ETSI TR 102 684 V1.1.1 (2012-04)

Reconfigurable Radio Systems (RRS); Feasibility Study on Control Channels for Cognitive Radio Systems

Reference
DTR/RRS-03008

Keywords
control, radio

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Introduction

For the efficient operation of Cognitive Radio Systems, mechanisms with that will allow for the exchange and distribution of information as well the coordination between various management entities are essential. In this respect, Control Channels have been identified as a key feature required for Cognitive Radio Systems, as means for transmitting elements of information necessary to manage and realize various operations within a Cognitive Radio Systems. In this scope, the present document aims to identify and study communication mechanisms:

1) for the coexistence and coordination of different cognitive radio networks and nodes, operating in unlicensed bands like the ISM band or as secondary users in TV White Spaces;

2) for the management of Operator-governed Opportunistic Networks, operating in the same bands as mentioned above. In particular, it is expected that these networks will include mechanisms for operator-governed ad-hoc coverage extensions or capacity extensions of infrastructure networks. The communication is expected to include procedures from terminal to terminal as well as between a terminal and infrastructure networks.

These mechanisms could be radio access technology (RAT) specific or/and be RAT-independent.

Further on, the present document presents and analyses implementation options for Control Channels for Cognitive Radio Systems, taking into account previous work on in-band-Cognitive Pilot Channel (CPC) and Cognitive Control Channel (CCC). The investigation of implementation options is a crucial step towards the realisation of the Control Channels and the deployment of Cognitive Radio Systems.

1 Scope

The present document aims to identify and study potential communication mechanisms on Control Channels for Cognitive Radio Systems:

1) for the coexistence and coordination among different cognitive radio networks and nodes, operating in unlicensed bands like the ISM band or as secondary users in TV White Spaces;

2) for the management of operator-governed Opportunistic Networks, operating in the same bands as mentioned above.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ITU-R Report M.225: "Introduction to cognitive radio systems in the land mobile service", 2011.

[i.2] ITU-R Report SM.2152: "Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)", September, 2009.

[i.3] ETSI TR 102 683: "Reconfigurable Radio Systems (RRS); Cognitive Pilot Channel (CPC)".

[i.4] ETSI TS 122 234 (V7.5.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (3GPP TS 22.234 version 7.5.0 Release 7)".

[i.5] ETSI TS 136 300: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300)".

[i.6] ETSI TS 124 302: "Universal Mobile Telecommunications System (UMTS); LTE; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (3GPP TS 24.302)".

[i.7] ETSI TR 102 907: "Reconfigurable Radio Systems (RRS); Use Cases for Operation in White Space Frequency Bands".

[i.8] IETF Working Group on Protocol to Access WS database (paws).

NOTE: Available at http://datatracker.ietf.org/wg/paws/charter/.

[i.9] IEEE 802.19-10/0055r3 Baykas, Kasslin, Shellhammer: "IEEE P802.19 System Design Document", March 2010.

[i.10] IEEE Standard 1900.4 for Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks, February 27, 2009.

[i.11] S.Buljore, H.Harada, P.Houze, K.Tsagkaris, O.Holland, S.Filin, T.Farnham, K.Nolte, V.Ivanov: "Architecture and enablers for optimized radio resource usage in heterogeneous wireless access networks: The IEEE 1900.4 Working Group" Communications Magazine, IEEE, Vol 47, no. 1, pp. 122-129, January 2009.

[i.12] P. Houze, S. Bonjour, L. Suciu, V. Gupta: "IEEE P1900.4 vs. IEEE 802.21", presentation, January 2009.

[i.13] ETSI TS 124 312: "Universal Mobile Telecommunications System (UMTS); LTE; Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (3GPP TS 24.312 Release 8)".

[i.14] OMA-ERELD-DM-V1-2: "Enabler Release Definition for OMA Device Management".

[i.15] ETSI TS 122 278 "Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for the Evolved Packet System (EPS) (3GPP TS 22.278 Release 8)".

[i.16] ETSI TS 123 402: "Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (3GPP TS 23.402 Release 8)".

[i.17] Foundation for Intelligent Physical Agents (FIPA).

NOTE: Web site, http://www.fipa.org, accessed March 2011.

[i.18] Java® Agent DEvelopment Platform (JADE).

NOTE: Web site, http://jade.tilab.com, accessed March 2011.

[i.19] JADEX Projects.

NOTE: http://vsis-www.informatik.uni-hamburg.de/projects/jadex/, accessed March 2011.

[i.20] ORBacus, IONA Technologies.

NOTE: http://www.orbacus.com/, accessed March 2011.

[i.21] A. Galani, K. Tsagkaris, N. Koutsouris, P. Demestichas: "Design and assessment of functional architecture for optimized spectrum and radio resource management in heterogeneous wireless networks", International Journal of Network Management, John Wiley & Sons, Vol. 20, Issue 4, pp. 219-241, July/August 2010.

[i.22] V. Stavroulaki, N. Koutsouris, K. Tsagkaris, P. Demestichas: "A Platform for the Integration and Management of Cognitive Systems in Future Networks", accepted in IEEE International Workshop on Management of Emerging Networks and Services (IEEE MENS 2010), in conjunction with IEEE Globecom 2010.

[i.23] ETSI TS 129 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (3GPP TS 29.229)".

[i.24] IETF RFC 3588: "Diameter Base Protocol", September 2003.

[i.25] IEEE 802.11-2007: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.26] IEEE 802.11u: Part 11 Amendment 9: "Interworking with external networks", February 2011.

[i.27] Bluetooth® SIG: "Bluetooth® 4.0 Specification".

[i.28] WiMedia Alliance: "Distributed Medium Access Control (MAC) for wireless networks", MAC Specification: Release 1.5, December 1, 2009.

[i.29] IEEE 802.21TM-2008: "IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", IEEE Computer Society, Sponsored by the LAN/MAN Standards Committee, January 2009.

[i.30] W3C Recommendation 10 February 2004: "Resource Description Framework (RDF): Concepts and Abstract Syntax".

NOTE: Available online at http://www.w3.org/TR/rdf-concepts.

[i.31] IETF RFC 3416: "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", December 2002.

[i.32] TR-069 Amendment 2: "CPE WAN Management Protocol v1.1", Broadband Forum, December 2007.

[i.33] ETSI TS 132 101: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Principles and high level requirements (3GPP TS 32.101)".

[i.34] ETSI TS 125 331: "Universal Mobile Telecommunications System (UMTS); Radio Resource Control (RRC); Protocol specification (3GPP TS 25.331)".

[i.35] ETSI TS 136 331: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (3GPP TS 36.331)".

[i.36] IETF RFC 4282: "The Network Access Identifier".

[i.37] ECMA-368: "High Rate Ultra Wideband PHY and MAC Standard".

[i.38] Bluetooth® 2.1.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Cognitive Control Network (CCN): network of nodes in different cognitive radio networks communicating with each other for controlling the frequency agile behaviour among the set of cognitive radio networks

Cognitive Control Channel (CCC): distributed approach for real time communication between different CRS nodes in a specific geographical area

NOTE 1: CCC may enable different CRS nodes to exchange information related to coexistence, generic spectrum usage rules or policies and/or specific capabilities and needs of different nodes.

NOTE 2: The information communicated on CCC may include, among other things, spectrum etiquette, rules for accessing specific bands, local availability of different bands, sensing information, available applications, or spectrum needs of different systems [i.1].

Cognitive Pilot Channel (CPC): channel (logical or physical) that is used to regularly push information out to the CRS node

NOTE 1: It can include the use of specifically transmitted messages, and having known transmission characteristics.

NOTE 2: The CPC can be used, among other things, to help a mobile terminal in identifying operators, policies and access technologies and their associated assigned frequencies in a given region. In some cases, when an uncoordinated deployed CRS base station (or Reconfigurable Base Stations) is booting up, CPC information may also be utilized to identify available spectrum in its current location [i.1].

Cognitive Radio System (CRS): radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained [i.2]

Control Channels for Cognitive Radio Systems (CC-CRS): Control Channels for Cognitive Radio Systems are used for sharing cognitive control information between or within Cognitive Radio Systems

NOTE: They may be logical channels transporting information on top of a physical channel. Such channels are responsible for conveying information between entities involved in Cognitive Radio Systems, such as devices, network elements, network/device management entities.

Opportunistic Network (ON): network which exploits opportunities with respect to the spectrum and the devices in the area

operator-governed Opportunistic Network (ON): operator-governed (through the provision of spectrum, policies, information and knowledge, exploited for its creation), temporary, localised network segment

NOTE: It involves devices organized in an ad-hoc manner, and is terminated at access points (macro base stations, femto base stations) of the infrastructure. An opportunistic network is set up as a temporary, coordinated extension of the infrastructure with the aim to improve the coverage and capacity of the infrastructure network.

White Space (WS): part of the spectrum, which is available for a radio communication application (service, system) at a given time in a given geographical area on a non-interfering / non-protected basis with regard to primary services and other services with a higher priority on a national basis

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ACL	Agent Communication Language
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
ASCF	Application Specific Command Frames
ASIE	Application Specific Information Element
ASN.1	Abstract Syntax Notation One
ASN.1	Abstract Syntax Notation One
ATT	Attribute Protocol
BCH	Broadcast CHannel
BS	Base Station
BS	Broadcasting Service
CCC	Cognitive Control Channel
CC-CRS	Control Channel(s) for Cognitive Radio Systems
CCN	Cognitive Control Network
CCP	Central Control Point
CDIS	Coexistence Discovery and Information Server
CE	Coexistence Enabler
CM	Coexistence Manager
CN	Cognitive Network

CORBA	Common Object Request Broker Architecture
CPC	Cognitive Pilot Channel
CR	Cognitive Radio
CRS	Cognitive Radio System
DDF	Device Description Framework
DM	Device Management
DME	Device Management Entity
DNS	Domain Name System
EGAN	Enhanced Generic Access Network
EIR	Extended Inquiry Response
EPC	Evolved Packet Core
FIPA	Foundation for Intelligent Physical Agents
GAS	Generic Advertisement Service
GSM	General System for Mobile Communications
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers or IEEE
IEs	Information Elements
IETF	Internet Engineering Task Force
IIOP	Internet Inter-object request broker Protocol
IMTP	Internal Message Transport Protocol
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
IWLAN	Interworking Wireless LAN
JDK	Java Development Kit
JRRM	Joint Radio Resource Management
Leap	Lightweight Extensible Agent Platform
LTE	Long Term Evolution
MAC	Medium Access Control
MAS	Medium Access Slot
ME	Micro Edition
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media-Independent Handover
MIHF	MIH Function
MIIS	Media Independent Information Service
ML	Markup Language
MLME	MAC Sublayer Management Entity
MMPDU	MAC Management Protocol Data Unit
MN	Mobile Node
MO	Management Object
MTP	Message Transport Protocol
N2N	Network To Network
NAI	Network Access Identifier
NMS	Network Management System
OMA	Open Mobile Alliance
OMG	Object Management Group
ON	Opportunistic Network
ORB	Object Request Broker
PAWS	Protocol to Access White Space Databases
PM	Performance Monitoring
PS	Packet Switched
PVSA	Public Vendor Specific Action
QoS	Quality of Service
RAN	Radio Access Network
RANOp	Radio Access Network Operator
RAT	Radio Access Technology
RDF	Resource Description Framework
RF	Radio Frequency
RFC	Request For Comments
RMI	Remote Method Invocation

RRC	Radio Resource Control
RRM	Radio Resource Management
RRS	Reconfigurable Radio System
SAP	Service Access Point
SDAP	Service Discovery Application Profile
SDP	Service Discovery Protocol
SDR	Software Defined Radio
SI	System Information
SME	Station Management Entity
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SP	Service Provider
T2N	Terminal to Network
T2T	Terminal To Terminal
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
TS	Technical Specification
TV	Television
TVWS	TV White Space
TVWSD	TV White Space Device
UDP	User Datagram Protocol
UE	User Equipment
UHF	Ultra High Frequency
UL	Up-Link
UL/DL	Up-Link/Down-Link
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
UWB	Ultra Wide Band
VSA	Vendor Specific Action
VSIE	Vendor Specific information element
WAP	Wireless Application Protocol
WFA	Wi-Fi Alliance
WI-FI	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WS	White Space

4 Motivation

The present document aims to identify and study communication mechanisms:

1) for the coexistence and coordination of different cognitive radio networks and nodes, operating in unlicensed bands like the ISM band or as secondary users in TV White Spaces;

2) for the management of Operator-governed Opportunistic Networks, operating in the same bands as mentioned above. In particular, it is expected that these networks will include mechanisms for operator-governed ad-hoc coverage extensions or capacity extensions of infrastructure networks. The communication is expected to include procedures from terminal to terminal as well as between a terminal and infrastructure networks.

These mechanisms could be radio access technology (RAT) specific or/and be RAT-independent. In particular, the present document addresses the following issues:

- Discovery and identification of neighbouring devices and networks.
- Advanced Multi-RAT Assistance in Heterogeneous Networks.
- Retrieval of information on available White Spaces from a geo-location database.

- Management of operator-governed opportunistic networks in terms of creation, maintenance and termination.
- Implementation options for Control Channels for Cognitive Radio Systems, taking into account previous work on in-band-Cognitive Pilot Channel (CPC) and Cognitive Control Channel (CCC).

5 Coexistence and coordination of different cognitive radio networks and nodes

5.1 Discovery and identification of neighbouring devices and services

Control Channels for Cognitive Radio Systems (CC-CRS) can be used to provide information on available networks and/or devices and/or services in the geographical neighbourhood.

When a UE is powered on in today's cellular networks, the UE usually queries its USIM for information on stored frequencies in an attempt to perform a Stored Information Cell Selection. This allows the UE to search for these particular cells without having to scan the entire band or bands that the UE is configured to operate on. During this process, the UE will traverse the list of stored cell frequencies in the USIM until it finds a suitable one.

If the UE is powered on in a completely new environment e.g. because the user has travelled into a foreign country, then none of these cells stored in the USIM will be found. Then, the UE should perform an Initial Cell Selection which requires no a priori knowledge of cell information and requires scanning of all frequencies to find a cell where the energy level is sufficiently high to attempt synchronization. This process of an Initial Cell Selection takes a couple of minutes before the UE successfully camps on a cell. Additionally, a UE should register on the network before knowing the available services, and may waste time gaining access to a network that cannot satisfy the user's requirements.

In ad hoc networks the discovery and connection set-up are based on transmitting and scanning discovery signals: a node in discoverable more transmits a discovery signal regularly (e.g. a beacon), and a node which wishes to detect and connect to an ad-hoc network starts scanning for the discovery signals. Alternatively, in some ad-hoc network technologies, a node in discoverable mode scans discovery signals regularly, and a node which wishes to detect and connect to an ad-hoc network starts transmitting discovery signals. The discovery time depends on the amount of the used discovery channels, and also on the beacon or scan interval of the discoverable node.

Different options exist on how control channels for cognitive radio systems can be used to improve the time to discover a first network or to improve the discovery of other networks which may e.g. provide other services.

5.1.1 Cognitive Pilot Channel

The Cognitive Pilot Channel (CPC) [i.3] is defined as a channel which conveys the elements of necessary information facilitating the operations of Cognitive Radio Systems. The CPC provides information from the network to the user devices e.g. on available radio access networks, their frequency bands, radio access technologies and spectrum usage possibilities. Two deployment options, the in-band CPC and the out-band CPC can be considered.

The in-band CPC is a logical channel within one or some of the technologies available in a heterogeneous radio environment. The purpose of the CPC is to distribute information about the radio environment at a certain location. Figure 1 shows the principle of the in-band CPC, with reference to the deployed RATs: The in-band CPC can be implemented in one or more of the available RATs. The in-band CPC may support downlink as well as uplink information transfer or alternatively only downlink information transfer. The CPC Manager may obtain the information to be distributed over the CPC from the Joint Radio Resource Management (JRRM) or other functions on network side, e.g. from the network management. The CPC Manager configures which information is to be distributed over the CPC.

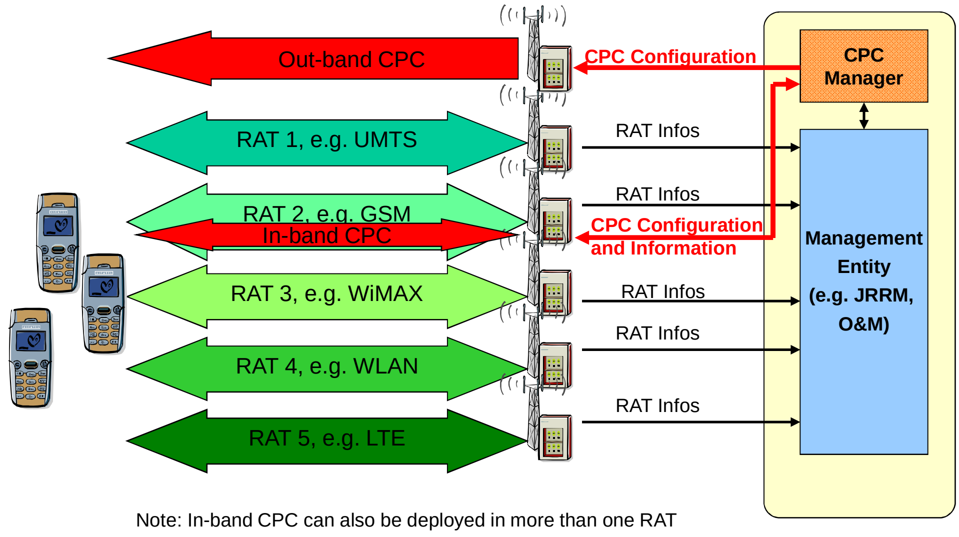

Figure 1: Principle of in-band and out-band Cognitive Pilot Channel (CPC) [i.3]

The out-band CPC is a CPC conceived as a radio channel outside the component Radio Access Technologies. The out-band CPC as also shown in Figure 1 either uses a new radio interface, or alternatively uses an adaptation of a legacy technology with appropriate characteristics. The out-band CPC ideally should operate on a well-know frequency, however, it is likely difficult to agree and regulate a worldwide unique frequency for such an out-band CPC.

5.1.2 Access Network Discovery and Selection Function (ANDSF)

The 3GPP Access Network Discovery and Selection Function (ANDSF) [i.13] can be seen as higher-layer CPC using RAT-independent, e.g. IP-based transport. The scope of the ANDSF is to support multi-access network scenarios with intersystem-mobility between 3GPP-networks (GSM, UMTS, LTE) and non-3GPP networks (e.g. WiMAX, WLAN).

The ANDSF as defined in 3GPP provides inter-system mobility policies and access network specific information from the network to the user equipment (UE) in order to assist the mobile node for discovery procedures and for performing the inter-system handovers. This set of information can either be provisioned in the UE by the home operator, or provided to the mobile node (MN) by the ANDSF [i.16].

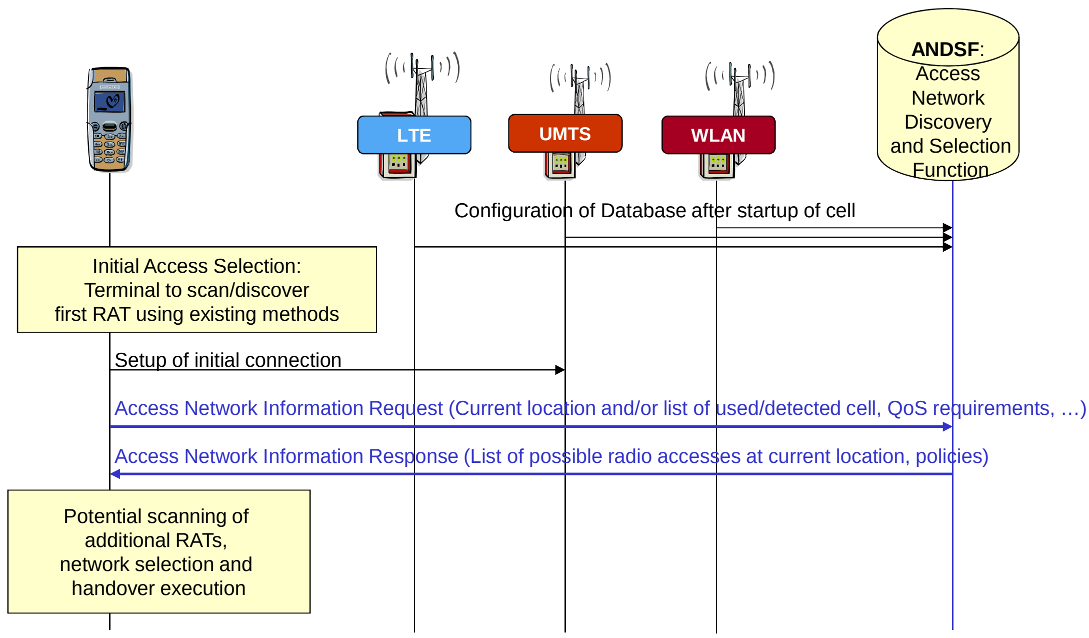

Figure 2: Example of radio access technology independent communication with ANDSF

5.1.3 Assisted Cell search with a helper device

Assisted Cell Search can be performed by helper device to provide cell information needed for a UE to synchronize with a suitable local cell. This helper device can be a nearby network operator-provided device or another UE that is capable of providing local cell information through a cognitive or ad-hoc network. When a UE is powered on in a new location, it is likely to be in close proximity of a helper device. The Assisted Cell Selection procedure requires the UE to discover the nearby helper device and establish communication with it. The UE will then query for the carrier frequencies and cell parameters, which the queried device will provide and the UE can search for this cell. Once the UE has found a suitable cell, the UE will select it. Since the information being provided is either from the network or by a UE that is already camped on a cell, the likelihood of that cell being suitable for the UE is high.

In order for this procedure to be effective the information exchange should be performed over a known control channel. This control channel could exist on any suitable RAT available to the UE i.e. Wi-Fi, or Bluetooth®. It can be implemented by means of one of the methods discussed in Clause 7.

The Assisted Cell Search concept is illustrated in Figure 3.

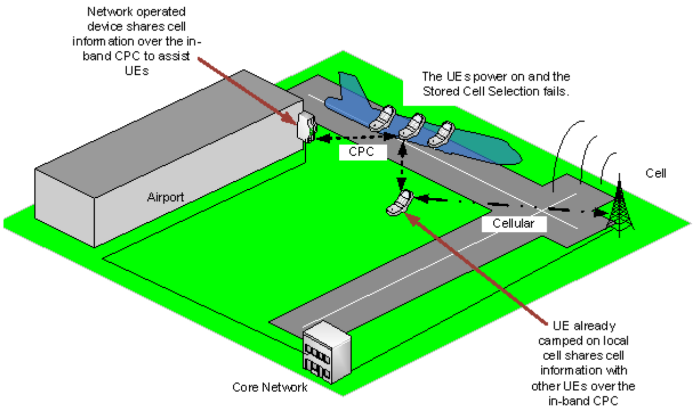

Figure 3: Assisted Cell Search concept

The helper devices can be also be used to speed up other processes. A UE which has synchronized to a suitable cell will want to decode the BCH in order to obtain system information. The BCH broadcasts MIBs/SIBs according to a schedule and it can take several seconds to acquire a full set of system information. In order to improve the performance of the system by reducing this time, the UE may be able to acquire the broadcast information by prompting a helper device.

The helper devices can also be used to share network functions and services e.g. instant messaging, push-to-talk services etc. If a new UE is aware of the services being provided by a network before camping on it, it can save time by choosing a cell that fulfils its needs on the first try.

5.2 Advanced Multi-RAT Assistance in Heterogeneous Networks

Networks in a home/office environment may operate exclusively over a single RAT, but many of the devices within these networks may be capable of operating on multiple different RATs simultaneously.

When networks operate independently on their respective RAT, each of these networks is typically 'closed' that is, there is no coordination between the network technologies, and they rely on their own procedures for network formation, network discovery, service discovery, and interference management. Many coexistence issues exist because there is no coordination between these cognitive radio networks, therefore networks operating in unlicensed bands will require new coexistence schemes in order to optimize radio resource usage. These coexistence schemes can be enabled by a new Control Channel for Cognitive Radio Systems. This channel can provide assistance for network coexistence, via the transmission of context information and measurement results, and also enable Multi-RAT control.

Inter-working between different RATs has been considered or implemented in areas such as 3GPP and IEEE 802 (e.g. I-WLAN, EGAN, IEEE 802.21 [i.29]). For instance, the IWLAN [i.4] suite of specifications allows UEs capable of WLAN access to use 3GPP services at the application layer (e.g. access control and charging, PS services, service continuity) through the WLAN RAT. I-WLAN and other multi-RAT services have focused mostly on data services and session continuity-based services. 3GPP has also specified multi-RAT RRM between 3GPP access networks (GSM, UMTS, LTE) [i.5] to dynamically select the best RAT for a particular service to reach a UE. However, these specifications have not considered certain scenarios of the use of devices with Multi-RAT capability to provide assistance services at the RAT and network layers for helping in network specific operations. Some of these scenarios, discussed in further detail in the following, constitute a form of assistance service that will be referred to as Advanced Multi-RAT Assistance.

Advanced Multi-RAT Assistance uses the ability of a particular device to communicate on different RATs in order to provide advanced services to networks on which that device is not active. A device's multi-RAT capability can be used to provide assistance to networks in an effort to coordinate transmissions across networks, and to improve the performance within a network. As can be seen in Figure 4, devices exist that are active on one network but are still capable of communicating with other network(s). A device that is active on RAT A could activate RAT B in order to (for example) track a Network B device without tracking capability.

Advanced Multi-RAT Assistance requires a control channel for information collection from the networks as well as signalling to carry control or assistance information to the networks, that is necessary for Advanced Multi-RAT Assistance procedures. In order to provide some of the assistant services, a central control point (CCP) may be used for information collection and decision making. The CCP would be expected to have multi-RAT capability. The networks can be governed by the same operator, different operators, or could be Wi-Fi networks with no operator.

Conceptually, Advanced Multi-RAT Assistance helps coexistence issues not only by minimizing interference, but also by expanding the pool of services available to devices to include services from devices outside the local network (i.e. each RAT forms its own local network). The services offered by every device (regardless of their active RAT) are added to a common service pool, but in order to access this pool a common control channel capable of RAT-agnostic communication is necessary.

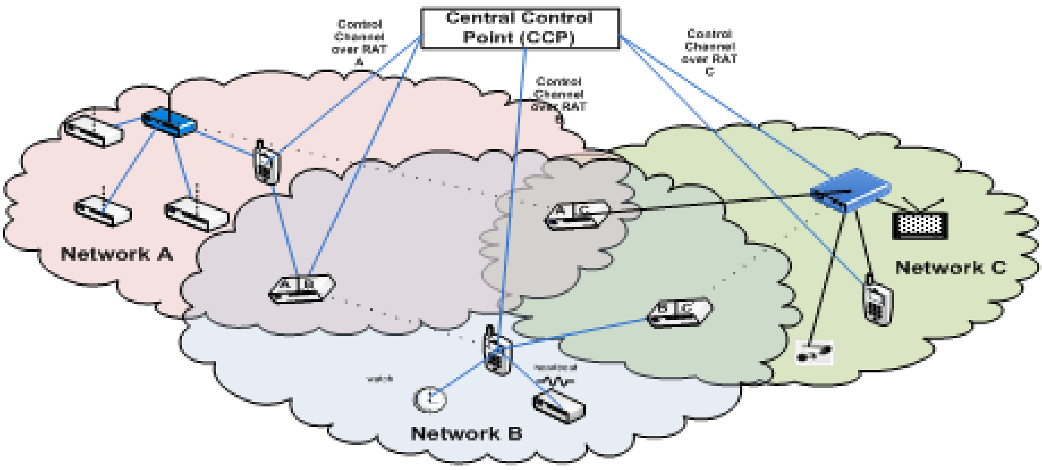

Figure 4: Advanced Multi-RAT Assistance Enabled by CCP

Some of the assistance service scenarios provided by Advanced Multi-RAT Assistance are described in the clauses below.

5.2.1 Inter-Network Sensing Assistance

Network A or device(s) belonging to network A can be requested to sense the operating channel of network B and report the results to a CCP. This could be useful for networks consisting of low-powered devices with limited sensing capability.

In a context of low power low complexity devices like ZigBee®/802.15.4 capillary networks, these devices spend most of their time in a sleep mode to save power (especially non-powered devices) and have limited sensing capability. By nature, these types of networks do not perform active RF-measurements. Therefore, they are subject to dynamic interference. In that context, a co-located network like the WI-FI Network (Network A) could take specific sensing measurement to assist a ZigBee®network.

The CCP collects devices location information and operating characteristics of a ZigBee® network as well as a Wi-Fi Network which includes the operating channel of the ZigBee® network. The CCP then instructs Wi-Fi devices to perform periodic RF-measurements on the ZigBees'® operating channel with specific sensing algorithm applicable to ZigBee® network. These RF-Measurements (per device) are collected periodically at the CCP. Only RF-measurements of Wi-Fi devices collocated with the ZigBee® devices are considered. If interference is detected, the CCP informs the ZigBee® network and/or controls the ZigBee® network to initiate a network channel switch.

Optionally, the CCP can also instruct the Wi-Fi devices to monitor a valid alternate channel for the ZigBee® network. Once the high interference is detected, the CCP can control the ZigBee® network to switch channel to the validated alternate channel. Hence, the service discontinuity, which occurs as a result of the interference, is reduced at the ZigBee® network.

5.2.2 Network Service Discovery Assistance

A device that is active on network A may need assistance in finding or joining a service (e.g. a Bluetooth® gaming session) that is available on a different RAT that the device supports. This can consist of using fused information including the information of available/ongoing services on plurality of RATs in order to assist a device (or devices) from a capillary network to enable a specific RAT and use a service.

For example, after turning on, a Smartphone device could attach to the CCP through the control channel. Upon attaching, the Smartphone could inform the CCP about its service preferences and its capabilities. The CCP could issue a directed response to the Smartphone with service offerings in its vicinity (based on the device's preferences/capabilities). Alternatively, the Smartphone could be made aware of the service offerings through CCP broadcast information. After a user selects an ongoing service, like a game, the CCP can assist the Smartphone with the location where the game is taking place and provide a direction and/or a distance. While the user is moving to the location (a room in the house) where the game is taking place on a Bluetooth® network, the CCP assists the Smartphone in enabling its Bluetooth® RAT (by default is disabled) and configures it with the channels to use and the channel hopping sequence. Therefore, the Smartphone can have a fast association to the Bluetooth®network which offers a fast game start experience to the user.

5.2.3 Location Tracking by Proxy

A device that is currently active in a given network A is requested to track the location of a device with unknown location or with no location tracking capability belonging to network B.

A request to track a device with unknown location is handled by the CCP by first identifying one or more devices with known location or tracking location capability and with RAT capability compatible the device with unknown location. The identified devices will activate the compatible RAT and start scanning around to actively or passively detect the presence of the device with unknown location. If one device finds the device to be located, it will inform the CCP and provide additional observation characteristics such as signal strength.

One example of this could be a request to find a Bluetooth® enabled camera. As shown in Figure 5, smartphones spread around a house or other consumer electronics devices with known location could be requested via the CCP to activate the Bluetooth® radio and scan for the camera using Bluetooth® technology and reporting the location information back.

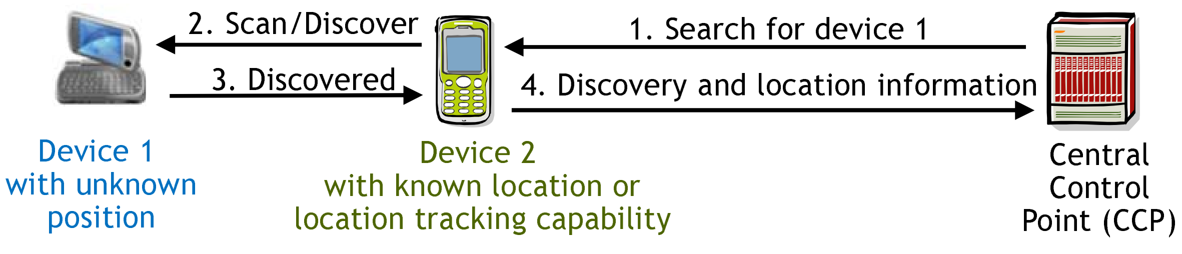

Figure 5: Example of location tracking by a proxy

5.2.4 Network Optimization

Network load within a network can be reduced by moving different device(s) between RATs or by changing a device's parent router which could be on the same or different RAT.

For example, the CCP may decide to rearrange a network. For instance, it may decide to split a network into two, or more, smaller networks and provide inter- network communication between these. The throughput on each of the split networks could then be independently maximized. This would require that the CCP be made aware of the load in a capillary network (e.g. routing congestion, delay statistics, throughput statistics, etc.). Alternatively, the CCP may instruct specific devices to change their parent router (to another more lightly loaded router).

5.2.5 Assistance for Network Healing

A device with multi-RAT capability can be set up to provide network healing assistance to a given network by communicating with a singleton node (a node that has lost connection to its original network) or neighbour nodes to reconnect the singleton node with its network.

As a first step, the CCP collects information about the different capillary networks in terms of their connectivity, their location and their RAT capabilities. Information is gathered and fused. The CCP can run an application to detect or confirm that a device in given network (e.g. network A) is not connected to the network, referred as singleton device or node. The singleton detection application could also be triggered by some of the devices in the network informing the CCP.

A network healing assistance application is triggered in the CCP where using the information previously fused, the CCP identifies a device with multi-RAT capability (e.g. a device with RAT capability Y assuming network A uses RAT Y) in the vicinity of the projected location of the singleton node. Since this device may not have the RAT used by capillary network A active, the CCP will inform the healing device of its needs, possibly using the device's current active RAT (e.g. RAT X). This will trigger the activation of RAT Y which is used by the singleton node. The healing device will communicate with the singleton node or possibly neighbour nodes to reconnect the singleton node with its neighbours.

To illustrate this, capillary network A could be for example based on Bluetooth® technology (Bluetooth® = RAT Y). In a scatternet, Bluetooth® nodes can be master or slave nodes. A master node cannot connect with another master node, therefore creating a bottleneck in the capillary network. The healing device could interact with these nodes and force them to change their role thus repairing the node permanently.

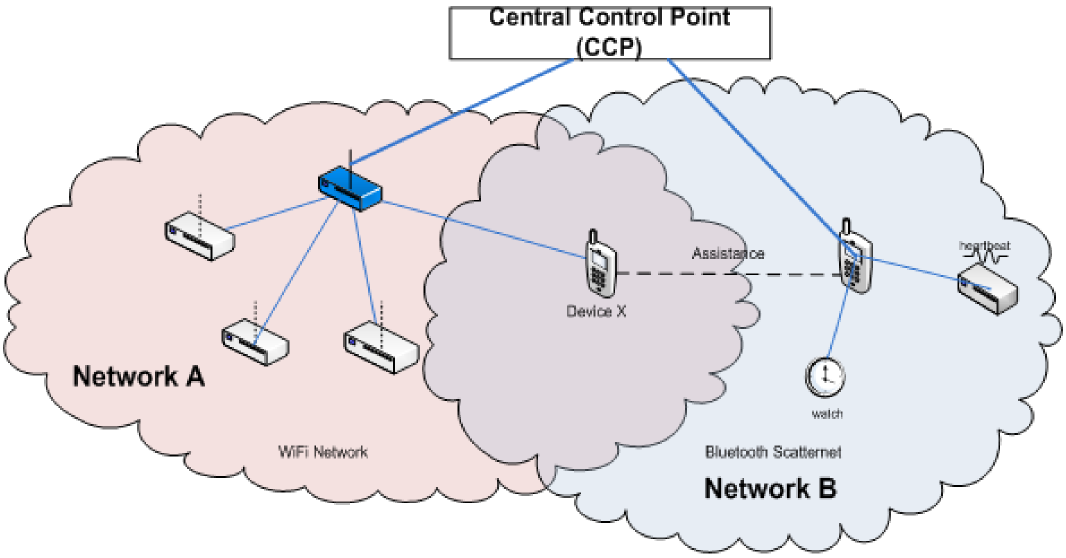

Figure 6: Multi-RAT Assistance between Wi-Fi and Bluetooth® Networks

In example 1, Network A consists of a Wi-Fi network (e.g. 802.11) and Network B consists of a Bluetooth® piconet. Device X indicates to the CCP the ability to provide Multi-RAT control services over the Bluetooth® RAT. This device can be instructed by the CCP to assist the piconet through some assistance services. The request would be sent by the CCP to device X (over the Wi-Fi RAT) for Device X to activate its Bluetooth® RAT and provide assistance services to a nearby Bluetooth® network.

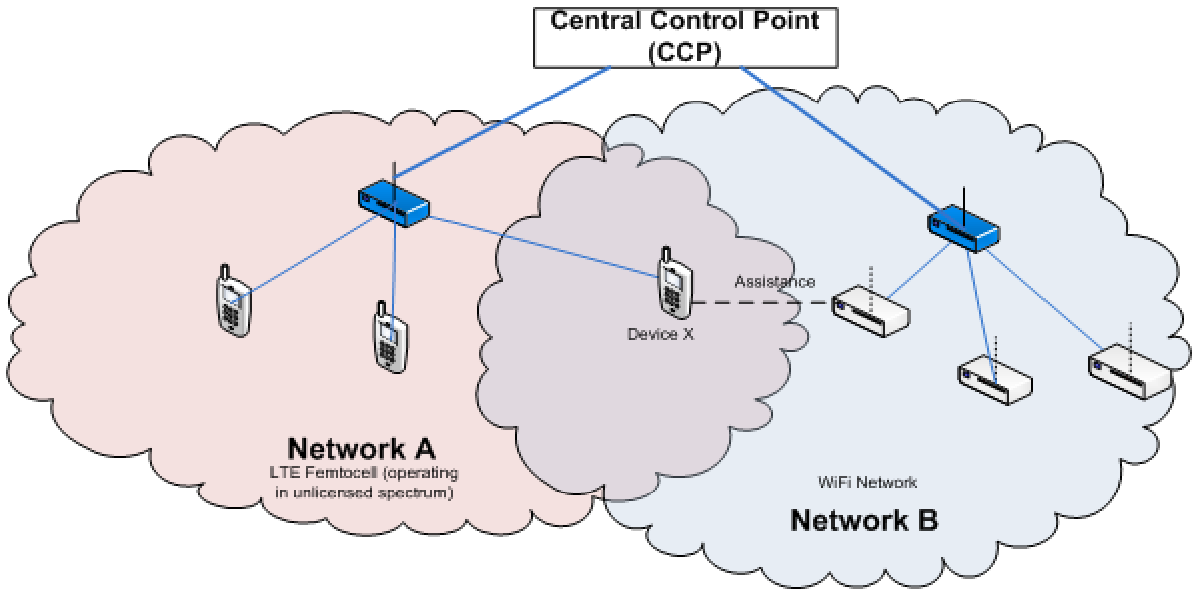

Figure 7: Multi-RAT Assistance between LTE and Wi-Fi

In example 2, Network A consists of an LTE network managed by a HeNB, and Network B consists of a Wi-Fi network. Both networks are operating over the unlicensed bands. Device X has been allowed by the operator of Network A to provide Advanced Multi-RAT services over the Wi-Fi RAT and indicates this to the CCP. This device can be instructed by the CCP to assist the Wi-Fi network through some assistance services. One possible solution for this is example is that the CCP provides "Access Network Discovery and Selection Function" (ANDSF) as specified by 3GPP [i.16] and [i.6].

The control channel in each of the examples above will allow the device to advertise the Multi-RAT assistance service it can provide (based on operator policies, for example) and will allow the CCP to determine which networks can make use of Advanced Multi-RAT assistance.

5.3 Retrieval of information on available White Spaces from a geo-location database

The Control Channel for Cognitive Radio Systems may be used to retrieve information on available white spaces at the devices location from a geo-location database. As shown in Figure 8, an access point or base station can access the geo-location database to retrieve information on available white spaces. In addition, Devices forming e.g. an ad-hoc network or an opportunistic network using white spaces need also to access the geo-location database.

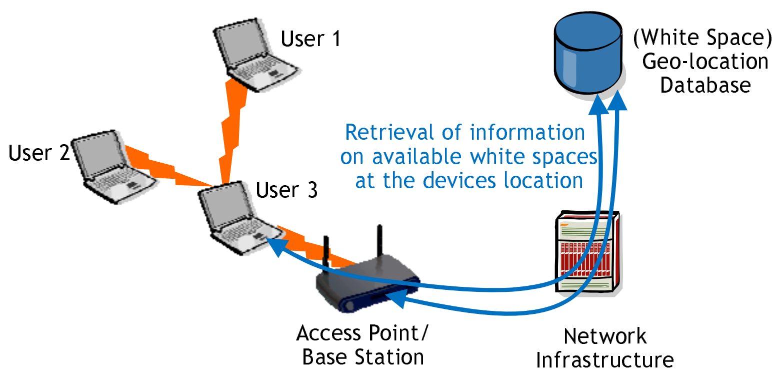

Figure 8: Using the Control Channel (shown in blue) to retrieve information on available white spaces from a geo-location database

Further use cases for operation in white space frequency bands can be found in [i.7]. A candidate protocol to access the geo-location database may be the "Protocol to Access White Space Databases (PAWS)" as currently developed in IETF [i.8].

6 Management of operator-governed opportunistic networks

6.1 Scenarios

This clause outlines five main scenarios where operator-governed opportunistic networks can be used with clear benefits for the actors, by creating opportunities for solving persistent issues of mobile networks or for offering new type of services on top of existing infrastructure. These scenarios are exploited so as to derive technical challenges related to the various phases of the management of opportunistic networks (suitability determination, creation, maintenance and termination).

The first scenario, **"Opportunistic Coverage Extension"**, describes a situation in which a device cannot connect to the network operator's infrastructure, due to lack of coverage or a mismatch in the radio access technologies. The proposed solution includes one or more additional connected users that, by creating an opportunistic network, establish a link between the initial device and the infrastructure, and act as a data relay for this link.

The second scenario **"Opportunistic capacity extension"** depicts a situation in which a device cannot access the operator's infrastructure due to the congestion of the available resources at the serving access node. The proposed solution proposes the redirection of the access route through an opportunistic network that avoids the congested network segment.

The third scenario **"Infrastructure supported opportunistic ad-hoc networking"** focuses on the creation of an infrastructure-less opportunistic network between two or more devices for the local exchange of information (e.g. peer-to-peer communications, home networking, location-based service providing, etc.). The infrastructure governs the ON creation and benefits from the local traffic offloading, as well as on new opportunities for service providing.

The fourth scenario **"Opportunistic traffic aggregation in the radio access network"** describes the usage of a local opportunistic network among several devices, in order to share a reduced number of infrastructure links towards a remote service-providing server or database. This situation allows some degree of traffic aggregation and caching that is useful to improve the overall network performance.

Finally, the fifth scenario **"Opportunistic resource aggregation in the backhaul network"** depicts how opportunistic networks can be used to aggregate both backhaul bandwidth and processing/storage resources on access nodes. In this case, the ON is created over access points rather than user terminals, thus offering a new focus on system performance improvement.

Actors identified for the various scenarios are the following:

Radio Access Network Operator (RANOp). A Radio Access Network Operator is the provider of mobile access via e.g. a cellular network, a Wi-Fi AP or a femto BS. It is responsible for the infrastructure node maintenance and for the deployment of the opportunistic networks and relevant technologies, plus specific decision-making logic to address the optimization goal.

Its main roles are:

- Setting up of the framework for ON existence, including its own equipment (macro- or femto-BS), resources (spectrum, policies, management capabilities) and context information (policies, knowledge on the operational scenario and on the profiles of the involved users, applications and devices).
- Full control of the lifecycle of ON, from suitability determination to the release decision.
- Full control of the authentication, selection and authorisation of the UE nodes contributing to its ON, based on subscription data and contextual data.
- Full control of routing of traffic and signalling within the ON and towards the infrastructure.

Service Provider (SP). A SP is the provider of a specific service that may need to be supported over an opportunistic network, so they need to request the establishment of an ON to the RANOp. In many cases, SP and RANOp are the same entity, so these requests are simplified.

A SP can also provide some supporting functionalities used within the ON management systems. For instance, a geo-located spectrum database provided by a third party may be used by a RANOp to feed its decision-making processes regarding spectrum suitability detection and selection.

Its main roles are:

- Collect context information (Quality of Service (QoS) requirements of the requested application, identification of end users, etc.).
- Monitor the performance of the application.
- Interface with the RANOp to request the creation/modification/release of the ON.
- Provide supporting functionalities for ON management.

ON End Users/Terminals. An ON End User/Terminal is the user/device which benefits or "enjoys" a service provided through an ON.

It contributes to the definition of the QoS requirements on the in-ON communication chain and to the determination of suitability, creation, maintenance and release of the ON.

Its main roles are:

- Provide the operator with all information related to its own capabilities (e.g. Radio Frequency (RF) and power) and required for the ON management function, and pro-actively inform of any change.
- Provide the operator with all information related to its own situation (e.g. location, mobility, QoS requirements, user preferences, sensed interferences, etc.) and required for the ON management function, and pro-actively inform of any change.
- Provide the operator with all information related to other ON nodes it is connected to (e.g. link quality, identifiers, etc.) and required for the ON management function, and pro-actively inform of any change.
- Execute the required procedures for connecting/disconnecting to/from other ON nodes on request from the ON management function.

ON Supporting Users/Terminals. A supporting ON User/Terminal is an entity which supports the communication by forwarding/relaying the traffic from one or more end users towards the infrastructure (and vice versa) or between end users (in the case of local communication). One entity can be both End User/Terminal and Supporting User/Terminal at the same time.

Its main roles are the same as the ones of the End User/Terminal, except it has no own QoS requirement. In addition, it should serve the following roles:

- Optionally provide some local storage/caching capabilities to contribute to the global performance of the delivery, managed by the ON management function.
- Provide all capabilities and perform all procedures required to locally enforce the end-to-end security based on policies and data from the RANOp.

6.2 Technical challenges

This clause describes the technical challenges, which can be derived though the scenarios described in the previous clause, for the suitability determination, the creation of an ON, the maintenance and the termination of an ON. Figure 9 depicts the interrelation between the four operational phases of an ON (plus the Security & Trust - which exists during all phases) along with the key functionalities allocated in each phase.

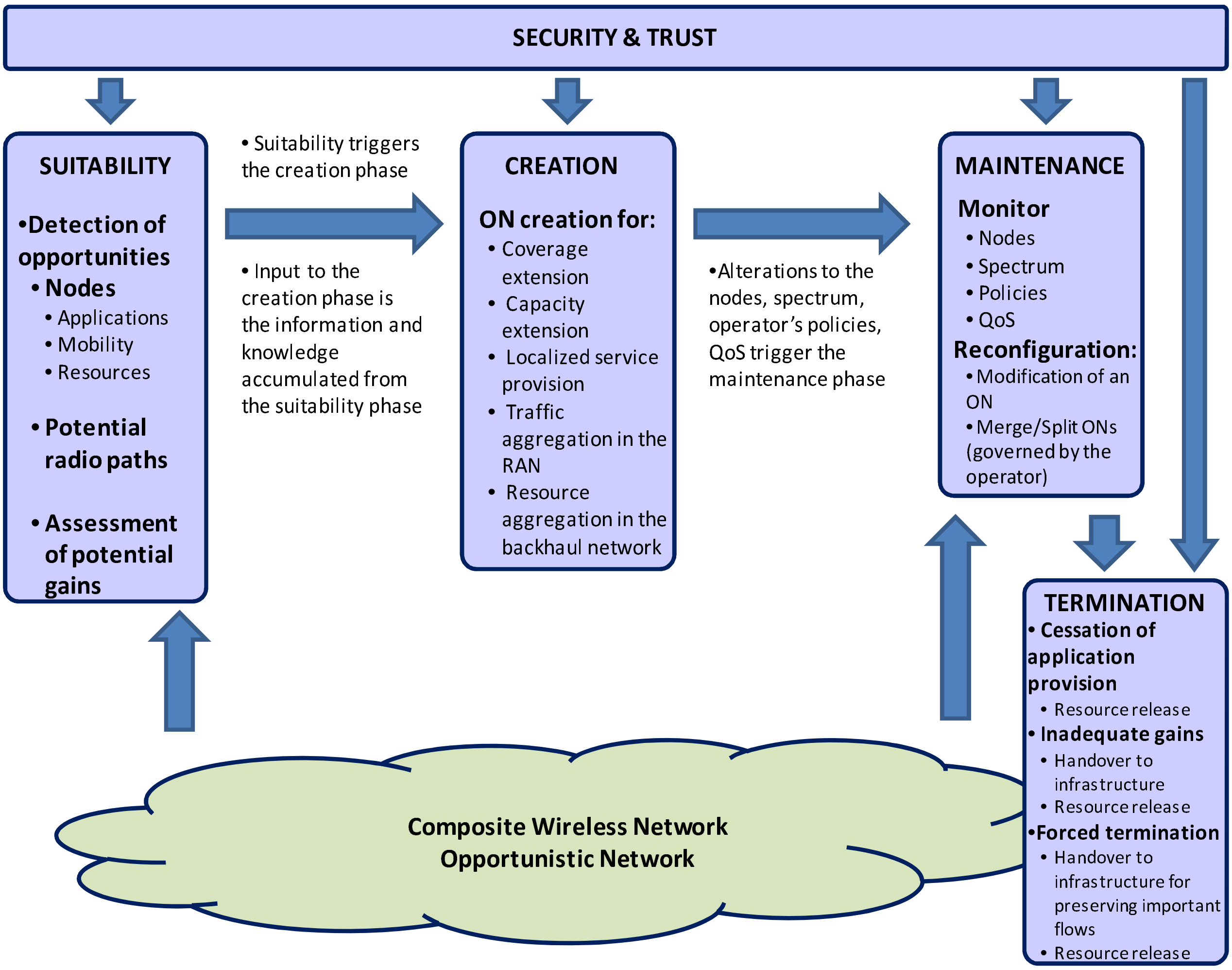

Figure 9: Main phases in the operation of an ON and related key functionalities

6.2.1 Suitability determination

This clause discusses on the suitability determination. It provides the definition, the triggers, the decomposition to sub-challenges and the output.

6.2.1.1 Definition

Based on the observed radio environment, the node capabilities, the network policies and the user profiles, the outcome of the Suitability Determination phase is to decide whether it is suitable to set-up an ON or not, at a specific time and place. The suitability assessment constitutes a first decision towards the creation of an ON, as a result of a rough initial feasibility analysis, in order to keep complexity moderate.

6.2.1.2 Triggers

The suitability determination phase may be triggered in the following cases:

- By the existence of node(s) which is(are) out of infrastructure coverage.
- By the overloading of the infrastructure's access network.
- By the existence of local application end-points.
- By the excessive overheads, the poor channel quality, the limited node capabilities, or the minimization of the time needed to transition from dedicated to common channels and vice versa.
- By the congestion in the backhaul of the infrastructure network.

6.2.1.3 Sub-challenges

The following sub-challenges are considered at the suitability determination phase.

6.2.1.3.1 Detection of opportunities for ON with respect to nodes

The operator needs to be aware (by discovery procedures) of the nodes' related information. Each node is distinguished by a set of characteristics. Node characteristics will include the capabilities (including available interfaces, supported RATs, supported frequencies, support of multiple connections, relaying/bridging capabilities) and status of each candidate node in terms of resources for transmission (status of the active links), storage, processing and energy. Moreover, the operator needs to be aware of the location and the mobility level of each node. A prerequisite is that the nodes need to have some type of access to the infrastructure, or to have some type of access to a decongested AP, or to be close enough, or to have high capabilities and/or good links to the macro BS, or to have some type of access to a decongested BS in the backhaul, respectively.

Furthermore, application requirements and the similarity level of the requested applications (i.e. common application interests) should be taken into consideration by defining the involved applications, their resource requirements, and their appropriateness for being provided through opportunistic networks.

6.2.1.3.2 Detection of opportunities with respect to potential radio paths

Identification of the potential radio paths is a rather crucial factor for the ON existence. ONs will operate in a dynamically changing environment, where inter-ON interference may be possible. It is important to find how many nodes are within the range of a given node, depending on the spectrum and the power used. In order to select the spectrum for the operation of the ON, there is the need to introduce mechanisms leading to the identification of spectrum opportunities (e.g. the available spectrum from the infrastructure side) that also ensure that the resulting interference conditions are acceptable. Spectrum sharing/ spectrum pooling mechanisms should be included to the solution in order to enable dynamic and efficient utilization across licensed and unlicensed (license exempt) spectrum. Furthermore, in terms of reallocation of resources from macrocells to femtocells, the MC-HSPA or the LTE-Advanced could be the only applicable technology. Finally, the segregation of spectrum allocations/channels for different ONs Energy Management may minimize spectrum pollution and energy consumption through better system efficiency.

6.2.1.3.3 Assessment of potential gains

The deployment of the ON approach is related with some gains. This paragraph considers the potential gains from a possible ON launching, with respect to technical network management metrics. These gains may be achieved through the application provision with a fair QoS, the efficient spectrum utilization and the lower transmission powers, which can lead to lower energy consumption (for the operator's BS). Finally, the potential positive impact to the operator's cash flow could be considered.

6.2.1.4 Output

The suitability determination will give as an output a request for the creation of the opportunistic network, associated with a pre-selected set of candidate nodes that offers at least one radio path to an infrastructure AP and at least one radio path between each pair of nodes. In case of a positive response to the creation request, feasibility analysis conducted in the suitability determination will provide alternatives/options to be further explored in the creation phase.

6.2.2 Creation

This clause discusses on the ON creation. It is structured similarly to the suitability determination phase.

6.2.2.1 Definition

This phase creates the opportunistic network based on the input received from the suitability determination phase. It focuses on choosing optimal radio paths (spectrum/power) along with routing scheme, based on these radio paths, in order to ensure optimal QoS. Finally, it performs all the required procedures to effectively connect ON members with each other and to ensure continuity of service for the members with regard to the infrastructure and it typically manages handover from the infrastructure to the ON when required.

6.2.2.2 Trigger

This phase is triggered mainly by the request for creation of the suitability determination phase.

6.2.2.3 Sub-challenges/Output

Given the output of the suitability determination phase, the output of the creation phase will consist of the selected nodes, the selected routes, and the selected spectrum followed by the signalling procedure establishing the ON. Notice that, in some cases, the creation phase could also come up with a decision for not finally establishing the ON. Additionally, in some cases, specific network creation challenges may be considered as follows.

6.2.2.3.1 Infrastructure coverage extension

For the successful creation of the network it is needed to determine the participant nodes, the spectrum/RATs selection and the topology between the nodes. The topology contains information on which nodes are covered by the infrastructure, which nodes are in vicinity of each other and which nodes are out of direct coverage of the infrastructure.

6.2.2.3.2 Resolve capacity issues of the infrastructure

In order to solve capacity issues of the infrastructure through an ON, initially it is needed to determine the problematic/overloaded area. Additionally, a node should be denoted which is part of the congested area and can directly access an uncongested area or by the use of interconnected mediators. In this case, that node will act as a gateway.

6.2.2.3.3 Opportunistic ad-hoc networking (for localized service provision)

In the case where there are closely located nodes which are willing to use the same application/ service, then an ON can be created among them, in order to locally serve them. Again, it becomes clear that the selection of the participant nodes, the spectrum availability and the interconnection of nodes is rather important in order to successfully create the ON.

6.2.2.3.4 Opportunistic traffic aggregation in the access network

In order to enable a better utilization of the available radio resources through an ON, an aggregator node(s) which will act as a gateway and provide the interconnection between the macro BS and the ON via a dedicated channel needs to be identified. The gateway node(s) should have strong resources and high quality of link (or links, in case of multiple interfaces) with the macro BS. Finally, it should be located in a good position/location regarding the macro BS (i.e. low level of interference, inbound the service area of the macro BS etc.) in order to be able to establish and maintain the connection.

6.2.2.3.5 Opportunistic resource aggregation in the backhaul

Finally, the ON may be created in order to handle resource aggregation in the backhaul network, in cases when the backhaul experiences overloading situations. Thus, a multiple-BS opportunistic network is created with respect to the above considerations.

6.2.3 Maintenance

The ON should be dynamic during all its operational life-time. In order to achieve this, once the creation phase has been completed, the maintenance phase should be initiated.

In general, the maintenance phase will:

- monitor nodes, spectrum, policies, QoS; and
- decide whether it is suitable to proceed to a merge/split of an ON, or to a reconfiguration of an ON.

6.2.3.1 Definition

The maintenance phase is responsible for applying, at the right time, all the appropriate changes at the ON configuration, in order to maintain the efficient operation of the ON and to provide adaptability to changing environmental conditions.

6.2.3.2 Trigger

The trigger to the maintenance phase is the successful completion of the creation phase.

6.2.3.3 Sub-challenges/Output

This phase key sub-challenges are the monitoring of the ON environment and the dynamic implementation of all the appropriate reconfigurations at the ON.

6.2.3.3.1 Monitoring

One basic process of the maintenance phase is that of acquiring information from ON nodes about their experiencing application QoS, mobility, spectrum condition changes and policy changes. This monitoring information will be used to define a fair level of the ON operation. This involves a variety of mechanisms and strategies whose target is to ensure the preservation of application provisioning and that the established QoS criteria are met by properly handling interference. Additionally, this information can be exploited so as to control/check that the amount of relaying of different does not affect the effectiveness of the ON. In case it is derived from the monitoring process that it is necessary appropriate reconfiguration actions may take place.

6.2.3.3.2 Reconfiguration decisions

This clause contains the reconfiguration decisions that can be made during the maintenance phase. These decisions can be made because of alterations in ON nodes' status, radio paths conditions or in policies.

6.2.3.3.2.1 Reconfiguration of an ON

The reconfiguration process, which is part of the ON maintenance phase, is responsible for applying all the appropriate changes at the ON configuration in order to achieve the most efficient operation of the ON. The reconfiguration process is triggered in cases of changes that may affect the operation of an ON. More specifically such changes may include alterations in the status of ON nodes (nodes leaving or new nodes joining), in the gateway of the ON, in the available spectrum, in policies by the network operator which affect ON users, etc.

6.2.3.3.2.2 Merging/Splitting of ONs

A special case of reconfiguration decision/actions that may be made during the maintenance phase is the merging or splitting of ONs. Merging/splitting decisions in any case is operator governed. Merging of ONs that are closely located may be triggered to enforce service provisioning in a certain ON. Similarly splitting of an ON into smaller ONs may enable maintaining efficient service provisioning.

The challenges which derive from the merging/splitting procedure can be listed as follows:

- The network operator should be aware of the ONs which operate in the same area, each ON current status, which means to have information about its serving users and each user condition (e.g. resources, location, provided QoS), and also to be aware whether or not an ON is in a critical situation (which means that is difficult to continue operating).
- If an ON splitting is going to take place, then a suitability determination, followed by a creation process, should be initialized.
- The network operator should arrange the handover of the weak ON's users to the better ON or to the new born ONs, in order to finish the merging/splitting procedure.

6.2.4 Termination

6.2.4.1 Definition

The termination phase will eventually take the decision to release the ON, thus triggering all the necessary procedures and associated signalling. It is distinguished according to the reason of termination. As a result we may have termination of the ON due to cessation of application provision, termination due to inadequate gains from the usage of the ON and forced termination.

6.2.4.2 Triggers

The triggers are distinguished according to the type of the termination, whether it is due to cessation of application provision, due to inadequate gains or a forced one. The trigger for the termination due to cessation of application provision is that the applications that the ON delivered has finalized, so there is no need to keep the ON operating. The trigger for the termination due to inadequate gains is that the gains from the operation of the ON are no longer significant so the operator decides to terminate it.

On the other hand, a forced termination may be triggered by the following:

- Lack of resources.
- Inability to maintain the ON with the desired QoS.

6.2.4.3 Sub-challenges/Output

In all cases, there are some common sub-challenges that need to be addressed. Specifically, the release of resources applies to all cases of termination. On the other hand, the sub-challenge of the handover to infrastructure for preserving the most important flows applies only to the inadequate gains and forced termination, because in these cases, there is the need to disrupt as little as possible the on-going processes.

6.2.4.3.1 Handover to infrastructure

One of the main aims of the termination phase is to maintain flawless application streams in case of an ON release. Thus, it becomes important to provide seamless handovers between infrastructure and relaying/forwarding nodes, without major disruption to the end users who are already using ON's resources to establish communication links between each other. Finally, the most important flows should be preserved thus a mechanism for prioritized process handling may be needed in order to define in an effective way the important processes by assigning them higher priority level.

6.2.4.3.2 Resource release

When an ON termination procedure takes place, then the ON used resources are released. The released opportunistic network resources can then be allocated to another ON, in order to provide an extension to the infrastructure or to solve congestion issues, etc.

7 Implementation options for Control Channels for Cognitive Radio Systems

7.1 Radio access technology independent implementation

7.1.1 IEEE 1900.4 based Information model

The IEEE 1900.4 [i.10] and [i.11] has specified an architecture for the management of spectrum and radio resources in heterogeneous and cognitive radio networks. Although, no explicit transport mechanisms or protocols have been specified for the delivery of management information, an Application/IP-based implementation seems to appear as a most fit solution through the IEEE 1900.4 [i.10] specifications. Specifically, the standard introduces an information model at the application layer based on an object-oriented approach and specifically addresses a heterogeneous wireless communication framework. Three key groups of classes are defined:

- Policy classes.
- Terminal classes.
- Composite Wireless network classes.

For each of those classes above, IEEE 1900.4 [i.10] describes its members and their type, where data types are specified using Abstract Syntax Notation One (ASN.1) notations. TCP/UDP messages can be then used for the transportation of corresponding information elements. As stated in [i.12] IEEE 1900.4 [i.10]may reuse handover initiation and handover preparation Services defined by IEEE 802.21 [i.29].

7.1.2 3GPP ANDSF-based/OMA DM-based implementation

For the support of multi-access network scenarios with intersystem-mobility between 3GPP-networks (GSM, UMTS, LTE) and non-3GPP networks (e.g. WLAN, WiMAX), 3GPP defines the so-called Access Network Discovery and Selection Function (ANDSF) [i.13] which is located in the 3GPP Evolved Packet Core (EPC). The ANDSF provides inter-system mobility policies and access network specific information from the network to the user equipment (UE) in order to assist the mobile node for performing the inter-system handovers. This set of information can either be provisioned in the UE by the home operator, or provided to the mobile node (MN) by the ANDSF [i.13]. In 3GPP release-8, the ANDSF is located in the subscriber's home operator network (H-ANDSF) while in 3GPP release-9, the ANDSF can also be located in the visited network (V-ANDSF).

The information distributed between the ANDSF and the UE is defined in the ANDSF MO (Management Object) which is compatible with the OMA Device Management (DM) protocol specifications, version 1.2 and upwards as defined in the OMA DM Device Description Framework (DDF) as described in the Enabler Release Definition [i.14]. This OMA DM is based on the Synchronization Markup Language (Sync ML). Typically, the ANDSF MO is transported over the OMA DM over HTTP over TLS over TCP over IP.

The service requirements and the functional requirements for the access network discovery and selection are described in TS 122 278 [i.15] and in TS 123 402 [i.16] respectively.

Since the ANDSF is operator-controlled, it is typically used for distributing information related to the non-3GPP network nodes that are under the control of the same operator that owns the 3GPP network carrying the ANDSF. While it is in theory possible to extend the ANDSF MO to Cognitive Radio related parameters, it is of limited usefulness in a multi-operator heterogeneous environment where operators have no roaming agreement and should thus be tailored to the needs of a single operator.

7.1.3 Distributed Agents based approach

This clause outlines aspects of the implementation of Control Channels for Cognitive Radio Systems with the use of a multi-agent environment. Within such a multi-agent environment/system, every component (such as a network infrastructure element, a user device or management software) can be represented by one or more intelligent agents that act as a mediator between the components' functionality and the rest of the system. Thus, each system component is loosely coupled to other components and can interact by exchanging messages through a high level interface. In such a context, a Control Channel for Cognitive Radio Systems can be seen as a RAT-agnostic, upper layer logical communication channel (mainly over TCP/IP) between distributed agents/agent platforms lying in both terminal and network sides and used for the conveyance of context information.

The work of Foundation for Intelligent Physical Agents (FIPA) [i.17], which is an international non-profit association of companies and organizations with the aim of generating specifications of generic agent technologies, can be used to provide a standardized, transport solution for communication in the scope of Control Channels for Cognitive Radio Systems. More specifically, in order to promote interoperability between agent platforms, a number of standard MTPs (Message Transport Protocols) and MTP interfaces have been defined by FIPA, in particular an MTP based on the Internet Inter-Object request broker Protocol (IIOP) defined by OMG. In addition, FIPA neither defines nor requires a specific protocol for intra-platform message delivery and each implementation can choose any Internal Message Transport Protocol (IMTP).

Framed within the above, JADE [i.18] (JADEX [i.19]) is a robust, fully Java® and FIPA compliant framework for developing distributed agent systems and can run on both PCs and wireless devices that support Java® Micro Edition (Java® ME) using the package developed by the Lightweight Extensible Agent Platform (Leap) Project. JADE components exchange messages which are serialized and transmitted over TCP, according to the FIPA Agent Communication Language (ACL) message structure specification.

The JADE messaging architecture differentiates between intra-platform and inter-platform communication. In the case of intra-platform communication, agents reside in the same platform and JADE uses its IMTPs for implementing delivery services. In order to minimize delivery time, JADE selects the most appropriate transport mechanism further distinguishing between the case of communicating agents that reside in the same container and agents that reside in different containers. A container, which is hosted by a Java® Virtual Machine, provides the run-time environment and the services for one or more agents. More specifically, for the case of intra-platform communication, JADE utilizes:

- Event passing when both the sender and receiver agents are in the same container.
- Remote Method Invocation (RMI) when the sender and receiver agents are in different containers.

In the case of inter-platform communication, the following MTPs are currently available for interaction among agents:

- CORBA IIOP MTP based on standard Sun ORB provided with the JDK (the default installation).
- CORBA IIOP MTP based on ORBACUS [i.20].
- HTTP-based MTP.

Interestingly, JADE (JADEX) and the above transport mechanisms have been utilized for implementing the CPC concept [i.21] (following the information model specified in the standardized P1900.4 management architecture [i.10]). The results obtained from the experimentation and assessment on this JADE-based implementation showed satisfactory behaviour in terms of induced signalling loads (number of delivered bytes, bit-rate, overheads imposed by agents' communication) and time delays, that is equivalent to minimal intervention in the real network operation. Starting from this work, an extended information flow has been defined in the form of an ontology, and an enhanced platform has been developed, also based on JADE, with a special focus on openness, scalability and dynamic extensibility of the platform [i.22]. Indicative results derived through this platform show that even though there is still some overhead (due to the agent platform) the overall amount of information exchanged (even in situations where there is a large amount of data that needs to be transmitted) is realistic.

7.1.4 IETF DIAMETER based approach

The DIAMETER base protocol is an extensible protocol originally designed to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter is also used in 3GPP based networks to access the Home Subscriber Server (HSS) [i.23].

The advantages of the Diameter protocol as defined by in IETF in RFC 3588 [i.24] is that:

- It is an easily extensible protocol to which new building blocks can be added for different applications.
- It provides already security framework including Authentication, Authorization and Accounting (AAA); User authentication information is transported for the purpose of enabling the Diameter server to authenticate the user.
- Relaying of messages is supported: Diameter relays forward requests and responses based on routing-related AVPs and realm routing table entries. Since Diameter relays do not make policy decisions, they do not examine or alter non-routing AVPs.
- Proxying of messages is supported: In addition to forwarding requests and responses, Diameter proxies make policy decisions relating to resource usage and provisioning.
- Proxying is supported: Messages can be sent over different hops and each node may make necessary updates.
- Diameter is a well established protocol used e.g. also in TS 129 229 [i.23].

Diameter is thus a candidate protocol for the implementation of Control Channels for Cognitive Radio Systems as relevant messages and parameters can be defined as extensions to the Diameter base protocol.

Some existing Diameter messages may also be used for the management of opportunistic networks. For example, the Diameter Disconnect-Peer-Request/ Answer messages may be used in certain cases to disconnect the transport layer of a peer. Furthermore, the Diameter Accounting-Request/Answer could be used to inform the infrastructure about the creation or release of an ON. Further on, the Capabilities Exchange messages should be used to allow the discovery of a peer's identity and its Diameter capabilities (protocol version number, supported Diameter applications, security mechanisms, etc.).

Like the other options using IP transport, this option can only be used if an IP connection is already available but not in phases like discovery.

7.1.5 IETF PAWS based implementation

A "Protocol to Access White Space Databases (PAWS)" is currently developed in IETF [i.8]. IETF PAWS will develop a specification of the mechanism for discovering a white space database, the method for accessing a white space database, and the query/response formats for interacting with a white space database.

Figure 10 shows an example where a base station or access point uses the PAWS to retrieve information from a geo-location database in order to select the white space frequency bands which will then be used to communicate with the devices.

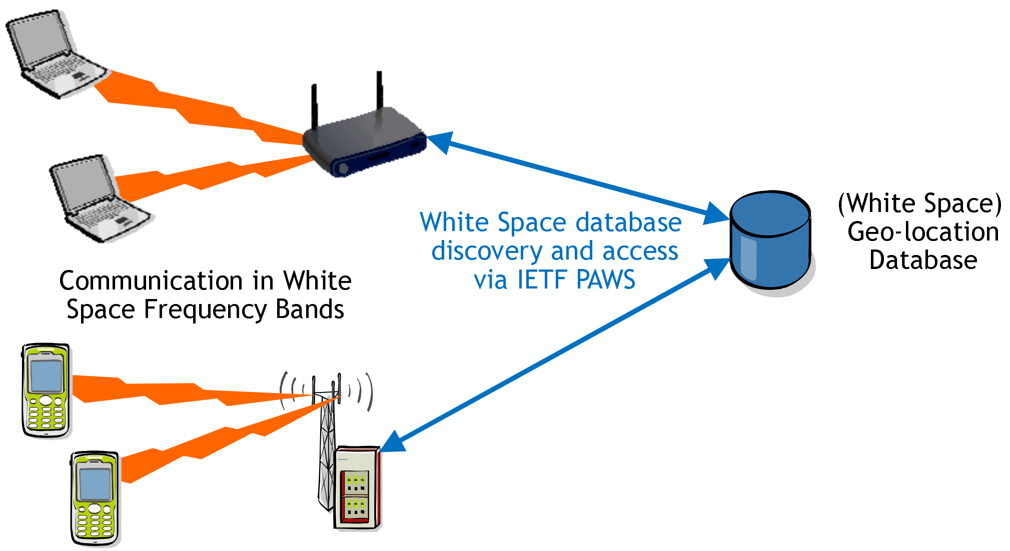

Figure 10: Using IETF PAWS to retrieve information on available white spaces from a geo-location database

As the development of this protocol is in a very initial state, it can currently not be judged if this protocol can be used or extended to be used for other coexistence and coordination purposes in cognitive radio systems besides accessing the white space geo-location database.

7.1.6 IEEE 802.21 based approach

The IEEE 802.21 "Media-Independent Handover (MIH) Services" standard [i.29] provides a set of extensible mechanisms mainly targeted to enable the optimization of handovers between heterogeneous IEEE 802 systems as well as facilitate handovers between IEEE 802 systems and cellular systems (e.g. 3GPP and 3GPP2). To that end, the standard defines:

- A new functional entity (i.e., MIH Function, MIHF) to be allocated within terminals and networks.
- A set of media-independent and media-dependent service access points (SAPs) for information exchange between the MIHF entity and other collocated system functional entities (e.g. link and network layer entities).
- A signalling protocol for message exchanging between remote MIHF entities.

The MIHF entity has some control on link layer operation though media-dependent SAP and offers a set of services to entities within upper layers of the protocol stack (denoted as *MIH users* according to 802.21 standard's terminology) though a media-independent SAP. Services provided to MIH users are classified as Media Independent Event Service (MIES), Media Independent Command Service (MICS) and Media Independent Information Service (MIIS).

MIIS is an information service conceived to provide mobile terminals with details on the (static) characteristics and services of the serving and neighboring networks (e.g. network type, operator identifier, frequency bands, etc.). MIIS is built on the specification of various Information Elements (IEs) that can be transferred between remote MIHF entities. IEs can be represented by means of two distinct methods specified in the standard: Binary representation and Resource Description Framework (RDF) [i.30]. In the former case, each IE is assigned a given binary identifier so that the addition of new IEs for other purposes than handover optimization is possible but requires an extension of the standard. On the contrary, in the case of RDF representation, it is possible to define an extended schema to introduce new IEs without requiring further modifications to the standard.

In addition to service specification, IEEE 802.21 [i.29] defines a complete protocol for message exchanges between remote MIH entities whose main characteristics are:

- Transaction oriented protocol. At any given moment, an MIH node should have no more than one transaction pending for each direction with a certain MIH peer.
- Support for reliable delivery service, flow control and fragmentation/reassembly. These functions are mainly intended to be used when transport mechanisms available to transfer MIH signalling messages between remote MIH entities do not support such functionalities.
- Each MIHF entity is identified by means of a network access identifier (NAI) that should be unique as per RFC 4282 [i.36] (e.g. fully qualified domain name). MIHF identifiers are included in all protocol messages. A multicast MIHF identifier is also defined.
- The protocol supports solicited and unsolicited MIH function discovery and capability discovery procedures.
- Transport-agnostic design: MIH signalling messages can be transferred by means of either layer 2 (L2) or layer 3 (L3) protocols.

MIIS and MIH protocol constitute two relevant pieces of the IEEE 802.21 [i.29] standard to be further considered in a potential implementation of Control Channels for Cognitive Radio Systems.

7.1.7 Network management based implementations

A further implementation option of CC-CRS is based on existing network management system solutions. Such an approach is applicable in cases where the network operator is willing to employ its own management systems to enable the exchange of CC-CRS data and would be especially useful to enable the exchange of data between different systems (in case the operator integrates and synchronizes different management systems). The basic idea of this approach is to reuse mechanisms and protocols employed by the management systems to exchange the CC-CRS relevant data between different network elements (e.g. ON signalling and/or Context information).

As the network management systems are not designed for the exchange of CC-CRS data, certain extensions are required to enable the exchange of CC-CRS relevant data. For example, Configuration Management (CM) changes should be applied immediately i.e. without any unnecessary delay which is usual in today's management systems because a delay may invalidate decisions resulting from the delivered data.

Similarly, the measurement data collection should also to meet the performance requirements of the Cognitive Management and Control Applications. Further on, new CC-CRS specific alarms may have to be supported.

The transmission and reception of CC-CRS messages over different management protocols such as SNMP [i.31] or TR-069 [i.32] could be achieved by translating between high level CC-CRS messages and low level protocol commands (such as GetParameterValues or SetParameterValues for TR-069). In such a case the transmission of a CC-CRS message could comprise e.g. several management protocol commands which would set values for manageable objects/parameters in a remote node. The reception of a CC-CRS message transmitted in such a form would require then a simple reading of the modified object/parameter values and combining it back to its original high-level form (see Figure 11).

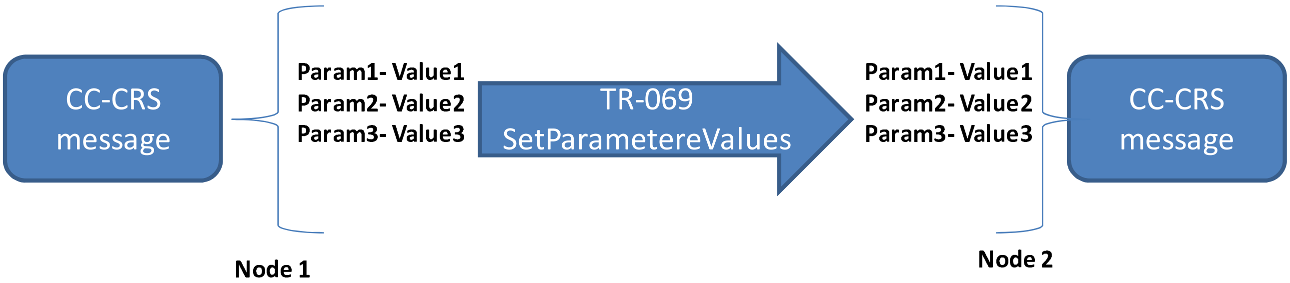

Figure 11: Possible realization of CC-CRS message transmission over TR-069 [i.32]

The main advantage of the proposed approach is the possibility of supporting CC-CRS in legacy systems. The main disadvantages of the approach are the additional load of network management systems (e.g. R, B interfaces in 3G/4G NMS [i.33]) and the necessary extension of Performance Monitoring (PM) and Configuration Management (CM) interfaces.

7.2 Radio access dependent implementation

7.2.1 3GPP based L1 and L2 implementations

The following clause reviews possible implementation options for the exchange of context information, policies and ON management signalling between UEs and infrastructure within 3GPP networks based on the reuse of the existing 3GPP interfaces and protocols. The following approach could be seen as an alternative to ANDSF which is based on the higher-layer protocols.

As can be seen in [i.34] and [i.35], the acquisition of System Information (SI) is possible in idle as well as connected states for UTRAN and E-UTRAN. An extension of the System Information (SI) broadcast methods of RRC seems to be then an appropriate way for delivering CC-CRS related information in downlink that is relevant to all UEs in a cell coverage. Such an extension would include the introduction of a new SI block. The information which could be exchanged using this method include e.g.:

- available non-3GPP access networks in the neighbourhood
- policies (e.g. related to the spectrum usage, related to forming an ON)
- available TV WS spectrum resources (e.g. for ON formation)

As some of the CC-CRS related information could be relevant only for certain UEs (e.g. some dedicated context information, distinct commands for establishment or release of an Opportunistic Network), a dedicated signalling method is also needed. For this reason some modifications to the UL/DL Information Transfer (for E-UTRAN) or UL/DL Direct Transfer (for UTRAN) procedures could be an option. These extensions would enable the transfer of CC-CRS data over Iub (UMTS) and Uu (UMTS/LTE) air interfaces to selected peer entities (in contrast to the broadcast of data described above).

For example, in LTE the "dedicatedInfoType" IE that is used in the *DLInformationTransfer* and *ULInformationTransfer* RRC Messages could be enhanced. The enhancements could be achieved, for instance, by adding a parameter like "dedicatedInfoCC-CRS" to create a new "channel" on top of RRC (non access stratum). If the "dedicatedInfoCC-CRS" IE is used, CC-CRS specific messages are exchanged and CC-CRS signalling is enabled between a UE and the infrastructure. This would however only work for distinct UEs that are residing in RRC_CONNECTED state. If a UE in RRC_IDLE was to send some CC-CRS data in UL direction, it would be required to kick-off the connection setup procedure (which consists of three transactions). The last of these messages is called "RRCConnectionSetupComplete" and would be used to indicate with the new "dedicatedInfoCC-CRS" IE if CC-CRS data is conveyed (in piggybacking mode).

As the information which is to be exchanged over CC-CRS is most likely to be collected and stored in a central database which could be located in the Core Network (as proposed e.g. in case of ANDSF) additional mechanisms enabling delivery of CC-CRS related data to the RNCs/HNBs (for UMTS) and eNBs/HeNBs (for LTE) are necessary. The additional mechanisms would complement the proposed RRC based approach and could be based on the use of the O&M systems (see clause 7.1.6) or the extension of the existing RAN and/or CN protocols (e.g. S1AP, RNSAP).

7.2.2 IEEE 802.11 based

7.2.2.1 Vendor Specific Information in MAC frames

The exchange of CC-CRS data between IEEE 802.11 devices, based on the existing IEEE 802.11 specification [i.25], can be achieved in two different ways. The first approach makes use of the Vendor Specific information elements (VSIE) which can be included in the management frames (e.g. Beacons, Probes, Action frames).

The Vendor Specific information element (VSIE) is used to carry information not defined in the IEEE 802.11-2007 [i.25] standard within a single defined format, so that reserved information element IDs are not usurped for nonstandard purposes and so that interoperability is more easily achieved in the presence of nonstandard information. The maximal size of the CC-CRS data which can be conveyed using this method is limited by the maximal size of the Information Element (IE) i.e. 255 octets (it is important to note that multiple VSIEs can be included in a single management frame).

The second approach is to use the Vendor Specific Action (VSA) frames which are stand-alone management frames. The size of the CC-CRS data which can be transmitted using the VSA frame in this case is limited by the maximum MMPDU size. In order to enable the data exchange between two not associated devices, Public Vendor Specific Action (PVSA) frames could be employed.

Table 1: Vendor Specific Information Element vs. Vendor Specific Action frame

Vendor Specific Information Element	Vendor Specific Action frame
Pros: • CC-CRS data transmitted along with beacons and other management frames Cons: • Only as part of 802.11 [i.25] management frames • Some octets are wasted on overhead and segmenting (CC-CRS PDUs may be segmented) • Additional overhead in case of a repetitive transmission (other 802.11 [i.25] IEs may not be required)	Pros: • No segmentation unless the size of maximum MMPDU is exceeded • Stand-alone management frame - No overhead due to the additional IEs Cons: • Large overhead in case of the exchange of small messages (L2 + L1 overhead)

It is worth noting that the implementation of CC-CRS requires an additional management entity to be implemented within devices. The new entity would be responsible for generation/reception of CC-CRS data and determining addresses of destination nodes. In case of the IEEE 802.11 [i.25] based approach, the new management entity would be responsible for the interaction with the IEEE 802.11 [i.25] MLME layer via Station Management Entity (SME) (SME may need to be extended to enable access of the new entity to the specific IEEE 802.11 [i.25] procedures).

7.2.2.2 IEEE 802.11u

An alternative approach for the transmission of CC-CRS data in 802.11 networks could be based on the Generic Advertisement Service (GAS) described in IEEE 802.11u [i.26] "Interworking with external networks". This service allows the exchange of arbitrary information between two not associated devices using public action frames. Additionally, 802.11u provides new IEs which can be included in beacons and probe responses to carry information about the type of information (Advertisement Protocol) which is being transmitted over GAS.

It is worth noting that the extensions proposed by IEEE 802.11u [i.26] (i.e. GAS and new IEs) are in principle based on the use of PVSA frames and VSIE fields, as proposed in clause 7.2.2.1. However, it is worth noting that the realization of CC-CRS based on IEEE 802.11u [i.26] could simplify the implementation (by the reuse of the existing procedures) and decrease the necessary standardization effort (in order to enable the transmission of CC-CRS data over GAS simply a new Advertisement Protocol ID (see [i.26], Table 7-43bi) would need to be introduced).

Similarly to the previous approach, the implementation of CC-CRS requires an additional management entity to be implemented within devices. The additional management entity would be responsible for generation/reception of requests and responses which are being transferred using corresponding GAS messages (i.e. GAS Initial Request, GAS Initial Response, GAS Comeback Request, GAS Comeback Response) as well as determining address of the destination node. It is worth noting that GAS request is always followed by the GAS response what may introduce additional overhead in case the exchange of CC-CRS data does not require acknowledgements.

7.2.2.3 Direct Wi-Fi Approach

Another possible approach for the realization of the CC-CRS could be based on Wi-Fi Direct. Wi-Fi Direct is a new solution provided by the Wi-Fi Alliance (WFA) which is based on IEEE 802.11 [i.25]. The solution introduces new features/functions which extend capabilities of Wi-Fi devices and enables for the direct communication without the use of an Access Point (AP). A major improvement is the notion of software AP supported by all Direct Wi-Fi devices, which allows new group configuration and topologies. The most relevant (from the CC-CRS implementation point of view) Wi-Fi direct features are related to the P2P Discovery and Group Operation functions.

Wi-Fi Direct provides additional information in 802.11 Wi-Fi MAC frame by using new specific Information Elements and new specific (Public) Action Frames. For instance, at the first steps of the node association in Direct Wi-Fi, additional information in VSIE is distributed which allows P2P Devices to have a coarse (and more precise if needed) overview about the status of neighbouring devices (e.g. connected or not connected to a network) and about the P2P Groups (e.g. list of devices in the group and their capabilities). The information collected during the P2P discovery (device discovery and service discovery) procedure could be easily used during the ON lifecycle (particularly in the ON suitability determination phase). Indeed the collected information from a Group Owner or from any probe response could be provided to some management entity which then chooses the best option for the ON creation. In order to provide additional ON specific information, further extension of the existing set of P2P Information Elements could be considered. In this case, the new IEs could deliver information related to e.g.: the type of network to which each node is attached (e.g. Wi-Fi, 3GPP legacy network), the ON to which each node is attached (e.g. its services, its availability).

Similarly to IEEE 802.11u [i.26], Wi-Fi direct provides a good framework that could facilitate the implementation of the CC-CRS and allow for a reuse of the existing procedures. One of the procedures which could be of particular relevance to the implementation of CC-CRS is the Group Owner Negotiation procedure which enables determination of the P2P Groups Owner as well as characteristics of the P2P Group. The procedure could be reused, for instance, to implement the ON Negotiation procedure. Another procedure which could be potentially reused is the P2P Invitation procedure which allows P2P Group members to invite not-associated devices to join an existing P2P Group (the invitation can be issued based on different reasons).

7.2.3 Bluetooth® based

The following clause describes possible implementation options for CC-CRS based on Bluetooth® technology. Bluetooth® is a short range wireless technology employed in most of the existing mobile devices currently available on the market. First, mechanisms that do not require connection between the devices are presented. They are based on the connection setup messaging. Then, possible mechanisms requiring a connection between the devices are presented. Such mechanisms may be based on Service Discovery Protocol (SDP), Attribute protocol (ATT), as well as a dedicated profile for CC-CRS purposes.

CC-CRS data may be conveyed without establishing an L2 connection between nodes by utilizing the Advertising Procedure and Scanning Procedure. They are Bluetooth® low energy protocol procedures for device discovery and for sharing small amounts of information connectionless. Following the Bluetooth® specification 4.0 [i.27], advertising procedure is used as a unidirectional broadcast transmission that reaches the scanning devices in the close neighbourhood and may be used to establish a connection with nearby devices, as well as to periodically broadcast arbitrary user data. Scanning procedure is used to listen to advertisements of nearby Bluetooth® devices, and also to connect to the advertising devices. For receiving the information sent in Advertisement packets, the scanning device only needs to listen to an advertising channel. In order to connect to an advertising device, the scanning device sends a Scan Request as a response to the received Advertisement packet. The advertising device responds to the Scan Request with a Scan Response. Although the Bluetooth® specification [i.27] states that the data carried by Scan Responses is "generally static in nature" it does not forbid the alteration of data carried by these packets. This basically indicates that the scanning procedure can also be used for the purpose of sending arbitrary user data. As can be seen in Figure 12, Bluetooth® specification [i.27] enables transmission of up to 31 octets of data in Advertisement and Scan Response packets. It should be noted that Advertisement and Scan Response packets are sent by the same device. Using only the Advertisement packets and passive scanning enables also uni-directional connectionless information sharing.

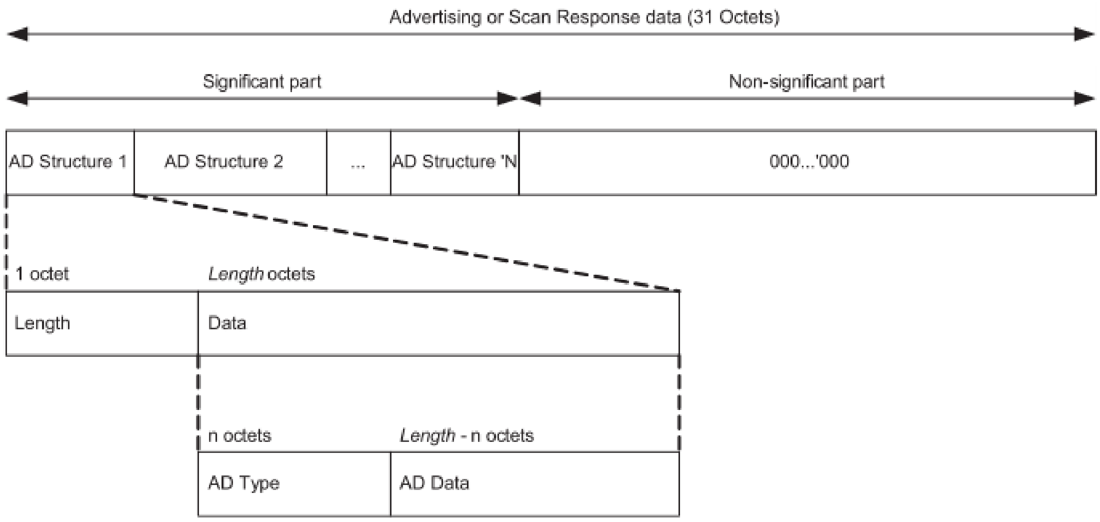

Figure 12 Advertisement and Scan Response data format [i.27]

An alternative approach suitable for transmission of CC-CRS specific data without establishing an L2 connection could be based on the usage of Extended Inquiry Response (EIR). The EIR is available for Bluetooth® basic/enhanced data rate protocols, and may be used in device discovery procedure to provide additional information. A Bluetooth® device that wishes to become discovered (being in "discoverable mode") should regularly perform inquiry scan and identify itself to the discovering devices, which send short Inquiry messages. The discoverable device responds to an Inquiry message with an Inquiry Response, which contains device's MAC identifier. As typically the MAC identifier is not enough to determine whether to connect to the device, additional information e.g. a local name and supported services needs to be shared. Traditionally a short connection was needed to exchange this information. The EIR procedure enables transmitting this information in an EIR packet which may be sent right after the Inquiry Response to the discovering device. Thus, the EIR procedure enables faster device filtering and discovery of the desired devices. The EIR packet may contain e.g.:

1) device local name;

2) UUIDs (Universal Unique Identifier) of services the device supports;

3) the transmission power; and

4) manufacturer specific values.

The EIR data format is presented in Figure 13. As can be seen, the EIR could potentially enable exchange of up to 240 B of arbitrary user data (e.g. CC-CRS specific data).

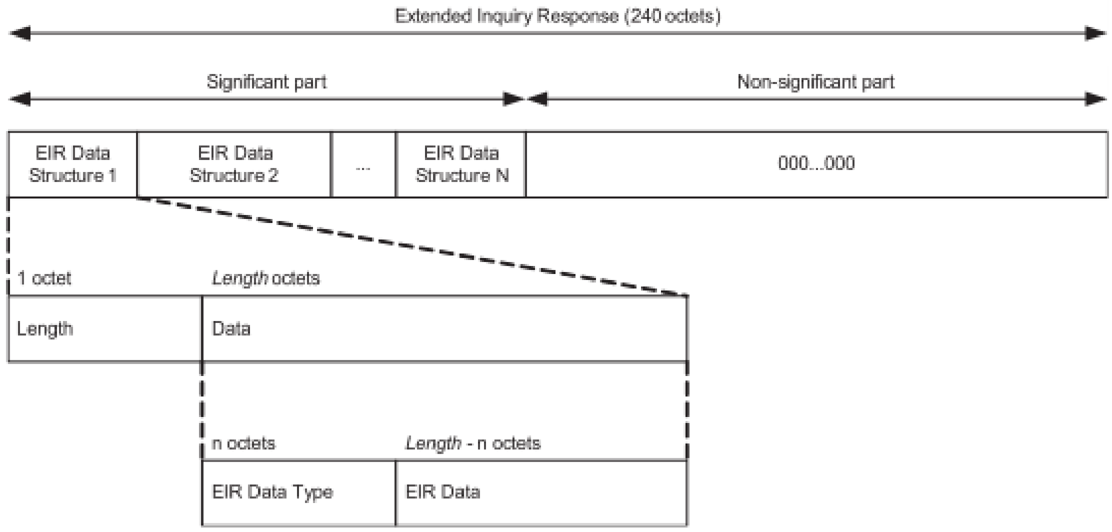

Figure 13: Extended Inquiry Response data frame [i.27]

Using the connectionless methods to transmit CC-CRS information enables transmitting quite limited amount of information at once. Also, due the lack of acknowledgements, there is no guarantee that the information is received by other devices. Connectionless methods are thus suitable for sharing small amounts of CC-CRS information locally and unreliably. In case, the CC-CRS information sharing requires transmission of larger amounts of information or reliable transmissions, the devices exchanging the CC-CRS information should form a connection to each other. However, this does not indicate very active and power consuming connection, because the link parameters may be setup in a way that sleep periods are long. The connected method may be utilizing the Service Discovery Protocol (SDP), the Attribute protocol (ATT), or a dedicated profile for CC-CRS.

The SDP provides mechanisms for applications running on one Bluetooth® device to discover which services are available on other Bluetooth® devices and to determine the characteristics of those services. A service is defined as an entity that can provide information, perform an action or control a resource on behalf of another entity [i.27]. Attributes of a given service are organized in Service Records. In order to enable exchange of CC-CRS specific data, a novel CC-CRS service would need to be added (which is allowed by specification) with attributes representing cognitive data (e.g. ON specific parameters, context information, policies).Devices supporting Service Discovery Application Profile (SDAP) would be able then to retrieve such data from neighbourhood entities. SDP implementation is mandatory in Bluetooth® basic/enhanced data rate devices hence should be considered as potential CC-CRS implementation option.

The ATT is a mandatory protocol for exchanging information between the Bluetooth® low energy devices. It is used for the service discovery, and it is also the basis for the Bluetooth® low energy profiles, most of which are targeted for exchanging small amounts of information regularly or on the need basis, e.g. sensor readings, incoming call notifications. Similarly, as for the SDP, the CC-CRS specific attributes should be defined to describe different CC-CRS data.

In addition to defining only the CC-CRS dedicated attributes, which are needed both in connectionless and connection-oriented methods, a CC-CRS dedicated profile may be defined. It enables defining the rules for the used connection modes, and thus may enable more efficient CC-CRS information exchange in different scenarios.

7.2.4 WiMedia UWB based

The following clause describes the CC-CRS implementation option based on the WiMedia technology. WiMedia is a short range ultra-wideband (UWB) wireless technology which provides high-speed connectivity (up to 480 Mbps) and offers relatively low energy consumption, compared to other short-range standards. Although WiMedia is currently used mostly for implementation of Wireless USB or for wireless audio-video data streaming, due to increasing interference in the ISM band and the need for larger bandwidth, it may be soon applied to much broader spectrum of applications.

The Distributed Medium Access Control (MAC) is one of the most important aspects of WiMedia. In general, WiMedia MAC is based on the concept of periodical beacon transmission in the reserved time slots. This allows WiMedia devices to exchange the necessary control information without collisions and decrease the energy consumption (devices may go to sleep after the beacon period, assuming no transmission is scheduled). An interesting feature of WiMedia MAC is that it supports transmission of arbitrary user data over beacon frames, using the Application-Specific Information Elements (ASIE) [i.28]. Depending on the number and size of additional IEs included in the beacon, the amount of potential user data (which can be essentially some CC-CRS data) that can be sent over a single beacon frame varies from 0 B to 320 B.

Although the realization of CC-CRS information exchange over WiMedia beacons is elegant (it does not require any standardization effort and prevents data loss caused by collisions), it may suffer from two main problems. The first problem is related to the possible low responsiveness to the changes of CC-CRS data (beacons are sent every 65 535 us) which may lead to unacceptable delay in some scenarios. The second problem is the available space for the CC-CRS data in ASIEs (320 B max), making it difficult or impossible to send all the necessary information over a single beacon frame. In order to address these issues, another WiMedia based implementation option could be employed. The alternative implementation option is based on the use of the Application Specific Command Frames (ASCF) [i.28]. As the size of the ASCF (4 095 B max) is significantly larger than the ASIE (320 B max.) more CC-CRS data can be transferred over a single frame. Moreover, ASCFs are transmitted during the data transfer period, meaning that the potential responsiveness to changes of CC-CRS data would be much better. Similarly to ASIE, ASCF has also some drawbacks. One of the most important is related to the additional overhead introduced by the Medium Access Slot (MAS) reservation procedure (the MAS reservation procedure assigns resources and is necessary to enable the exchange of information between devices). Moreover, the MAS reservation would require WiMedia devices to remain active during at least one MAS, hence increasing the overall energy consumption. It is also important to note that, in case small messages are transmitted, the combined L2 and L1 protocol overhead of this method may be large.

The proposed methods for the exchange of CC-CRS data between WiMedia terminals include the utilization of the Application-Specific Information Elements or Application-Specific Command Frames (ASIE format and ASCF payload format are presented in Figure 9 respectively). In order to enable their implementation, an additional management entity for interaction with DME needs to be introduced. The additional management entity would be responsible for creation and reception of the application specific data content. It is also worth noting here that a possible WiMedia based CC-CRS implementation could be a hybrid of the two methods, thus enabling much better flexibility.

octets: 1	1	2	N
Element ID (=255)	Length (=2+N)	Specifier ID	Application-specific Data

octets: 2	...
Specifier ID	Data

Figure 14: Application Specific Information Element format (top) and payload format for Application Specific Command frame (bottom) [i.28]

7.3 New Common Multi-RAT Control Layer Approaches

7.3.1 IEEE 802.19.1 TV White Space Coexistence Methods

IEEE 802.19 task group 1 [i.9] started work on defining standard for TV White Space Coexistence Methods in January 2010. The scope of the work is radio technology independent methods for coexistence among dissimilar or independently operated TV band networks and devices. The purpose of the standard is to enable the family of IEEE 802 Wireless Standards to most effectively use UHF TV WS, but the defined solutions may also be useful for non IEEE 802 network and devices.

The group has defined and agreed on system design document to assist in the standardization process. It includes draft system architecture and requirements for neighbour TV WS device discovery, coexistence decision making, as well as management commands and information sharing. The logical entities providing those services and their relations are described in Figure 15. The Coexistence Enabler (CE) interfaces the IEEE 802.19.1 [i.9] coexistence system with a TV WS device (TVWSD). It obtains information needed for the coexistence from the TVWSD, and provides control and information from the coexistence system to the TVWSD. The Coexistence Manager (CM) makes the coexistence decisions. It discovers and solves the coexistence conflicts of the TVWSDs operating in the same area. A CM serves one or more TVWSDs associated to the CEs. The TVWSDs, which potentially cause interference to each other, may be served by different CMs. The Coexistence Discovery and Information Server (CDIS) assists the CMs to discover the neighbour TVWSDs and facilitates opening interfaces between the CMs which serve those TVWSDs. Some of the system entities are implemented in the wireless device and some in the network. The functional split may depend on the deployment. The protocols for different interfaces for accessing and sharing management commands and information are still to be defined. Potential approaches are described below.

Interfaces B1-B3 are system internal interfaces. They are expected to be defined in details to enable interoperability between multivendor entities. All these interfaces are RAT independent. Possibly an existing solution may be used, but new messages may have to be defined:

- Interface B1: Over this interface the CM accesses TVWSD information from the CE, such as TVWSD's characteristics, operating parameters, and measurements results, and provides TVWSD configuration commands or information to the CE.
- Interface B2: Over this interface the CM registers a TVWSD to the CDIS, and receives a list of neighbour TVWSDs, and information on how to access their CMs.
- Interface B3: Over this interface the CMs exchange characteristics and resource use information of the neighbour TVWSDs.

Interfaces A, C and D connect the coexistence system to external entities:

- Interface A: Over this interface the coexistence system accesses TVWSD specific information and configures the TVWSD. This interface is implementation and RAT dependent. For providing the coexistence services the system should be able to interface different RATs which operate in UHF TV WS. Because RAT-specific messaging is beyond the scope of the 802.19.1 [i.9], the interface is expected to be defined only loosely in 802.19.1 [i.9].
- Interface C: Over this interface the coexistence system accesses information from TVWSD. The interface is RAT independent. Such interface is currently being defined in IETF PAWS.
- Interface D: Over this interface an operator may be able to configure the system in some specific deployments. This interface is out of scope of the 802.19.1 [i.9] standards and is currently not being defined elsewhere.

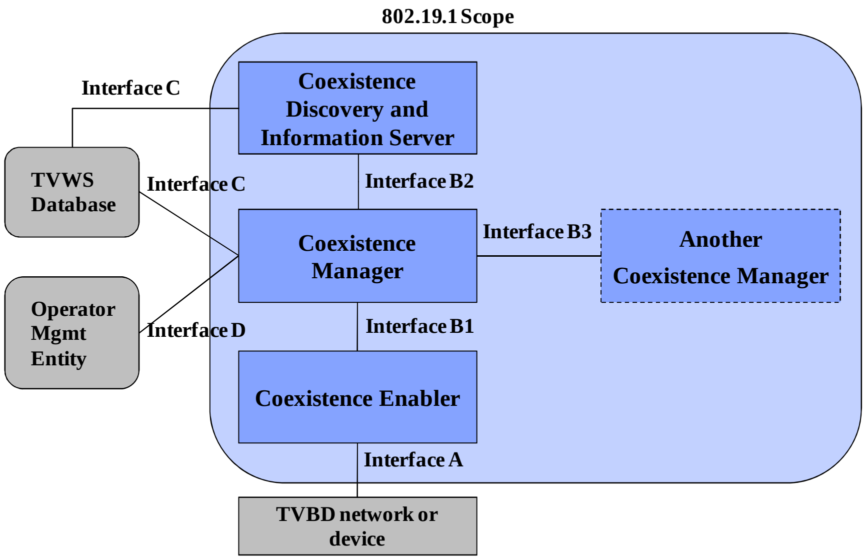

Figure 15: Coexistence system entities and their relations [i.9]

7.4 Overall assessment of implementation options

As specified earlier, Control Channels for Cognitive Radio Systems are responsible for conveying information between different entities involved in Cognitive Radio Systems (terminals, network elements) for the coexistence and coordination of different cognitive radio networks and nodes as well as for the management of Opportunistic Networks. In order to achieve that, Control Channels for Cognitive Radio Systems need to support exchange of information over three different interfaces, i.e. Terminal to Terminal (T2T), Terminal to Network element (T2N) and Network element to Network element (N2N). A network element is a node of a radio access network such as a Base Station in an operator network, an access point in WLAN, etc. T2N denotes a bidirectional interface to transmit data from Terminal to Network and/or from Network to Terminal. It may also be a node in coexistence or network management system, which manages for example the coexistence of heterogeneous networks, or connection handovers among different RANs.

The following clause highlights the advantages and disadvantages of the identified options and assesses their suitability for implementation of the above mentioned interfaces. Radio access independent based approaches are quite generic; however an important drawback is that there is need for pre-established connectivity.

It should be noted that in the following there is no reference to the IEEE 1900.4 [i.10] standard. The IEEE 1900.4 [i.10] standard has specified an architecture for the management of spectrum and radio resources in heterogeneous CR networks. Although no explicit transport mechanisms or protocols have been specified for the delivery of management information, elements of the defined information model could be exploited for the CC-CRS implementation. However, as an information model it is quite different from the other options addressed in clauses 7.1 to 7.3; therefore it is not further analysed here.

- The distributed agents based approach is an implementation option which could potentially enable a simple development and deployment of a Control Channel for Cognitive Radio Systems solution which supports T2T, T2N and N2N interfaces. As the inter-agent communication is based on the IP protocol, the approach requires however the IP connection to be setup before the exchange of information can be conducted. This significantly limits the usability of the approach, especially for the T2T and T2N interfaces, making it not suitable for implementation of Control Channels for Cognitive Radio Systems in scenarios where the basic IP connectivity is not always given.

- The 3GPP ANDSF option builds on top of the Mobile Device Management solution (OMA-DM) thus supporting the information exchange between a terminal and an infrastructure entity (T2N interface). The ANDSF based approach supports IP as well as SMS and WAP based information transport, enabling the provision of some limited amount of information without establishing an IP connection. Similarly to the distributed agents based approach, the ANDSF based approach may introduce a significant protocol overhead. Additionally, since the ANDSF is operator-controlled, it is typically used for distributing information related to the radio networks that are under the control of a single operator. This indicates that the approach may be of a limited usefulness in a multi-operator heterogeneous environment where operators have no roaming agreement (and thus the ANDSF is focussing to the needs of a single operator).

- The IETF Diameter protocol is designed in a way which allows it to be easily extensible. Although Diameter is designed to enable Peer-To-Peer architecture thus theoretically could be employed for realization of T2T, T2N and N2N interfaces, the mechanisms for dynamic peer discovery are based on DNS which is not suitable for terminal discovery. Similarly to the distributed agent based approach, the Diameter based implementation of Control Channel for Cognitive Radio Systems requires the IP connection to be setup before the information can be exchanged, limiting the usability of the solution to scenarios in which there is an active IP connection.

- The IETF PAWS supports T2N interface. This approach focuses on the interface of devices with white space databases and its use may be limited to discovering and accessing the geo-location database, and exchanging information with it. Also, it plans to exploit the existing protocols for information exchange. As such it could be exploited as a part of the CC-CRS but not as a standalone solution.

- IEEE 802.21 [i.29] provides a complete framework enabling the exchange of information in different scenarios. As the IEEE 802.21 [i.29] was driven by handover optimization, it is mainly designed for the information exchange between terminals and infrastructure entities as well as between infrastructure entities (T2N and N2N interfaces). IEEE 802.21 [i.29] supports L3 and higher transport mechanisms like IP based transport as well as L2 based transport mechanisms, enabling information exchange without setting up an IP connection. In contrast to the other radio access independent approaches, IEEE 802.21 [i.29] supports also dynamic peer discovery procedures which use other types of mechanisms than DNS. A potential drawback of the IEEE 802.21 [i.29] based solution is related to the fact that the IEEE 802.21 [i.29] standard is not used in practice.

- IEEE 802.19.1 [i.9] is defining a coexistence system for providing coexistence services between wireless standards of unlicensed devices. The system comprises entities in a wireless device, and in the backbone. Thus it supports T2N and N2N interfaces. For those interfaces IP-based solutions are considered. The coexistence system definition intends to define the solution for managing the coexistence for heterogeneous networks which may be operated independently or by different operators. Because the solution is not yet available, the applicability of it for various CC-CRS purposes remains to be seen.

- The network management based approach is dedicated for enabling information exchange between network entities (N2N interface). The main advantage of the approach, compared to Diameter and IEEE 802.21 [i.29], is the possibility of supporting CC-CRS in legacy systems. The realization of the CC-CRS using the network management protocols is related however with the additional load imposed on the network management systems (e.g. R, B interfaces in 3G/4G NMS), which may not be acceptable by some network operators.

Radio access dependent approaches are more likely to enable more efficient provision of information (in terms of overhead, latency); however they may require some additional standardization effort.

- The RRC based approach allows for time and resource efficient realization of the T2N interface for Control Channels for Cognitive Radio Systems. Due to the limited bandwidth dedicated for the C-Plane traffic in the 3GPP systems as well as the low priority of the CC-CRS traffic (compared to the 3GPP signalling traffic), the usage of this type of channel could be limited only to small amount of data. Additionally, the introduction of the approach requires changes in the standard, which needs to be discussed and agreed within 3GPP.

- The IEEE 802.11 Vendor Specific Information in MAC frames approach supports T2N and potentially T2T. However, it does not provide support for reliable data delivery, authentication and authorization necessary for data exchange. As already mentioned this approach would require an additional management entity to be implemented within devices. The new entity would be responsible for generation/reception of CC-CRS data and determining addresses of destination nodes. IEEE 802.11u [i.26] supports T2N. Similarly to the previous approach, this option would require an additional management entity to be implemented within devices.

- Direct Wi-Fi comprises various procedures that could be re-used mainly for T2T support and thus would not require any major extensions. However it does not provide support for T2N and N2N interfaces.

- The Bluetooth® based solution supports mainly T2T, providing for reliable and unreliable data delivery, transmission of information with a relatively low data rate (additional solution for enabling higher data rates for the T2T interface could be necessary to complement the Bluetooth® based solution). Bluetooth® does not provide support for T2N and N2N interfaces.

- The WiMedia based solution mainly supports T2T. It does not provide support for reliable data delivery. However, no extension of the existing standard would be required.

In general, the CC-CRS solutions based on Radio access dependent implementation options support realization of T2N and T2T interfaces. This basically means that, compared to some of the radio access independent solutions, the Radio access dependent solutions cannot be considered as standalone solutions (no support for N2N interface). An important advantage of the Radio access dependent solutions is however the possibility of implementing efficient discovery mechanisms and provision of information without the need of establishing a higher layer connection. This substantially reduces the overall overhead and enables fast provision of time critical information. A drawback with radio access dependent solution is that all the entities participating in CC-CRS should support at least the radio access technology which is used for CC-CRS.

Table 2 presents a summary of the information on the identified implementation options in terms of the types of supported interfaces, information delivery model, whether basic connectivity is required, the level of extension of baseline standards required and the underlying protocols. It should be noted that the criterion for whether extension of baseline standards is required is whether the existing specification of a certain option (i.e. the messages type and format, the relevant procedures) can be exploited as is for the Control Channels for Cognitive Radio Systems or whether the introduction of additional messages/structures or procedures is required. Furthermore, it should be underlined that this column refers only to the baseline standard even though further standards may be required e.g. to define the object/information models.

From the above analysis it seems that none of the proposed options is by itself suitable for enabling a full implementation of the CC-CRS. Therefore, it is expected that the final CC-CRS implementation will be based on a combination of different radio independent and radio dependent solutions. Such a combination would eliminate the identified shortcomings and allow full implementation of CC-CRS supporting exchange of information for T2T, T2N and N2N interfaces as well as enabling efficient exchange of time critical information. Also different solutions are targeted and optimized for a specific problem, and thus, multiple solutions may be needed even for same interfaces.

For instance, a possible solution could be based on a combination of 1) Bluetooth® or Direct Wi-Fi based CC-CRS for enabling the exchange of necessary information between terminals (T2T interface), 2) OMA-DM/ANDSF, 3GPP RRC based/database (e.g. IETF PAWS) or IEEE 802.21 based CC-CRS solution for enabling the realization of the interface between terminals and the infrastructure (T2N interface) and 3) Diameter based CC-CRS for realization of the N2N interface (e.g. to exchange information between entities belonging to different operators).

Table 2: Overall presentation of Control Channel implementation options

CC-CRS protocol option	Supported Interfaces	Information delivery model	Basic Connectivity Required	Extension of baseline standards required	Protocols	Addressing
Radio access independent						
3GPP ANDSF	T2N	Unicast	No	Minor	OMA-DM	IP or E.164
Distributed Agents	T2T, T2N, N2N	Unicast, Multicast	Yes	None	CORBA/IIOP	IP
IETF DIAMETER	T2N, N2N	Unicast	Yes	Minor	DIAMETER	IP
IETF PAWS	T2N	Unicast	Towards database	None	To be defined	To be defined
IEEE 802.21 [i.29]	T2N, N2N	Unicast, Multicast	No	Minor	MIH	IP, L2 and MIH identifier
TR069	N2N	Unicast	Yes	Minor	HTTP-SOAP	IP
Radio access dependent						
3GPP RRC based	T2N	Unicast, Broadcast	No	Minor	RRC	3GPP user equipment identifier
IEEE 802.11 [i.25]	T2T, T2N	Unicast, Broadcast	No	Minor	802.11	L2
IEEE 802.11u [i.26]	T2N	Unicast, Broadcast	No	None	802.11u	L2
Direct WiFi	T2T (mainly)	Unicast, Broadcast	No	Minor	802.11	L2
Bluetooth®	T2T (mainly)	Unicast, Broadcast	No	None	Bluetooth® 2.1 [i.38], 4.0 [i.27]	L2
WiMedia UWB	T2T (mainly)	Unicast, Broadcast	No	None	ECMA-368 [i.37]	L2
New Common Multi-RAT Control Layer Approaches						
IEEE 802.19.1	T2N, N2N	Unicast	Yes	None	To be defined	To be defined

8 Conclusion

For the efficient operation of Cognitive Radio Systems, mechanisms which allow the exchange and distribution of information as well the coordination between various management entities are essential. In this respect, Control Channels have been identified as a key feature required for Cognitive Radio Systems, as means for transmitting elements of information necessary to manage and realize various operations within a Cognitive Radio Systems. In this context, the present document addressed the following issues:

- Discovery and identification of neighbouring devices.
- Advanced Multi-RAT Assistance in Heterogeneous Networks.
- Retrieval of information on available White Spaces from a geo-location database.
- Management of operator-governed opportunistic networks in terms of creation, maintenance and termination.
- Implementation options for Control Channels for Cognitive Radio Systems, taking into account previous work on in-band-Cognitive Pilot Channel (CPC) and Cognitive Control Channel (CCC). The investigation of implementation options is a crucial step towards the realisation of the Control Channels and the deployment of Cognitive Radio Systems.

Various implementation options were investigated, including Diameter, ANDSF, IETF PAWS, Distributed Agents, 3GPP RRC, IEEE 802.21 [i.29] MIH, IEEE 802.11 [i.25], WiMedia UWB, Bluetooth® and IEEE 802.19.1 [i.9].

From the analysis of potential implementation options it was concluded that none of the proposed options is by itself suitable for enabling a full implementation of the Control Channels for Cognitive Radio System. Thus, it is anticipated that the final CC-CRS implementation will be based on a combination of different radio independent and radio dependent solutions. Such a combination would eliminate the identified shortcomings and allow full implementation of CC-CRS supporting exchange of information for T2T, T2N and N2N interfaces as well as enabling efficient exchange of time critical information. Also different solutions are targeted and optimized for a specific problem, and thus, multiple solutions may be needed even for same interfaces. For instance, a possible solution could be based on a combination of 1) Bluetooth® or Direct WiFi based CC-CRS for enabling the exchange of necessary information between terminals (T2T interface), 2) OMA-DM/ANDSF, 3GPP RRC based/database (e.g. IETF PAWS) or IEEE 802.21 [i.29] based CC-CRS solution for enabling the realization of the interface between terminals and the infrastructure (T2N interface) and 3) Diameter based CC-CRS for realization of the N2N interface (e.g. to exchange information between entities belonging to different operators).

History

Document history		
V1.1.1	April 2012	Publication