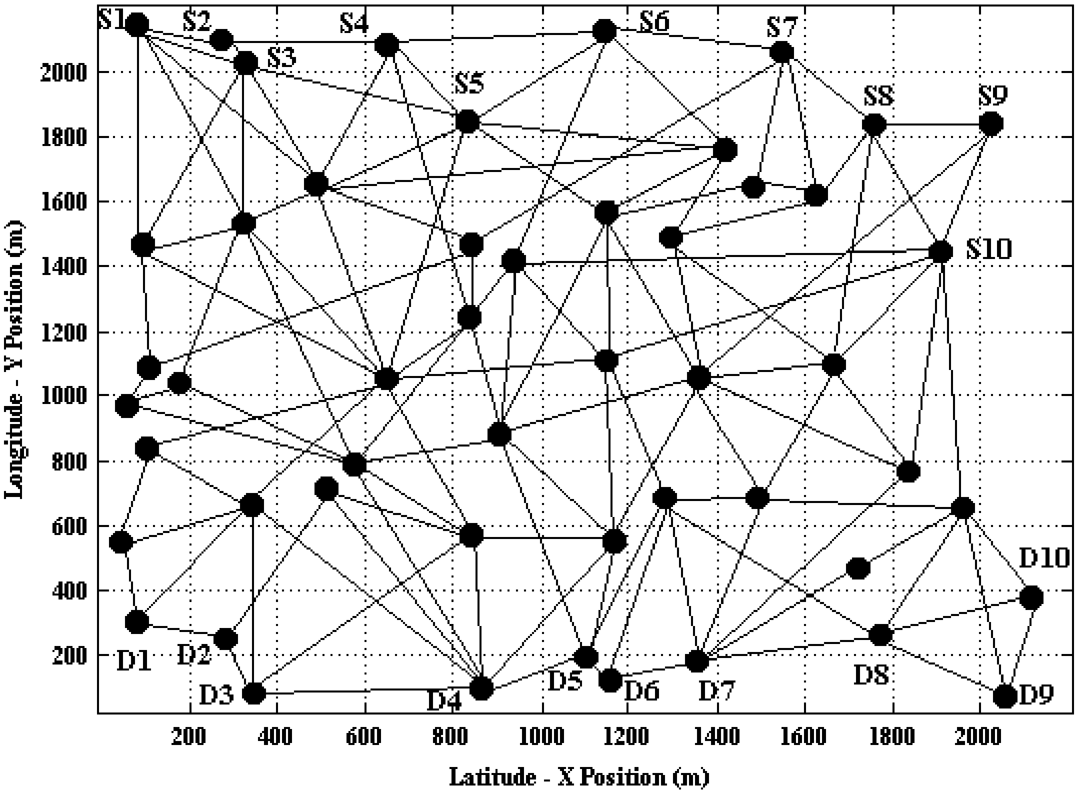


Figure 16: Mesh network topology (simulation scenario)

Figure 17 shows the simulation results and the performance comparison of mean End-to-End Delay while the number of active flows is increasing. It is clear that when routing protocol incorporates the assigning mechanism, heavy service load is distributed around every intermediate node. It has to be note here that when the number of active flows in the network is small, assigning mechanism does not show much advantage, since queuing system is just formed or the load is not heavy enough to launch the flow redirection. However, when the number of active flows exceeds 3, intermediate nodes begin to suffer the accumulating queue, and from then on the flow redirection become necessary. It is also observed that the mean End-to-End Delay increases, in case of the enhanced protocol, due to heavy traffic in the intermediates node queues, so more time is required to process and find the most preferable path. However this traffic is smoother compared to those of the basic routing protocol.

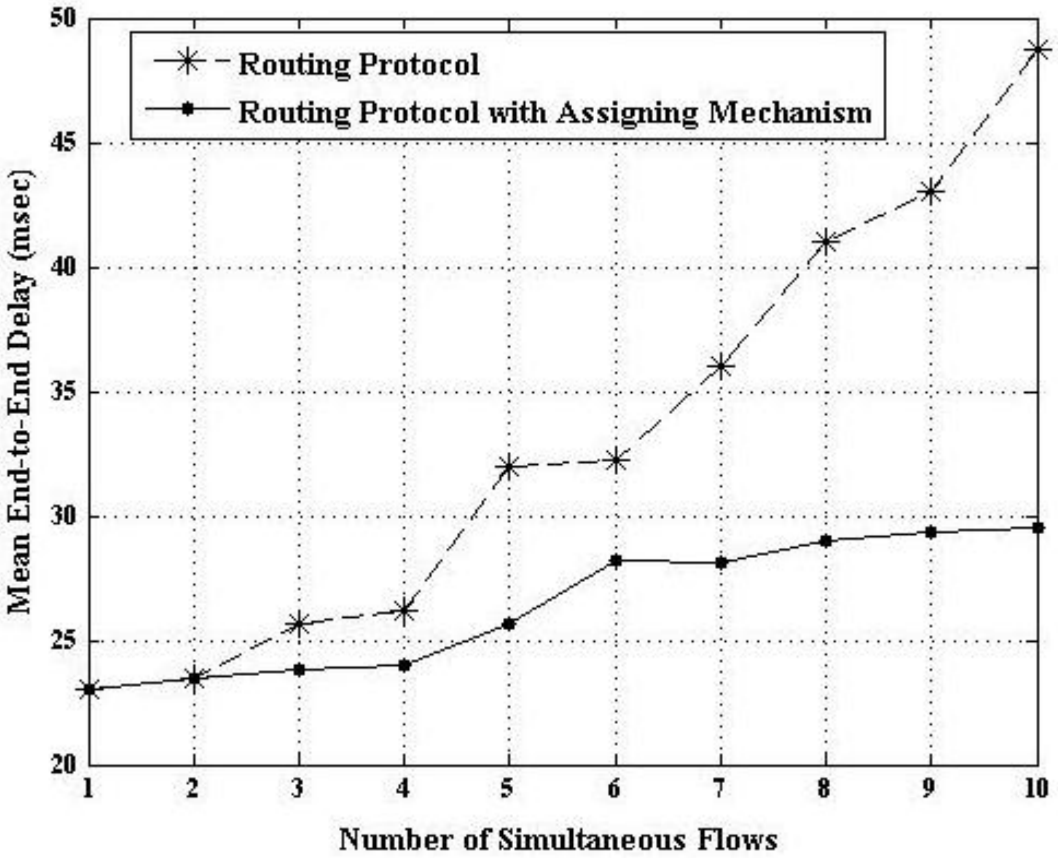


Figure 17: Mean End-to-End Delay for different number of simultaneous flows

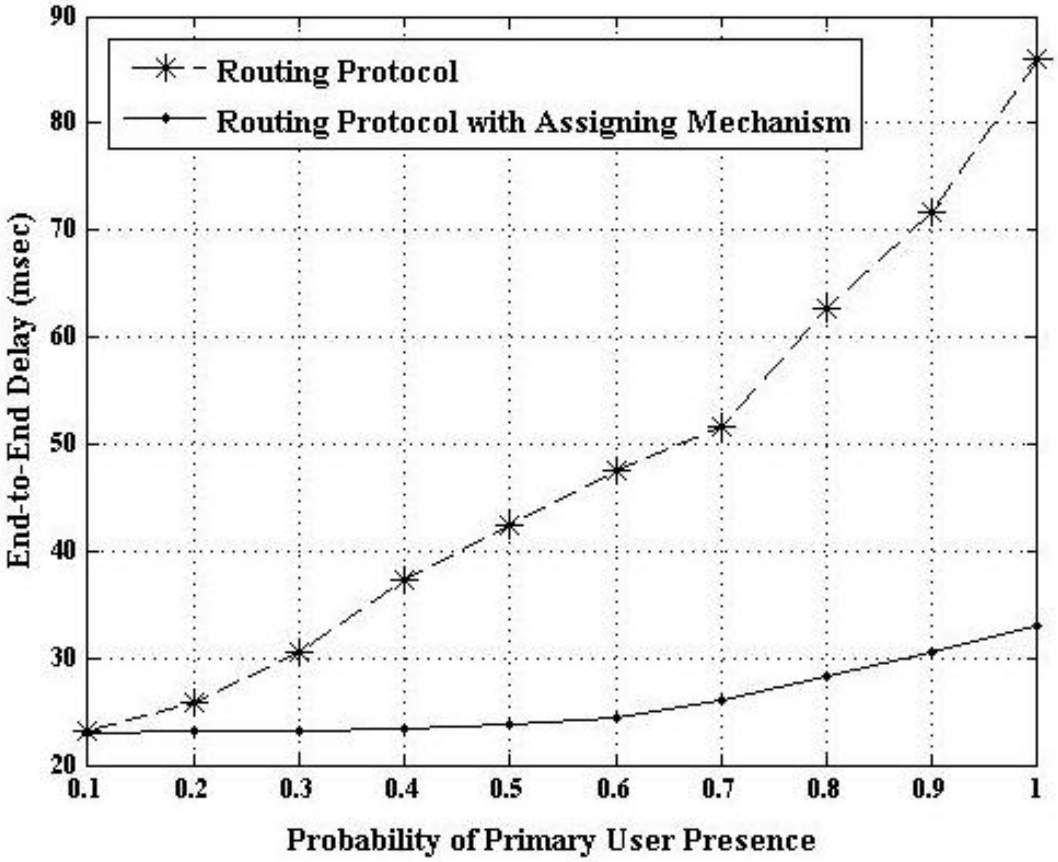


Figure 18: End-to-End Delay for the 1st flow versus probability of PU presence

Figure 18 shows the simulation results of End-to-End Delay of one flow (i.e. 1st flow S1-D1) when the probability of primary user presence increases, while Figure 19 presents the same metric, but in this case each point represents the average of End-to-End Delay for all flows (S1-D1 up to S10-D10) for a certain value of primary user presence probability. Both figures present that, as the probability of Primary users' presence is getting higher, the delay is increasing, while in the case of basic routing protocol the delay increase is more significant. This result is reasonable, since the probability of the presence of an incumbent system is detected as a route failure of the flow, introducing in this way additional delay. Moreover, it is observed that the probability of a primary system presence, affects significant routing procedure in this scenario, as the available TVWS are only 3. This makes difficult to obtain links between secondary intermediate nodes. Therefore, the possible routing paths are high, as the topology of the node is a mesh network, and the assigning mechanism of each node requires enough time to compute the delays of all possible routing paths.

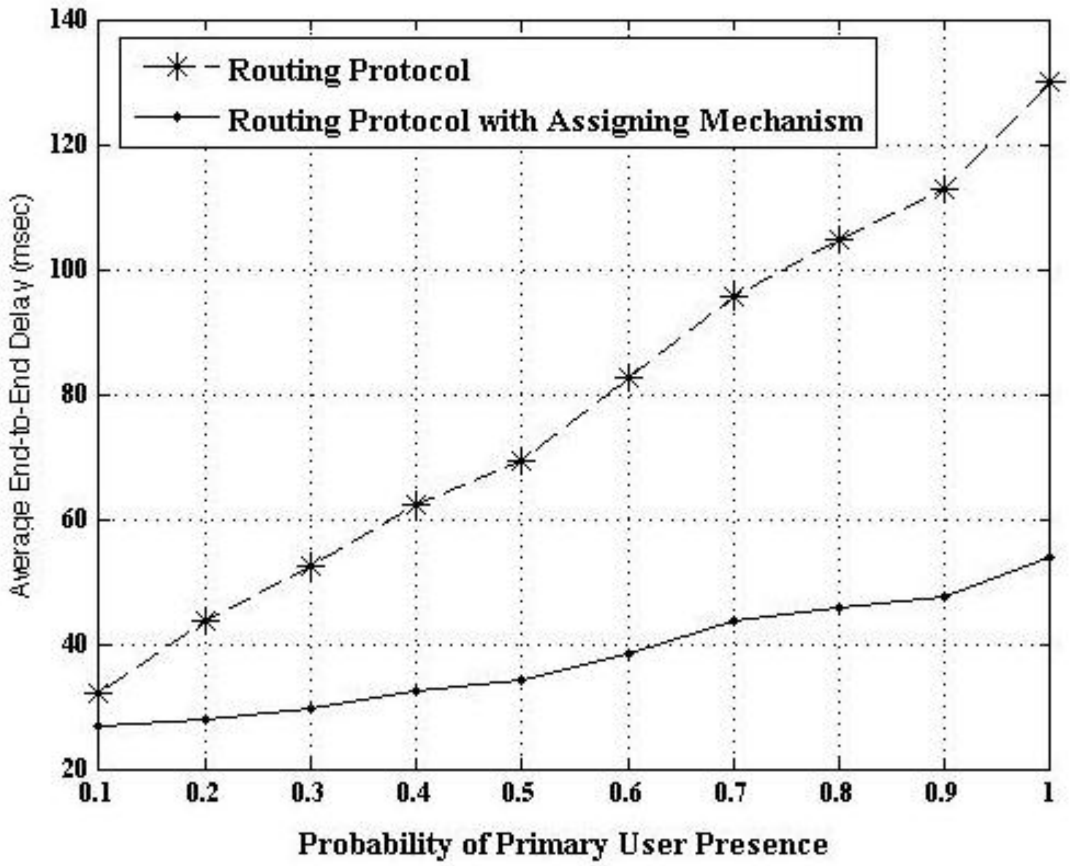


Figure 19: Average End-to-End Delay for all flows versus probability of PU presence

Figure 20 presents the average End-to-End delay that occurred among the source and destination nodes as the distance between them is increased. From Figure 20 it is clear that the distance affects the delay among nodes. This result is reasonable since the longer is the routing path, the more numerous are the primary nodes that affect the path, and the more significant are the effects of the route range/diversity. It is further observed that the basic routing protocol adds higher delays as the distance is increasing rather than those occurred when assigning mechanism is introduced, resulting the most optimal routing path between the source and destination nodes. Consequently, the longer is the path, the more significant are the effects of the route diversity. Finally, Figure 21 shows the comparison among the two routing protocols, under the number of hops that are required in order to make feasible all paths between the source and the destination nodes, for each flow set according to the simulation scenario. This comparison results that the assigning mechanism performs better, as the second protocol makes the decision on every hop instead of the first one.

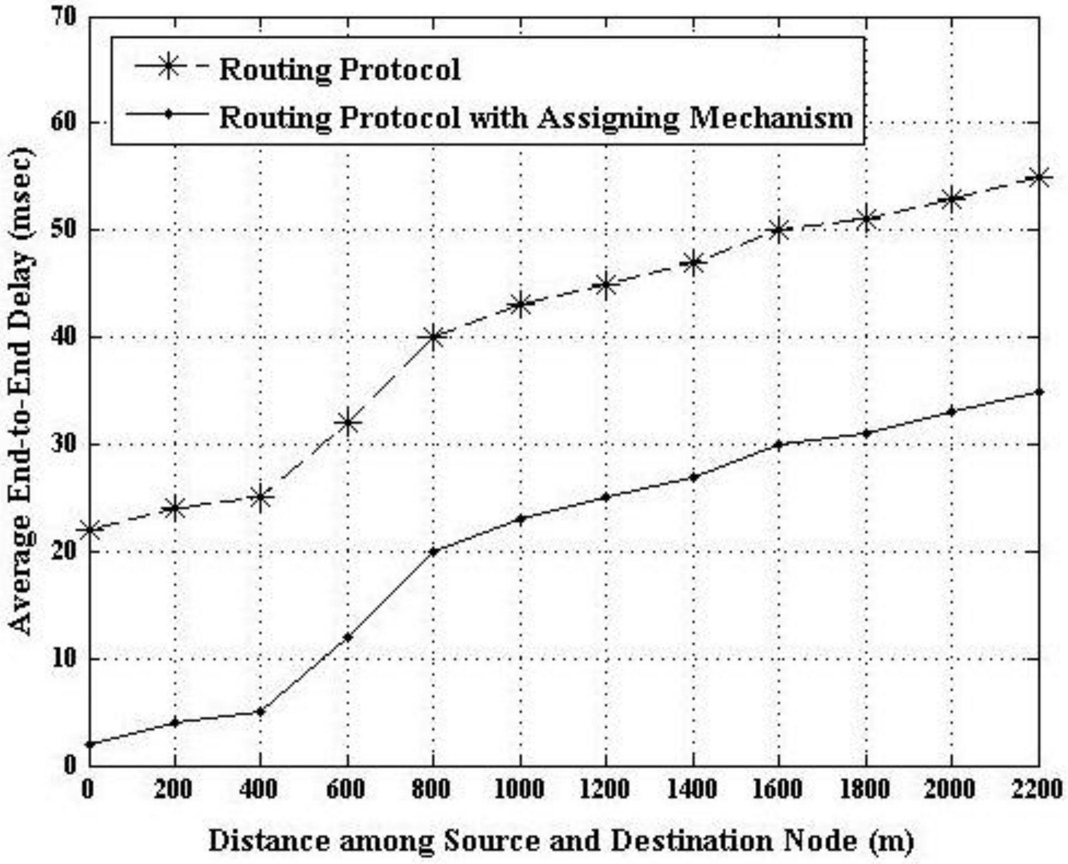


Figure 20: Average End-to-End Delay versus node distance

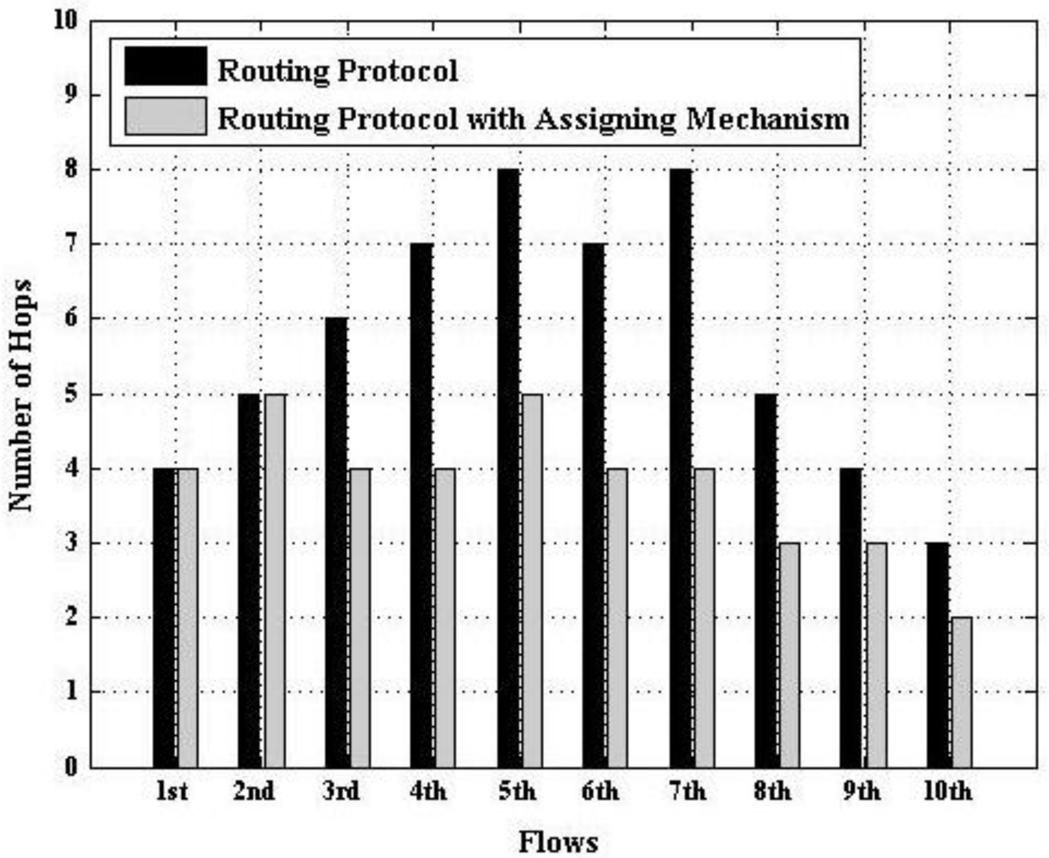


Figure 21:Number of Hops per each flow

4- Transport Protocols for Public Safety Networks over TVWS

As a key asset of mission critical communications, public safety networks technologies are used to offer direct communications capabilities for terminals out of coverage of the infrastructure network.

The 3GPP standardization body has put in place working groups to tackle this particular topic of so called proximity based services for public safety. The 3GPP TSG-SA WG147 [22] working group is progressing on the service level definition. Thales is participating to that working groups and will do so for any other working groups that will serve public safety bodies.

This direct communication between terminals (or User Equipment) is referred to as Direct Mode (DMO), Device-to-Device communication (D2D), Off-Network mode, proximity based services or even “Talk around”. This specific communication scheme between User Equipment (UEs) in the absence of the network has two components:

- Absence of Radio network – radio infrastructure communication down
- Absence of Core network – Cut off between radio infrastructure and Core network (also called Fallback service mode)

For that purpose First Responders terminals products supports direct communications features according to their role in the network: handsets under the same coverage can communicate together over duplex or group calls with Push-To-Talk, relay terminals, usually hosted by vehicles are able to relay full duplex or group calls between handsets forming a **wireless mesh network** (as described in section 3.1-, Figure 10, and Figure 11) while gateways offer dual mode capabilities in order to link handsets in direct communications with the possibly available infrastructure network.

Functional requirements as recommended by NPSTC Public Safety working group [23] on Off-network communications are the key to bring a similar level of services for mission critical communication over a broadband system.

The key issue to operate Direct Mode is the spectrum: what spectrum shall be devoted to such direct communications (is it part of the public safety network infrastructure bandwidth, a separate part within the currently used spectrum for narrow/broad band systems or part of unlicensed spectrum?). In this context, and with recent regulators movements as reported in previous COGEU Deliverables, **TV White-Spaces is a formidable opportunity to overcome those spectrum issues**. Thus, a special kind of wireless mesh networks: Cognitive Radio Ad Hoc Networks (CRAHNs), constitute a viable solution to solve the current problems of inefficiency in the spectrum allocation, and to deploy highly reconfigurable and self-organizing wireless networks that meet mission critical requirements as exposed in section 3.1-,. Thales has been working on the implementation of direct communications for a long time and leveraging its technology & experience in military mesh networks where direct communications are key for tactical radio systems. Whatever the timeframe needed to get a standard for the direct communications, Thales plans to implement the direct mode of operation over an unlicensed waveform (DMO over TVWS is a serious candidate) within the end 2013 release of its ruggedized handset. Of course, the solution will be aligned to the standards as soon as they are available.

At the transport layer, modifications have to be made to TCP in order to efficiently transport end-to-end information in a cognitive radio environment and avoid performance degradation. Congestion control in TCP depends on the packet loss rate and the round-trip-time (RTT). With a wireless link, a TCP sender could misinterpret packet loss due to wireless error as a sign of congestion. As a result, congestion avoidance and slow start mechanisms would be wrongly invoked. Some variants of TCP were proposed to cope with this problem in a wireless environment.

In Cognitive Radio Ad hoc Networks (CRAHN), many factors such as the bandwidth of the spectrum opportunity, co-existence with competing secondary users, and the interference level can affect the packet loss rate. Unpredictable External Interference due to co-existing Secondary Users is illustrated in Figure 22 below. It shows end-to-end information losses introduced by either:

- **Unpredictable External Interferences** due to co-existing secondary users on the unlicensed TVWS spectrum
- **Channel Mobility/Switching**. Changes in TVWS availability. Primary User appears at this location, forcing Secondary users to leave the spectrum.
- **Heterogeneous Channel Bandwidth Availability** (link capacity being related to the number of channels available, it is not constant on the end-to-end path)

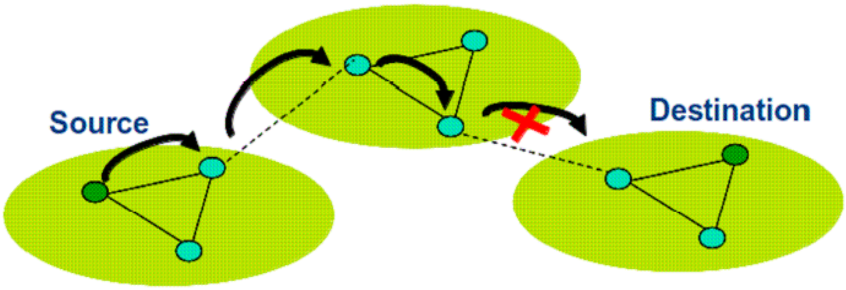


Figure 22: illustration of TVWS CRAHN unpredictability of available radio resources

Similarly, RTT can be affected by the delay due to spectrum sensing, and spectrum switching for which when the current channel becomes unusable for an unlicensed user, the unlicensed user has to search for a new channel. Therefore, the transport layer protocol has to consider these effects to optimize end-to-end rate control.

4.1- Transport Layer Protocols in wireless mesh networks

Standard TCP (i.e, Tahoe, Reno, Vegas, New-Reno) makes assumptions on the nature of the underlying communications layers which greatly affect its performances when deployed on networks for which it was not originally designed for. For example, each packet loss detected (resulting in RTO: Retransmission TimeOut) is considered to be due to network congestion, because wired networks are reliable and have very low bit error rate. However, Multi-hop wireless networks may suffer from non-congestion losses due to high rates of bit errors that lead to corrupted TCP segments, long delays, variable bandwidth, and failures due to mobility of the link.

Different approaches have tried to resolve these problems [24][25][26][27][28], which can be classified into two main categories:

- Split the transport connection: it prevents the TCP sender reduces the congestion window when there is a link error (disconnection due to mobility, transmission error). It deceives the transmitter into believing that the packet was received (false ACK). Snoop module inspects and stores a copy of the packet. There are other similar solutions, including: I-TCP, MTCP, M-TCP. These methods have the disadvantage of losing the end-to-end paradigm transport layers usually adopt.
- Cross-Layer: information from the lower layers is transmitted to the upper layers, so that TCP knows when an error is NOT caused by congestion. For example, Snoop protocol [20] uses this idea to provide a reliable link layer, which is aware of the presence of TCP over it, and inspects each packet, in order to delay or discard some, however , Snoop target wireless networks that have a fixed host (base station). This solution can be considered as a violation of the principle of the model layer, but it proves to be very effective. There are several cross-layer methods that are effective:
    - Explicit Link Failure Notification (ELFN): This notification informs the TCP sender of a link error.
    - TCP-Feedback (TCP-F): as ELFN, it can use error notifications and recovery routes (RFN and RRN).
    - Ad-hoc TCP (ATCP) [29]: Adds a layer between TCP and IP, which has the advantage of being compatible with wired connections.

Performance Enhancing Proxys

PEPs (Performance Enhancing Proxies, see RFC 3135 [30], RFC 3449 [31]) can also be used to improve MANETs. They are attached to a node and provide additional data processing to be sent or received by other nodes. PEPs that do not require a modification of the protocol they seek to improve are deemed transparent. Other generally targets a single layer (usually the transport layer or application layer).

PEPs can be divided into two groups: integrated or distributed. Integrated PEPs operate on a single node, while PEPs can be distributed on both sides of the communication, allowing the use of custom protocols without affecting neither end-to-end data source nor recipient.

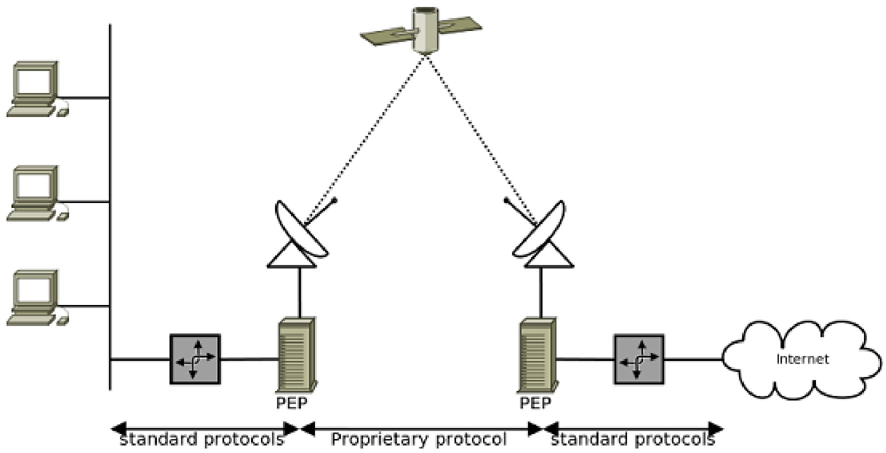


Figure 23:PEP setup illustration

PEPs can be further divided into two categories: symmetric and asymmetric. Symmetric protocol PEP aims to improve the link in both directions, while the asymmetric protocols PEP focus on improving one only direction.

PEPs operate at the transport layer using two different methods to improve communication: they can implicitly sniff the traffic that passes through it, and modify, add or remove packets according to their needs (snoop PEPs), or explicitly become a node in the network and establishing a connection to the end-points (split PEPs). The later has the disadvantage of breaking the end to end connection pattern. In both cases, they are intended to mitigate TCP misinterpretation due the specific communication channel.

Different techniques can be deployed to improve the overall performance of the communication:

- PEPs using split TCP operate without the knowledge end node could have. They can disrupt TCP connections with large RTTs. In TCP, RTT is generally estimated on the fly by calculating a centroid of the value of the old and the new RTT. RTT measurement, weighted by a coefficient intended to amplify rapid adaptation to changes in time, or contrary to be immune to occasional peaks or collapses.
- ACK Filtering or ACK deleting is used in networks where the TCP acknowledgment is the limiting factor. Acknowledgments are filtered or deleted. This type of PEP is particularly used in highly asymmetric links.
- Snoop type PEPs are usually integrated proxies that duplicate ACKs caused by interference or collisions. This method is used in wireless networks. ACKs are deleted and lost packets are retransmitted. The objective of this strategy is to hide possible losses to the TCP sender, so it does not reduce TCP window size when it is not necessary. Without this ACK “interception” TCP could indeed mistakenly think that this loss was due to congestion.
- D-proxies are similar to snoop, but use a more proactive approach: they monitor TCP sequence numbers instead of simply interested in acquittals.
- PEPs can also be used to make a connections more efficient in case of trouble on the link, eg, M-TCP [32] maintains TCP connection alive when temporary wireless disconnections occur.

4.2- **Transport layer protocols in Cognitive Radio Ad-Hoc Networks over TVWS**

TVWS Devices acting as Cognitive radio (CR) devices are envisaged to utilize the spectrum in an opportunistic way by dynamically accessing different licensed portions of the spectrum. To this aim, most of the recent research has mainly focused on devising spectrum sensing and sharing algorithms at the link layer, so that TVWS devices can operate without interfering with the transmissions of other licensed users, (PUs). However, it is also important to consider the impact of such schemes on the higher layers of the protocol stack, in order to provide efficient end-to-end data delivery.

For the usage area targeted in the introduction of the section (DMO over TVWS forming a Cognitive Ad-Hoc Network), resilience and capacity are mandatory characteristics tackled using multiple radios capable of operating on a diverse set of channels. Deploying such 802.11a/b/g based networks in dense urban areas leads to several problems of interference and coexistence with existing equipment as such networks typically operate in the unlicensed ISM bands.

Fluctuations in wireless channel quality and congestion are the main high-level problems that affect the performance of transport layer protocols in those networks. Moreover, at the end nodes, the transport layer has limited information about reasons for packet loss. Therefore, packet loss due to interference caused by external Secondary users may be wrongly interpreted as congestion, resulting in unnecessary throughput degradation. Several studies have been undertaken to optimize TCP for such wireless (multi-hop) environment, mostly focusing on improving the performance problems introduced due to node mobility and route breaks.

Slingerland et. al. [33] analyzed TCP performance in dynamic spectrum access (DSA) scenarios using a single hop cognitive radio access network such as considered by e.g. IEEE 802.22 WRAN. Felice et al [34] evaluated various TCP versions such as TCP Reno, New Reno, Vegas and Sack in a cognitive multi-hop ad hoc network under varying PN workload, sensing duration and heterogeneity of channel bandwidth. However, they do not consider the impact of channel switching on TCP performance and ignore the impact of channel (re-)assignment on performance.

Chowdhury et. al. [35] proposed a new transport layer protocol, TP-CRAHN for cognitive ad hoc networks. TP-CRAHN uses additional states considering different effects from cognitive ad hoc networks, such as delay from spectrum sensing or spectrum mobility. Due to the additional states and messages, it is complex to implement and requires Additional buffer space information along the path. Sarkar et al [36] proposed TCP Everglades (TCPE) for single-hop cognitive radio networks. Authors assumed spectrum sensing duration is longer than RTO and extended TCP Westwood with several rules of a knowledge based module that decides TCP operation. As TCPE is designed for a single-hop cognitive wireless environment, it is not appropriate for multi-hop wireless cognitive radio based networks where channel switching, spectrum mobility and interference due to primary users happen frequently along multiple links.

4.2.1- *Challenges considered for COGEU use-case*

From State-Of-The-Art analysis, the most challenging issues identified can be summarized to:

- **Unpredictable External Interference**: Due to co-existing Primary/Secondary users in the unlicensed TVWS band creating interferences, transmissions in the CRAHN may face heavy packet losses. Such packet loss can lead to TCP misinterpretations of the nature of the losses. This may result in low TCP throughput due to frequently triggered slow-start.
- **Heterogeneous Channel Bandwidth Availability:** When a node change the receive channel on the R1, the new channel may show a significant available capacity in-crease. However, due to the TCP congestion avoidance scheme, the congestion window does not ramp up fast enough to immediately utilize the available bandwidth, leading to unnecessarily low throughput.
- **Channel Mobility/Switching:** During channel switching (aiming at leaving a “now occupied”/ “previously unoccupied” channel) CRAHN links become disconnected, leading to potential packet loss. A delay is introduced by packets arriving to the receiving interface and queued at the correct channel queue for the next hop. If a node serves many neighbors, there may be a potential large switching delay until a given specific channel is served again. Such large delay can be detrimental to TCP performance as the number of intermediate forwarding nodes in the path increases. This is because channel switching jitter distortes RTT estimates and negatively affects RTO and throughput.
- **Spectrum Sensing:** For the channel assignment, CR devices estimate PUs traffic workload based on spectrum sensing. However, during such cooperative sensing nodes are not able to transmit, potentially leading to TCP retransmit timeouts (RTO). There is a trade-off between estimation accuracy and sensing overhead. To reduce the total sensing time, CR devices can exchange sensed channel workload information. Such collaboration among CR devices can decrease the required sensing window, which eventually may improve TCP throughput.

4.3- Hop-by-Hop transport protocol (HBH) for CRAHN over TVWS

Results from State-Of-The-Art showed that two types of solutions have been developed so far: those who try to modify some aspects of TCP, for example through the use of PEP proxies and those offering a completely new protocol for congestion control and reliability as an alternative to TCP.

In the context of COGEU use-cases and challenges associated, we found interesting to investigate in-between these two alternatives, by developing an architectural proposal based on distributed PEP proxies: since we control and can deploy our solution on all nodes in the network (nodes are deployed in a usually very controlled Public Safety Network) we have the flexibility to create a new protocol more adapted to each intermediate CRAHN nodes, while providing standard interfaces to applications, so that they do not need to be changed (keeping standard TCP sockets at application level).

4.3.1- *Proposed solution and TVWS Spectrum awareness objectives*

The main objective is to provide a better use of CRAHN in TV White-Space environment in terms of bandwidth, latency and fairness, without disrupting the operational applications used by first responders. Technically, this is done by positioning our solution just below OSI layer 4 to add information to improve the choices made by the network. As highlighted earlier in this document, legacy transport protocols are poorly adapted to the specificities of CRAHN. We then aim at **increasing the reliability perceived from the point of view of the application layer** (or another TCP running on top of our solution) in CRAHN. Moreover, in the case where the reliability can be improved locally, it prevents unnecessary use of network resources by **pushing internal losses to the source of incoming flows**. Consequently, our solution has two main mechanisms that ensure the quality of the perceived link:

1. **Hop by hop reliability** tuned using spectrum knowledge

2. **Hop by hop Back-pressure** to prevent congestion

The general idea is to improve the perceived quality of the network by taking functionality usually used by end-to-end TCP, and implement congestion control, and reliability mechanism hop-by-hop. This results in a separation between management of link errors and congestion control, in order to react efficiently to environmental stimuli like losses induced by lower layers of the CRAHN.

Reliability setting can be adjusted in order to adjust to spectrum availability. This mechanism is introduced thanks to the pro-active knowledge provided by interrogating a TVWS Database (or COGEU TVWS occupancy repository). This way we intend to resolve the “Unpredictable External interference problem” by requesting in advance of the session, the number of secondary users competing for the spectrum. Effectively, this is done by dynamically adjusting a parameter R_2 (Max number of retransmissions). Prediction of a perceived percentage of losses encountered on links is based on the number of Secondary users registered in the database and competing for spectrum in the available TVWS channels.

Back Pressure notification introduced is also “Spectrum Aware”. It aims at avoiding unnecessary losses in the network when we know the frequencies availability (and thus capacity) will not be constant on the flow path. With this mechanism we intend to solve the “Heterogeneous Channel Bandwith Availability” problem. Congestion notification could also be used as a way to prepare the end-to-end session in the case of dynamic variation of spectrum availability.

4.4- HBH protocol design for transport over TVWS

HBH is composed of two distinct parts. The first aims to intercept a packet when it enters the CRAHN (interception module in blue in Figure 24), and, likewise, to return when it comes out. This part is installed at the end-points of a CRAHN (at the gateway). The second part, which is the most relevant work of HBH, consists of a hop by hop transmission in the network nodes, using our own protocol, based on IP and implementing the Back-pressure congestion control and hop-by-hop reliability. The second part will be presented in the next section.

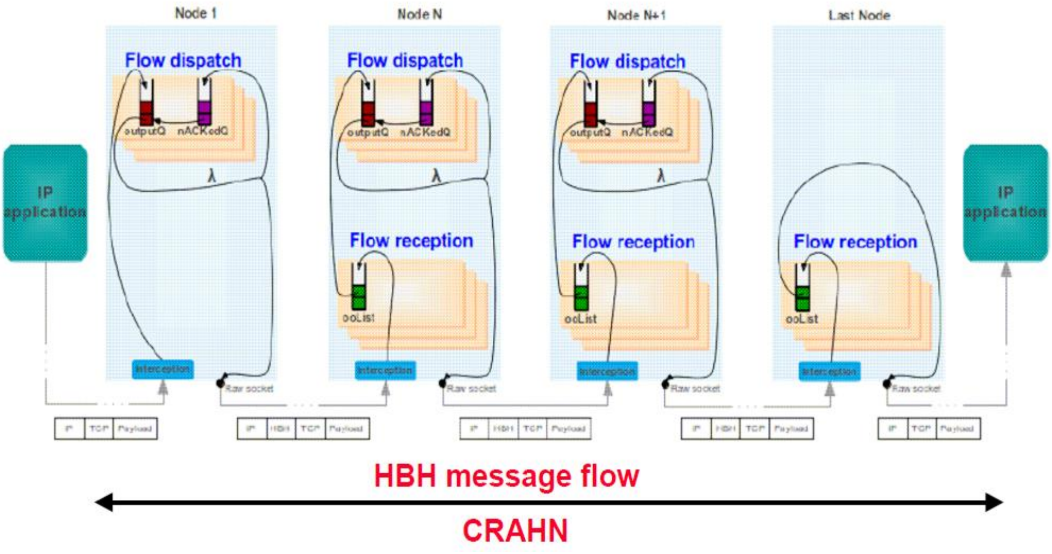


Figure 24 : HBH (Hop-by-Hop transport protocol) message flow.

HBH protocol intercepts all unicast IP packets that reach the considered Cognitive Radio Ad-Hoc Network or that are emitted inside this CRAHN (see Figure 24). HBH then encapsulates IP packets into a HDM message by adding HBH header protocol, which is inserted between the headers of layers 3 and layer 4. Similarly, the last node in the CRAHN must de-encapsulate the HBH header before sending HBH packets. As HBH is not a “legacy” transport protocol, a raw socket should be used to forward packets to the next node. HBH does not interfere with the routing protocol, which independently selects the next node to which the packet should be transmitted.

4.4.1- *Macroscopic description of HBH*

For such a protocol to succeed in his task, monitoring data should be carried on each hop (i.e. between two consecutive nodes of the network).

HBH control information is added to each packet as a header that follows the IP header. Then the payload delivered by HBH is the actual IP packet content (this header is placed between the layer 3 and layer 4). The packet is then transported hop-by-hop using the default IP routing.

Data flow is unidirectional from a source to a destination (these nodes at the ends may or may not, within the CRAHN) and locally between a node N and node N+1, hereinafter respectively called 'sender node and 'receiver node' (or simply 'sender' and 'receiver').

There are two types of PDUs (Protocol Data Unit) defined by the proposed HBH protocol:

- HDM (HBH Data Message)
- HAM (HBH Acknowledgment Message).

For simplicity, they have the same structure as described in next section 4.4.4-.

In the remainder of this section, is described the specification of HBH protocol and structure of HBH packets.

4.4.2- *Hop-by-hop spectrum-aware reliability mechanism*

Hop-by-hop reliability is ensured by robust retransmission until the transmission succeeds or until the robustness metric reaches the expectation of ρ parameter (e.g., the maximum number of retransmissions R_2 has been reached). The receiving node must keep memory of out-of-order packets received, via “ooList” list in order to ensure reliability. The source has the option of requesting the receiver to clear this list (with the Reset RST option), for example in the case where the source has exceeded the maximum number of allowed retransmissions and decides to drop that packet.

In addition, HBH provides the ability to acknowledge multiple packets at a time (cumulative acknowledgments), to reduce the amount of control messages needed. HBH is therefore a sliding window protocol. The window size W is measured in packets and only manage reliability (but not the flow itself, which is regulated by the mechanism of back-pressure). W is updated at each RTT by AIMD (Additive Increase / Multiplicative Decrease). It has a minimum and maximum value, which are small and close, (considered equal for the rest of this study).

Finally, a Selective Acknowledgment (SACK) feature is provided to avoiding unnecessary retransmission of out-of-order packets. With selective acknowledgments, the data receiver can inform the sender about all segments successfully arrived, so the sender only needs to retransmit the segments actually lost.

Figure 25 illustrates the interests of reliability mechanisms described above by various examples. In this figure, the size of the window W is 3 and the number of retransmissions allowed R_2 is 1.

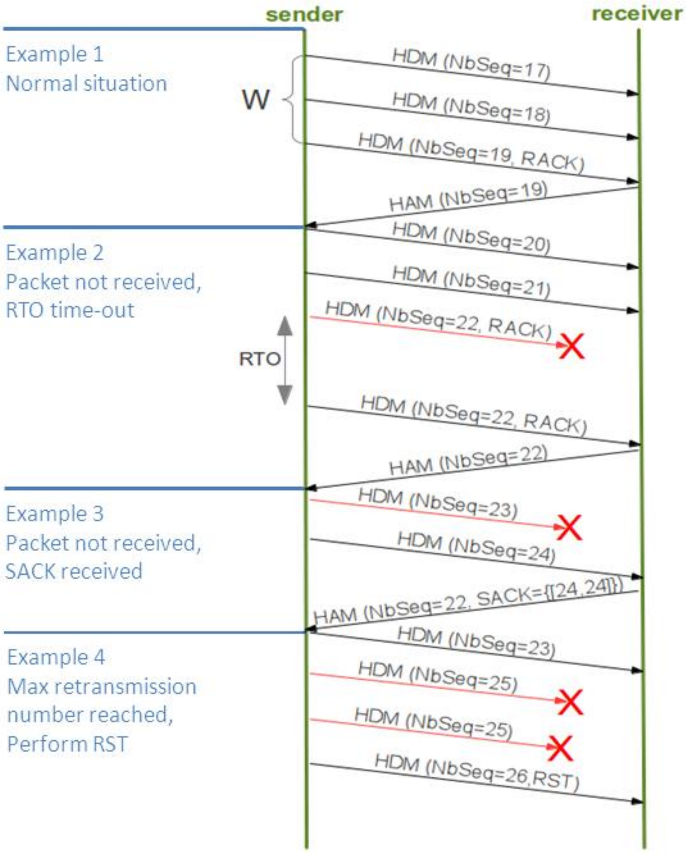


Figure 25:Reliability mechanisms examples.

In Example 1, a single HAM (HBH acknowledgment message) is sent for three HDMS (HBH Data Messages) received. This illustrates cumulative acknowledgment.

In Example 2, the retention period expires and causes the loss of message with sequence number 22.

In Example 3, packet 24 is sent before the packet 23 (which is lost), then the receiver informs the sender (while forwarding to the next node). This illustrates selective acknowledgment.

In Example 4, maximum number of retransmissions R2 is reached. Sender decides to drop packet 25. It informs the receiver it must reset “ooList” using the RST option. Dynamically adjusting the maximum number of allowed retransmission based on Co-existence information provided by a TVWS geolocation database or COGEU TVWS occupancy repository can theoretically improve the performances of the retransmission scheme. It is similar to knowing in advance the packet loss ratio experienced on each link.

4.4.3- *Hop-by-hop Back-pressure mechanism*

Back pressure is a congestion control mechanism. Unlike TCP dealing with congestion on a end-to-end basis, Back pressure intends to relay congestion control notification using a hop by hop scheme.

Back-pressure mechanism works by sending congestion control notification from the receiving node to the sender node as a HCN flag (hop by hop Congestion Notification) inside a HAM. This indicates that HCN packets do not leave the receiving node as fast as they enter it, causing an accumulation of packets on the receiving node, and thus congestion. This message is sent back to the sender whenever a threshold S_1 is reached in the output queue of the considered receiver node. However, incoming messages are not ignored as the length of the queue outputQ do not reaches its maximum size $L\ (\geq S_1)$. One could also consider implementing a second threshold $S_{2,}$ in order to notify the end of the congested state.

Sender, upon reception of a HAM HCN flag, reduces its sending rate in relation to its internal parameterλ, regulating the number of packets transmitted per unit of time.

Two congestion avoidance modes can be defined. When sending the first message, we enter the initial mode and the data is sent as soon as possible by layer 2. When the first back-pressure message is received, we enter the continuous mode, in which λ controls the sending rate.

In continuous mode, λ is computed using AIMD (Additive Increase / Multiplicative Decrease). When switching between the two modes, λ is initialized to the instantaneous flow rate, which is continuously estimated by a moving average.

Back Pressure notification introduced is also “Spectrum Aware”. It aims at avoiding unnecessary losses in the network when we know the frequencies availability (and thus capacity) will not be constant on the flow path. With this mechanism we intend to solve the “Heterogeneous Channel Bandwidth Availability” problem.

4.4.4- *HBH messages structure definition*

HAM and HDM message structure (see Figure 26):

- **TPE:** Represents the PDU TYPE (HDM or HAM). This bit is 0 for HDM, and 1 for a HAM.
- **RQT:** Request special packet. For HDM, it represents RACK flag (Request Acknowledgment), and for HAM it represent the HCN flag.
- **OptionValue:** Represents SACK options for HAM. A SACK option is set to 0b000000 if it is not used, (63 pairs of intervals can be selectively acknowledged). For HDM, it represents the RST flag (first bit of the field) and the optional FEC option (Remaining 5 bits). The RST option (ReSeT) can explicitly ask receiver to reset the variable rcvNext and to clear ooList.
- **SeqNb:** for HDM, it contains a sequence number. For HAM it is the acknowledgment number.
- **flowid:** Contains a unique ID for a flow. This value is set hop by hop). It is calculated from the 5-tuple (IPSrc, IPDest, PortSrc, PortDest, TransportProtocol).
- **Checksum:** Contains the checksum of the header and payload.
- **OrigProto:** protocol version of original transport protocol.
- **Reserved:** Reserved for future use.
- **Data:** for HDM, it contains Layer 4 protocol data (header and payload). For HAM it contains the intervals SACK options (if OptionValue is set to 1).

<table>
<tr><th>Offsets</th><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet</th><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td>TPE</td><td>RQT</td><td colspan="6">OptionValue</td><td colspan="8">SeqNb</td><td colspan="16">FlowID</td></tr>
<tr><td>4</td><td>32</td><td colspan="16">checksum</td><td colspan="8">OrigProto</td><td colspan="8">Reserved</td></tr>
<tr><td>8+</td><td>64+</td><td colspan="32">Data</td></tr>
</table>

Figure 26: Hop by Hop protocol header.

4.4.5- *Internal HBH variables*

Many variables are registered both at sender and receiver sides. Below is their definition split in three categories: Internal global variables, Flow related internal variables, and Packet related internal variable.

Internal global variables:

- **MaxReord:** Maximum number of HDM in a given flow.
- **MaxMem:** Maximum memory allocated to inputs/outputs buffers.
- **R_1**: Number of retransmission trials before informing the routing protocol, if applicable.
- **R_2:** Number of consecutive retransmissions before discarding the packet.
- **MaxSocks:** maximum number of flow that can be simultaneously managed
- **ρ:** Parameter to set the desired reliability. This value can be sent inside the header of HDM. It impacts, among other things, R_1 and R_2.
- **S_1:** threshold triggering the sending of congestion control notification HCN.
- **S_1:** if OutputQ goes below this threshold, an explicit message is send to notify the end of the congested state.
- **L:** outputQ maximum size.

Flow related internal variables

- **Flowid:** unique ID to identify a flow.
- **rcvNext:** next sequence number expected by receiver.
- **currentSeqNumber:** current sequence number.
- **srtt, RTTVAR, RTO:** Variables used to calculate an estimated RTT (and RTO). This calculation contains two constants $g = \frac{1}{8}$ and $h = \frac{1}{4}$ to define the relationship between old and new RTT. A constant n = 4 aims to define the relationship between RTT and RTO. Relations are as follows (where M is the new RTT measurement):

$$\begin{array}{rcllcll} srtt & \leftarrow & (1-g) & srtt & + & g & M \\ rttvar & \leftarrow & (1-h) & rttvar & + & h & |M - srtt| \\ RTO & \leftarrow & & srtt & + & n & rttvar \end{array}$$

- **λ:** Parameter (in bit / s) to limit sending rate to the next node in the congestion avoidance mode. This parameter uses two constants p and q to define the relationships between old and new λ). It is computed using AIMD:

$$\lambda \leftarrow \begin{cases} \lambda & + \quad p \quad \text{at each RTT} \\ \lambda & \cdot \quad q \quad \text{at each HCN received} \end{cases}$$

- **W:** size of the window (measured in packets).

Packet related internal variable

HDM and HAM consist of a header and a payload, and all non-Acknowledged HDMS (HBH Data Messages) are buffered by the sender. Two internal parameters nbTx and stime are kept by the sender to keep a memory the number of retransmissions already made for this packet (see parameter ρ), and time at which this transmission took place, in order to tune time-outs.

4.5- Design of the HBH implementation

As stated earlier in this document (section 4.3.1-), the HBH implementation aims at providing two innovative features for CRAHN: reliability and back-pressure congestion control mechanisms.

Indeed, we believe finely tune reliability parameter (R_2) depending on the spectrum availability would benefits end-to-end transport of information, and reaction to inevitable losses. The use of COGEU TVWS occupancy repository (or a simpler geolocation database access) will provide current information about the spectrum use along the path taken by flows in the CRAHN, and the possible presence of competing secondary users. Then, Back-pressure congestion control mechanism, triggered by the spectrum awareness introduced will avoid unnecessary losses in the network when we know in advance the number of TVWS channel availability (and thus path capacity) along the path. With this latest mechanism, the goal being to prevents unnecessary use of network resources by pushing losses to the source of incoming flows (instead of losses occurring inside the CRAHN).

4.5.1- *HBH Design description*

HBH protocol intercepts all unicast IP packets that reach the considered Cognitive Radio Ad-Hoc Network or that are emitted inside this CRAHN (see Figure 24). HBH then encapsulates IP packets into a HDM message by adding HBH header protocol, which is inserted between the headers of layers 3 and layer 4. Similarly, the last node in the CRAHN must de-encapsulated the HBH header before sending HBH packets. As HBH is not a "legacy" transport protocol, a raw socket should be used to forward packets to the next node. HBH does not interfere with the routing protocol, which independently selects the next node to which the packet should be transmitted.

As illustrated in Figure 27, dealing with flows in HBH is divided into several parts: one is responsible for receiving packets (Packet interception module), another is responsible for sending them (Output queue module). Each stream (identified by flowid in the flow manager module) has its own queue in the so called transport relays.

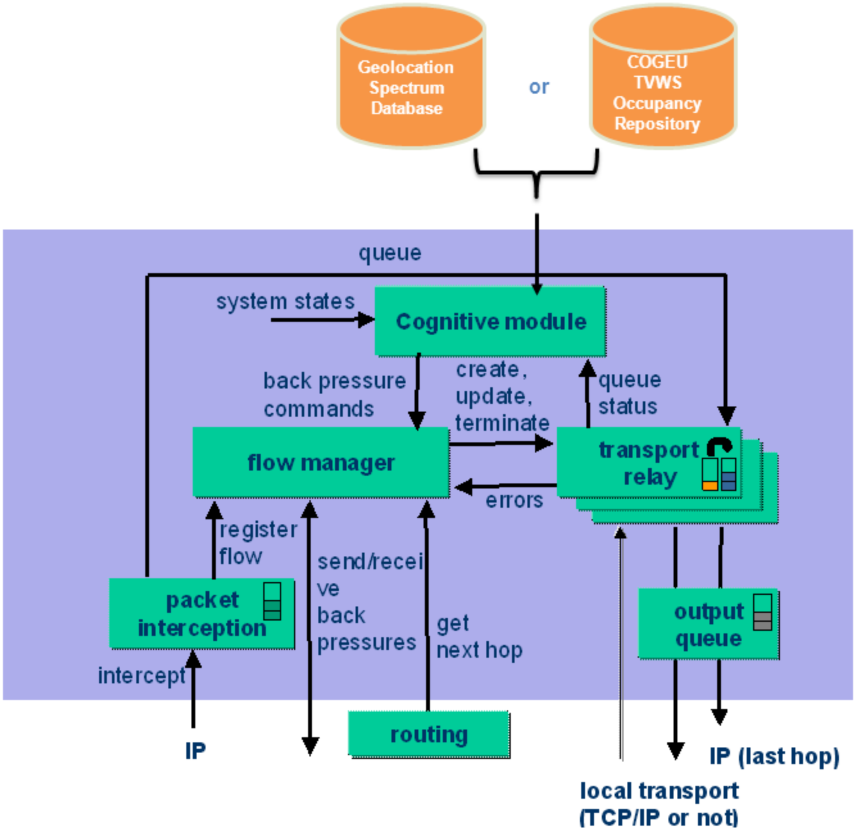


Figure 27: HBH node implementation.

Packet interception module intercepts IP packets entering the network and registers data flows to the flow manager module. Packets belonging to already registered flows are send to the transport relay (flow dispatch operation). The flow manager module maintain a list of flow and holds the sequence number of packets that have been received out of order (ooList already introduced in previous section). This list is required in order to send HAMs with the appropriate information. Packets themselves are not kept in the queue: they are immediately forwarded to the next node, because packet reordering is not a feature needed for HBH.

The **Flow manager module** keep status about active flows currently transiting inside the considered node. For each new flow, a treatment is achieved resulting in the instantiation of **transport relays** implementing a logical HDM/HAM reception (more information available in the UML diagram of esction 4.5.2-). Updates of flows status are then managed while the **cognitive module** can trigger events related to environmental stimuli. The cognitive module have access to environmental data that can be external to the considered system (sensing information, spectrum availability, resource allocations strategies). It is also responsible for sending back pressure notifications triggering congestion control (via reception of HAM messages with HCN flag) in intermediate nodes.

The **output queues module** contains two different queues:

- The outputQ stores packets that are ready to be sent, but are waiting because either a slot in the W window (when it is already full), or because current sending rate is above rate allowed by λ (the internal parameter controling the sending rate according to the perceived congestion).
- The queue of unacknowledged packets (nACKedQ) stores a copy of packets that were sent but not acknowledged yet (in the case a retransmission would be necessary).

4.5.2- *HBH implementation details*

All IP packets are intercepted in the interception module. This module can decide to discard the packet, let it run its course (eg, in the case where it is not unicast), or use the HBH protocol for transport to its destination. If the intercepted packet is already a HBH packet, it is given to the appropriate HDM / HAM reception module (via flow manager). The HBH packet is then transmitted to the module in charge of sending HDM packets. The module in charge of sending HAM is also called if necessary (see Figure 28 illustrating IP reception and new flow management).

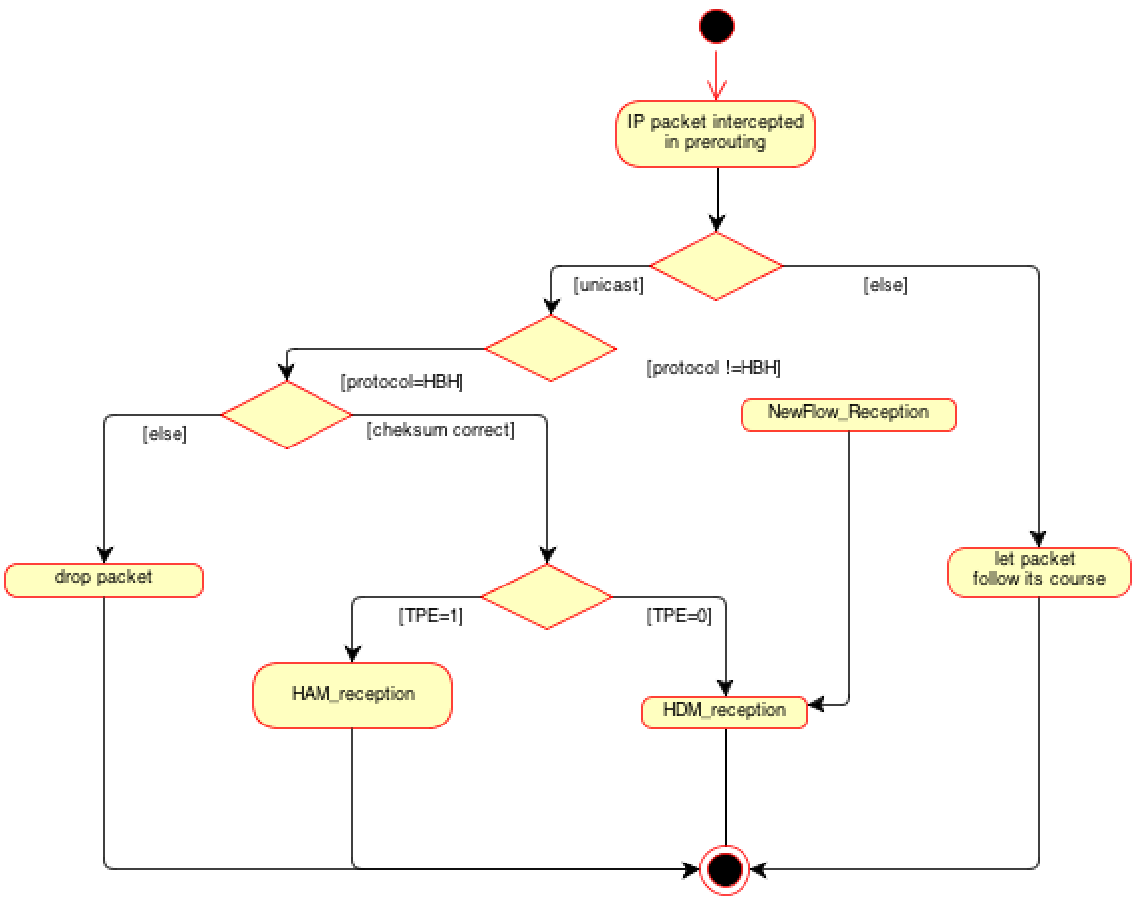


Figure 28: IP interception and flow management.

HDM reception and HAM reception are described by UML activity diagrams, and are shown in the figures below.

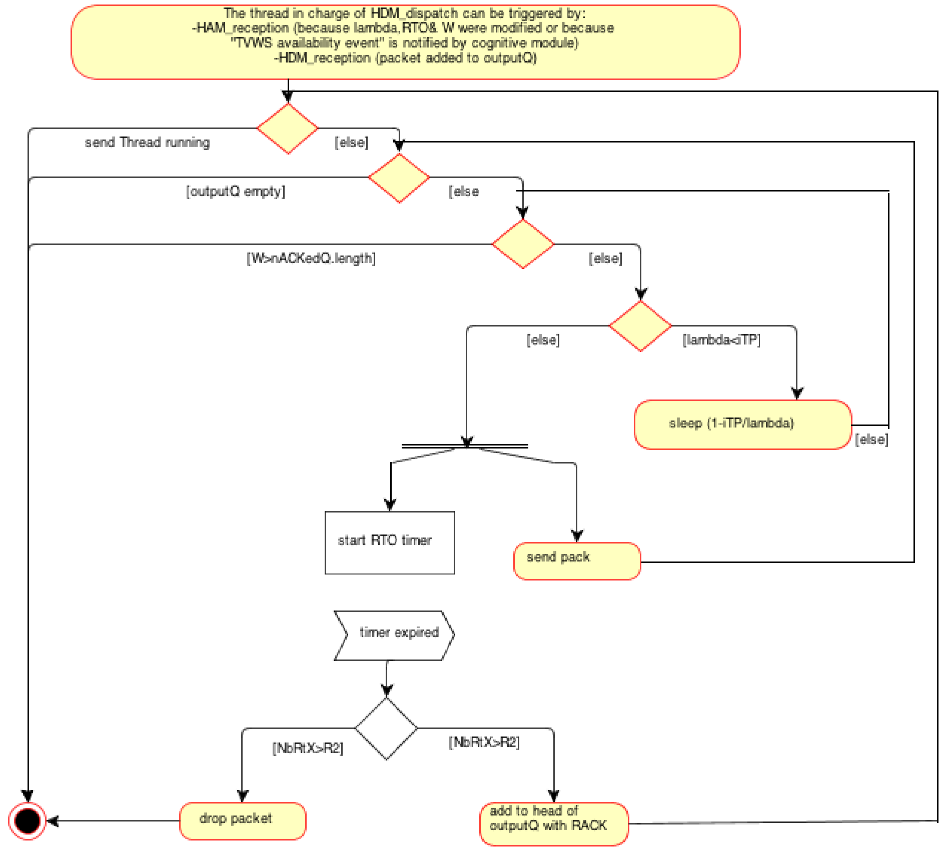


Figure 29: HDM Dispatch.

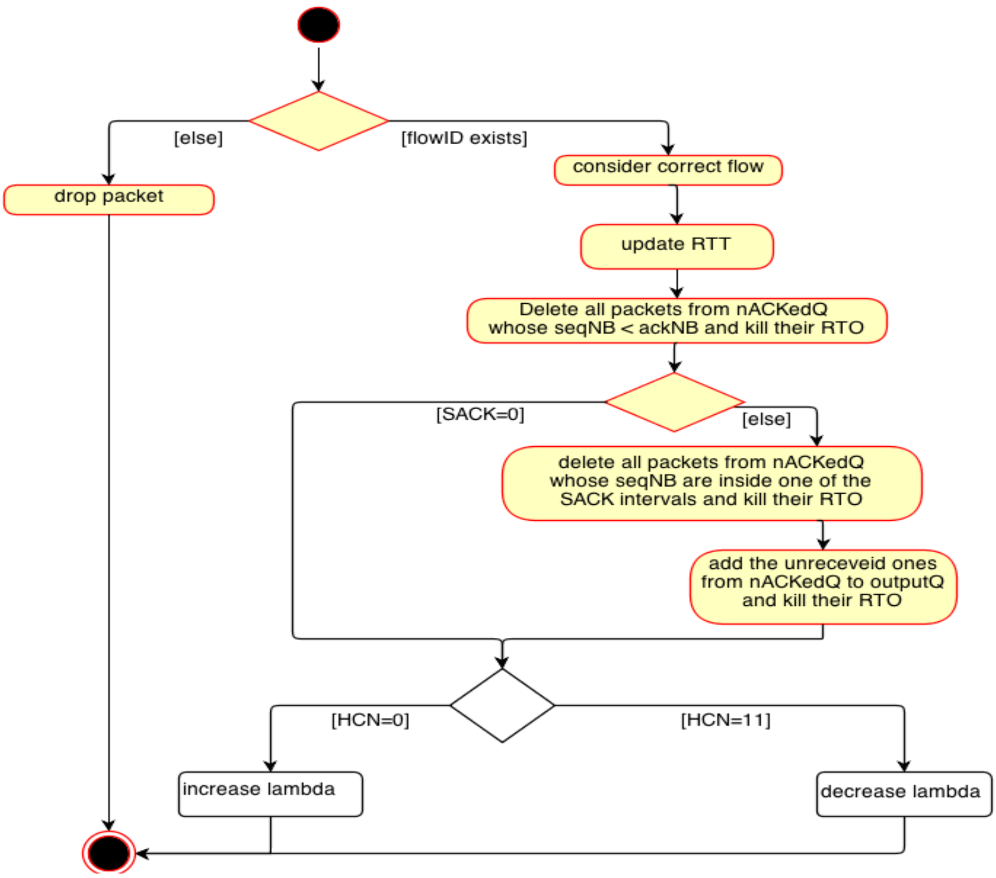


Figure 30: HAM reception.

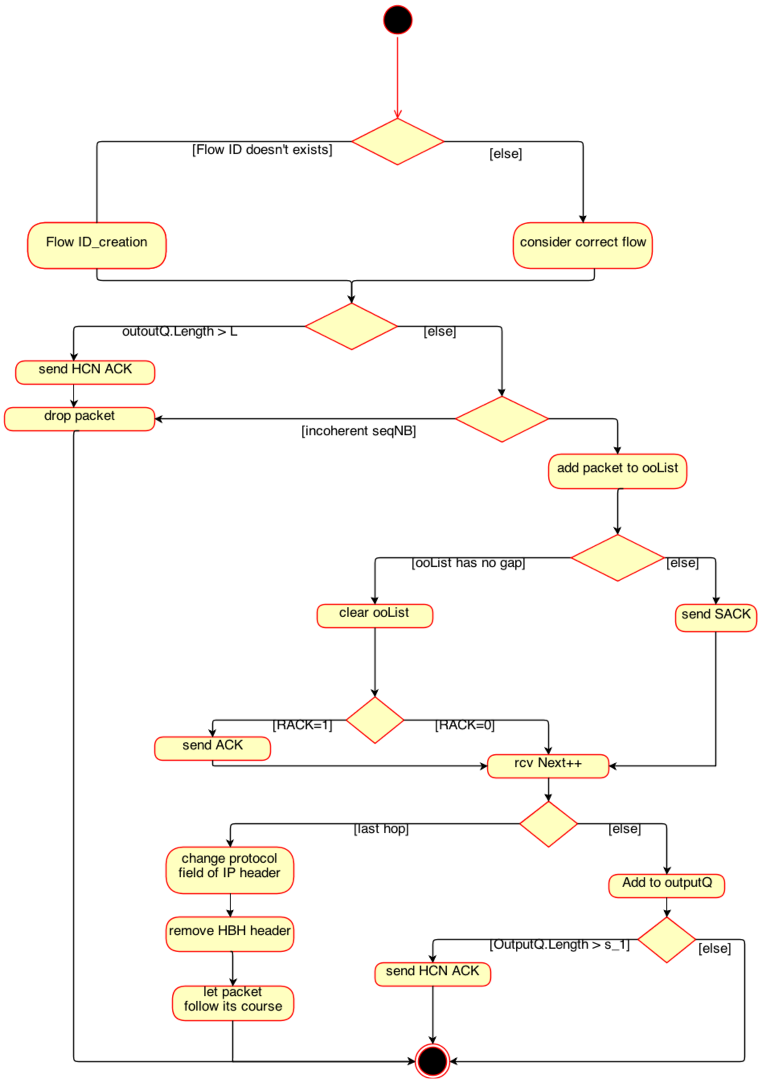


Figure 31: HDM reception.

4.5.3- *Simulation evaluation of the HBH transport layer results*

The HBH protocol implementation was done in C++, and tested using the network simulator ns-3 avaialble at www.nsnam.org . Ns-3 is a discrete event network simulator widely used in research, academia and industry, which aims to replace the much more complex ns-2. Its architecture has the advantage of being modular. The use of such a simulator can easily change the number of nodes, their geographical distribution (topology, grid, star, tree, ...) and their evolution over time (e.g., random movements in an area data). Protocol stack can be chosen by the developer, and the most popular protocols are already implemented (including legacy lower layers). The characteristics of the link (delay, throughput, loss rate, ...) can also be easily modified to test HBH protocol in various types of networks constrained.

HBH is a transport protocol implemented between OSI layer 3 and layer 4. Insofar as the specifications have been described in detail in previous sections, with UML activity diagrams, it is not necessary to go into more detail on the implementation section. It was also required to develop a netfilter module to intercept IP packets, because this feature is absent in ns-3.

Once the HBH protocol implemented, simulations were run by varying relevant parameters. A script that runs several simulations, extract from simulation logs the appropriate information, performs processing on this information and finally displays the results in graphic form were used in orde to run experiments

in our controlled environment easier and reproduceable. Among the modifiable parameters in the simulation, the most used were: the distance between nodes, number of nodes, the number of Secondary Users competing for access using the same channel, the number of TCP flows, the choice to enable or disable our solution to easily compare the improvement compared to standard TCP, the number of simulations required to obtain averages and reliable results, the number of bytes to send, the link capacity (We made the assumption that the number of available TVWS channel is directly related to the link capacity multiple radio interface system: the more channels are available between two nodes, the more capacity this link has) the channel delay, error rate (packet) of the channel, the transport protocol to use on top of HBH (TCP or UDP), the HBH window size W, or the maximum allowed number of retransmissions R_2.
Several theoretical performances studies were made (delay, throughput, loss rate, overhead, ...) that could get HBH, under certain simplifying assumptions and in line with the COGEU use-cases. For example, Figure 32 is the calculation of the overhead induced by the retransmissions, depending on the loss rate on a 3 hops network (chain topology) and depending on the maximum allowed number of retransmissions (1-5, named R1 to R5).

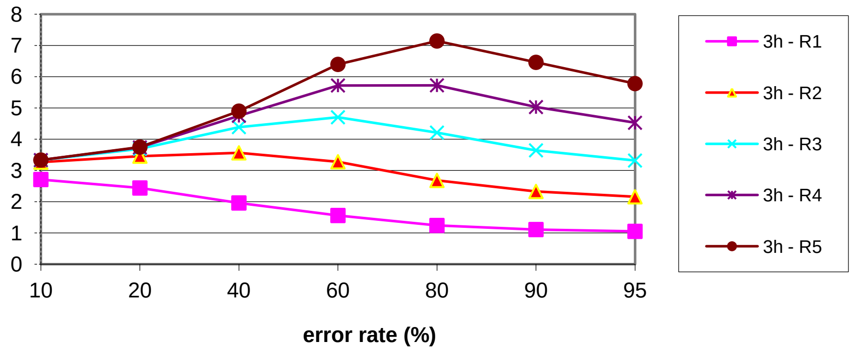


Figure 32: HBH overhead introduce by varying R2 (max. retransmission number).

We can conclude from this result that the overhead introduced by HBH (Y-axis in Figure 32) increase significantly depending on both R (maximum number of allowed retransmission) and error rate. R should not be static but should be pro-actively adjusted to the expected error rate if we want to reduce the expected overhead.

For the following part of this study we will focus on a linear topology with 5 nodes (as illustrated in Figure 33). We consider unnecessary to develop more complex topologies for transport layers studies because complexity comes from the various parameters used and not the topology itself. TCP performances are well known to decrease with an increasing number of hop in a multi-hop wireless mesh network.

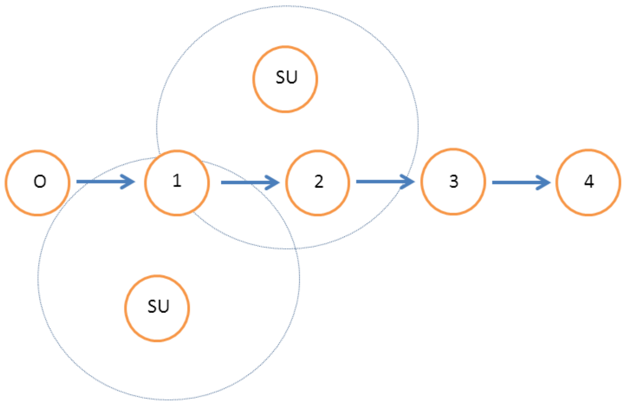
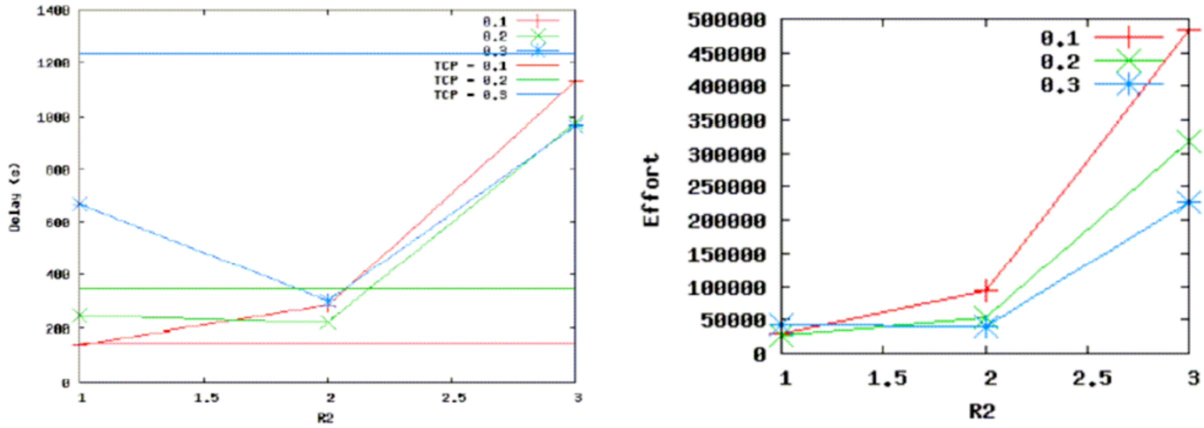


Figure 33: Five nodes chain topology.

We evaluate the performance of TCP Reno compared to the spectrum aware HBH protocol. We send a single TCP over the chain topology (Figure 33) from node 0 to node 4 representing our Cognitive Radio Ad-Hoc Network. Starting from this simple scenario, we vary the number of Secondary Users present and using one of the 11 channels available for unlicensed use. External Interferences are introduced by entering in competition for the available channels with other Secondary Users transmitting close to chain topology considered. Those external Secondary Users are using the unlicensed TVWS available at a given location making access to the communication channel more difficult for our considered CRAHN due to contention. The more TVWS devices are present in the coverage area, the bigger error rate is. We introduced up to 11 external secondary users close to the chain topology in order to obtain an error rate varying from 10% to 30%.



Delay Vs Reliability (R_2) Effort Vs Reliability (R_2)

Figure 34: Delay / Overhead Effort Vs Reliability

In terms of overall HBH performance, we have a low overhead in ideal situation (with low losses), which is expected and means that even in the HBH worst case (reliability mechanisms are useless), the overhead is still acceptable.

We also noticed from Figure 34 that the maximum number of retransmissions R_2 has a strong impact on the performance of HBH. When static R_2 is used (no contact with the COGEU TVWS repository), we obtain a curve in V-shape for the number of retransmissions function of delay. R_2 should not be too low, otherwise there will be end to end retransmissions and our hop-by-hop local retransmission would in fact worsen the overall performance. In the other hand, R_2 should not be too high either, because we could be in a situation where TCP RTO expires and where local retransmission occurs while a packet is already being retransmitted from the original source of the flow. In this sense, the parameter ρ, which affects R_2 should definitely be related to a Spectrum occupancy metric (and thus related to the local error rate encountered on each link) and locally computed per each node on a case per case basis. When R_2 (maximum allowed number of retransmission) is static, HBH cannot adapt to the varying error rate encountered among the path in CRAHN.

By making each node able to locally compute parameter ρ, (which affects R_2) based on information related to the number of external Secondary Users in the coverage area, HBH outperform legacy TCP as illustrated in Figure 35. In this figure, one can observe TCP collapses when the error rate is too high, while HBH is much more resistant to errors and decreases almost linearly with error rate thanks to the flexibility of R_2 value introduced.

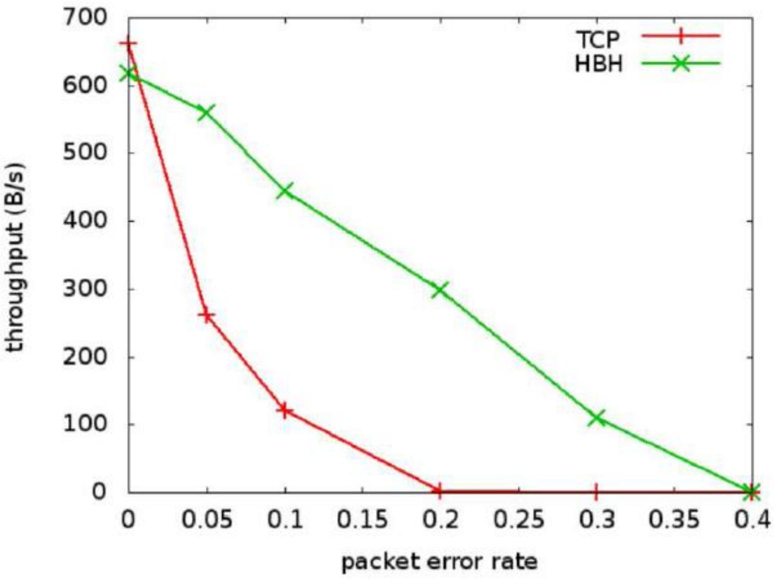


Figure 35: TCP & HBH comparison for a dynamic R2 value (1 ≤ R2 ≤ 4).

4.6- Summary

Direct Mode terminal communications forming Cognitive Radio Ad Hoc Networks over TVWS constitute a viable solution if issues faced by TCP in this environment can be resolved. Investigations presented in this document adopt a pragmatic approach by proposing an information transport protocol while avoiding modifying the original TCP stack. Indeed, many attempts to modify/adapt TCP over wireless have failed to be deployed in the past because modifications to TCP involve modification of the majority of applications currently used over IP and also involve a rapid and wide adoption of the new stack version for compatibility reason. In the specific use-case investigated in COGEU where Public Safety Network are usually well controlled and user terminals strictly operated, the HBH proposal could be categorized in Distributed Performances Enhancement Proxies (PEPs) type of OSI layer 4 optimization. A better use of CRAHN in TV White-Space environment has been demonstrated in terms of bandwidth, latency and network resources without disrupting the operational applications used by first responders. Exploiting the services provided by the COGEU reference model like request of TVWS devices currently in operation at a given location, has been proven efficient in this attempt to design a spectrum aware transport protocol.

5- Conclusions

This deliverable reports research work performed in Tasks 6.2, 6.3 and 6.4 of WP6. It elaborates on the design, implementation and evaluation of networking protocols (i.e. signaling, routing and transport layer), regarding the efficient communication between players in COGEU use-cases.

More specifically, chapter 2 presents the design and implementation of an application protocol “PAWS” for geo-location database services that allows any white space device or the spectrum broker to grand access to the services of the geo-location database by communicating over commonly used Internet. For COGEU purposes PAWS implementation adapted to specific rules defined by the FCC and the description of these requirements are also presented in this document.

Chapter 3 investigates multi-hop routing schemes and proposes novel routing approaches, in order to provide efficient data delivery across regions with heterogeneous spectrum availability. The proposed protocols exploit an assigning mechanism, in order to perform network connectivity, even if the end-to-end path is temporarily unavailable. In this context, a Public Safety use-case is studied based on a mesh, ad-hoc network architecture, where secondary nodes communicate, exploiting the proposed routing protocols, enhanced with the assigning mechanism. The routing protocols were designed, implemented and evaluated, in order to validate their efficient exploitation in COGEU use cases, taking into account real data regarding TVWS availability in Munich area. A routing simulator was developed in terms of COGEU Public Safety Ad-hoc scenario, where the AODV protocol was modified and adapted in order to overcome the challenges that occurred by TVWS (i.e. the absence of a CCC between the secondary users). Results verified the validity of the proposed routing protocols, besides identifying fields for further research, in order to enhance this research approach with additional mechanisms, towards optimizing performance of the provided simulation results.

Chapter 4 reports a modification of transport protocols adopting a Distributed Performance Enhancing Proxy scheme called Hop-by-Hop protocol. It is designed in order to operate in a cognitive radio environment, where frequent disruption is a norm and end-to-end paths are hardly available such as in some COGEU secondary usage scenarios (DMO based Public Safety Network operating in TVWS), has been investigated. In cognitive radio networks, many factors such as unpredictable external interference, heterogeneous channel bandwidth availability, or channel mobility/switching can affect the packet loss rate. Similarly, RTT can be affected by the delay due to spectrum sensing and spectrum handoff, for which when the current channel becomes unusable for an unlicensed user, the unlicensed user has to search for a new channel. Therefore, the modified transport layer protocols consider these effects to optimize end-to-end congestion control and to tune reliability accordingly. The result of this work was subject to a patent submission. The work performed by Thales under the frame of COGEU resulted in a patent application related to OSI Layer 4 Transport Protocols. Thales Communications & Security patented a process for optimized end-to-end transport in Wireless multi-hop networks with a focus on cognitive radio characteristics possibly available on those networks.

References

[1] http://www.ietf.org

[2] http://www.internetsociety.org

[3] http://datatracker.ietf.org/wg/paws/

[4] https://mentor.ieee.org/

[5] http://spectrumbridge.com

[6] http://datatracker.ietf.org/doc/draft-sbi-paws-protocol/

[7] http://www.fcc.gov/document/part-15-tv-bands-devices

[8] http://datatracker.ietf.org/doc/draft-ietf-paws-problem-stmt-usecases-rqmts/

[9] http://www.wikipedia.org/wiki/XML

[10] E. Hossain, D. Niyato, Z. Han, “Dynamic spectrum access and management in cognitive radio networks”, first ed. Cambridge University Press, 2009.

[11] Hafid, A., Gendreau, M., “Wireless Mesh Networks Design — A Survey” Communications Surveys & Tutorials, IEEE, 2012

[12] Perkins CE, Royer EM, “Ad hoc on-demand distance vector routing”. In: Proc. of IEEE workshop on mobile computing systems and applications, New Orleans, LA.

[13] COGEU geo-location database http://projectos.est.ipcb.pt/cogeu2/cogeu_novo.php

[14] The European 7th Framework Programme project: COGEU (ICT-248560) - Deliverable 6.2 - Spectrum-aware routing, transport protocols and negotiation protocols between players for secondary spectrum trading - Initial specification, December 2011

[15] H. Ma, L. Zheng, X. Ma, Y. luo, Spectrum aware routing for multi-hop cognitive radio networks with a single transceiver, in: 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008, 2008, pp. 1–6, doi: 10.1109/CROWNCOM.2008.4562509.

[16] G. Cheng, W. Liu, Y. Li, W. Cheng, Spectrum aware on-demand routing in cognitive radio networks, in: 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2007, 2007, pp. 571–574, doi: 10.1109/ DYSPAN.2007.80.

[17] G. Cheng, W. Liu, Y. Li, W. Cheng, Joint on-demand routing and spectrum assignment in cognitive radio networks, in: IEEE International Conference on Communications, ICC ’07, 2007, pp. 6499–6503, doi: 10.1109/ICC.2007.1075.

[18] Z. Yang, G. Cheng, W. Liu, W. Yuan, W. Cheng, Local coordination based routing and spectrum assignment in multi-hop cognitive radio networks, Mobile Networks and Applications 13 (1-2) (2008) 67–81. doi: 10.1007/s11036-008-0025-9.

[19] J. Van den Berg, F. Roijers, M. Mandjes (2006) Performance modeling of a bottleneck node in an IEEE 802.11 Ad-hoc network. In: The 5th International Conference on Ad hoc Networks and Wireless, Ottawa, August 2006

[20] V. B. Iversen, Teletraffic Engineering Handbook, http://www.tele.dtu.dk/teletraffic/handbook/telehook.pdf

[21] J. Roberts, Traffic Theory and the Internet, IEEE Communications Magazine, Jan. 2001, pp. 94-99 http://perso.rd.francetelecom.fr/roberts/Pub/Rob01.pdf

[22] http://www.3gpp.org/

[23] http://www.npstc.org/

[24] K. Fall, "A delay-tolerant network architecture for challenged internets," In Proc. SIGCOMM, 2003.

[25] G. Holland and N. Vaidya, "Analysis of TCP performance over mobile ad hoc networks," In Proc. ACM Mobicom'99, Seattle, WA, 1999.

[26] S. Kopparty, S.V. Krishnamurthy and M. Faloutsos, "Split TCP for mobile ad hoc networks," Tripathi, S.K., GlobeCom 2002.

[27] Ming Li, Devesh Agrawal, Deepak Ganesan, and Arun Venkataramani, "Block-switched Networks : A New Paradigm for Wireless Transport," In Proceedings of the 6th ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI 2009), Boston, Apr 2009.

[28] Yao-Nan Lien and Yi-Fan Yu, "Hop-by-Hop TCP over MANET," IEEE APSCC 2008.

[29] J. Liu and S. Singh, "ATCP: TCP for Mobile Ad Hoc Networks," IEEE Journal on Selected Areas in Communications. 1999.

[30] RFC 3135, "Performance Enhancing Proxies (PEP) Intended to Mitigate Link-Related Degradations".

[31] RFC 3449, "TCP Performance Implications of Network Path Asymmetry".

[32] K. Brown, S. Singh, "M-TCP : TCP for Mobile Cellular Networks," ACM Computer Communications Review Volume 27(5), 1997.

[33] A. M. Slingerland, P. Pawe lczak, R. V. Prasad, A. Lo, and R. Hekmat. Performance of Transport Control Protocol over Dynamic Spectrum Access Links. In Proc. of IEEE Dyspan, 2007.

[34] M. D. Felice, K. R. Chowdhury, and L. Bononi. Modeling and Performance Evaluation of Transmission Control Protocol over Cognitive Radio Ad Hoc Networks. In Proc. of ACM MSWiM, 2009.

[35] K. R. Chowdhury, M. D. Felice, and I. F. Akyildiz. TP-CRAHN: a Transport Protocol for Cognitive Radio Ad-Hoc Networks. In Proc. of IEEE INFOCOM, 2009.

[36] D. Sarkar and H. Narayan. Transport Layer Protocols for Cognitive Networks. In Proc. of IEEE INFOCOM CWCN, 2010.

List of Figures

Figure 1: Generic networking issues in the TVWS and COGEU options... **Error! Bookmark not defined.**
Figure 2: Logical arrangement of this deliverable. .... **Error! Bookmark not defined.**
Figure 3: COGEU reference architecture for commons and secondary trading, using a web-based geo-location database access. 6
Figure 4: Implemented solution based on IETF PAWS. 7
Figure 5: Relational Database Diagram for PAWS 9
Figure 6: List of enrolled master WSD in the database. 10
Figure 7: Message exchange, upon registration request from the WSD to the geo-location database. . 11
Figure 8: Recorded data from the WSD in the geo-location database 11
Figure 9: Message exchange for a channel list request from the WSD to the geo-location database. All possible answers are represented, but only one is sent at each request. 12
Figure 10: Slave ID request message exchange. 13
Figure 11: Graphical web interface to demonstrate COGEU PAWS between a geo-location database and a WSD (fixed or Mode 1 Portable) 14
Figure 12: Communication across Public Safety workers operating over heterogeneous TVWS 19
Figure 13: Mesh network architecture for Public Safety use-cases 20
Figure 14: Message exchange process of COGEU routing protocol 22
Figure 15: Message exchange process, including redirection 22
Figure 16: Optimised message exchange process 23
Figure 17: Munich urban-area with public safety network nodes operating over TVWS 24
Figure 18: Mesh network topology (simulation scenario) 25
Figure 19: Mean End-to-End Delay for different number of simultaneous flows 26
Figure 20: End-to-End Delay for the 1st flow versus probability of PU presence 26
Figure 21: Average End-to-End Delay for all flows versus probability of PU presence 27
Figure 22: Average End-to-End Delay versus node distance 28
Figure 23:Number of Hops per each flow 28
Figure 24: illustration of TVWS CRAHN unpredictability of available radio resources 30
Figure 25:PEP setup illustration 31
Figure 26 : HBH message flow 34
Figure 27:Reliability mechanisms examples 35
Figure 28: Hop by Hop protocol header 36
Figure 29: HBH node implementation 38
Figure 30: IP interception and flow management 39
Figure 31: HDM Dispatch 40
Figure 32: HAM reception 40
Figure 33: HDM reception 41
Figure 34: HBH overhead introduce by varying R2 (max. retransmission number) 42
Figure 35: 5 nodes chain topology 42
Figure 36: Delay / Overhead Effort Vs Reliability 43
Figure 37: TCP & HBH comparison for a dynamic R2 value (1 ≤ R2 ≤ 4) 44

List of Abbreviations

AODV	Ad hoc On-Demand Distance Vector Routing
CCC	Common Control Channel
CLRP	Channel List Refresh Period
CR	Cognitive Radio
CRAHN	Cognitive Radio Ad-Hoc Networks
CRNs	Cognitive Radio Networks
CRT	Channel list Request Timer
EIRP	Equivalent isotropically radiated power
HTML	HyperText Markup Language
HBH	Hop by Hop
HDM	HBH Data Message
HAM	HBH Acknowledgment Message
I-TCP	indirect-TCP
IEEE	The Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISOC	Internet Society
JS	JavaScript
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Medium Access Control
MANETs	Mobile Ad-Hoc Networks
PAWS	Protocols to access white space
PHP	Hypertext Preprocessor
QoS	Quality of Service
RREP	Route request
RREQ	Route replay
RTT	Round-trip-time
RVP	Registration Valid Period
TCP	Transmission Control Protocol
TTL	Time to Live
TV	Television
TVWS	TV White Spaces
UDP	User Datagram Protocol
UHF	Ultra High Frequency
VRT	ID Verification Request Timer
WiFi	IEEE 802.11
WLAN	Wireless Local Area Network
WP	Work Package

WSD	White Space Device
XML	Extensible Markup Language