Protocols, performance assessment and consolidation on interfaces for standardization – D3.3

Project Number:	ICT-2009-257385
Project Title:	Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future Internet - OneFIT
Document Type:	Deliverable

Contractual Date of Delivery:	30.06.2012
Actual Date of Delivery:	30.06.2012
Editors:	Tomasz Wierzbowski
Participants:	See contributor's list
Workpackage:	WP3
Nature:	PU[1]
Version:	1.0
Total Number of Pages:	128
File:	OneFIT_D3.3_20120630_FINAL.doc

Abstract

This deliverable presents the final, detailed description of the "Control Channels for the Cooperation of the Cognitive Management System" (C4MS) protocol which is designed to enable the management of operator governed Opportunistic Networks and provide the evaluation signalling related to the operation and management of Opportunistic Networks (ONs). The deliverable elaborates on the signalling evaluation methodology and evaluation plan as well as on the performance results themselves. The deliverable is extended by an appendix provided as a separate document.

Keywords List

Control Channels for Coordination of Cognitive Management Systems, C4MS, Opportunistic network, Protocol, Messages , Information management, Data structure, Protocol state machine

[1] Dissemination level codes: **PU** = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

Executive Summary

The following document presents a detailed description of the protocol for the "Control Channels for the Cooperation of the Cognitive Management System" (C4MS) which provides the necessary means to enable proper management of Opportunistic Networks. Additionally, the document defines the methodology that was applied for the purpose of signalling evaluation.

The protocol overview presented in section 2 of the main document, provides the C4MS principles. The section includes, among others, the description of the protocol identifiers, procedures, protocol state machines and message format as well as the security aspects.

Section 3 provides a high-level description of the data structures defined within the scope of OneFIT project. The data structures are classified into five categories, i.e.: Profiles, Context, Decisions, Knowledge and Policies. The high level description is complemented by some detailed data structures in the Appendix to D3.3 Section 3 [10].

Section 4 provides details on the evaluation methodology applied for the purpose of C4MS performance assessment. The section presents the evaluation plan along with a description of metrics that are to be exploited in the scope of WP3.

Section 5 and Section 6 are composed of the signalling evaluation results. Section 5 focuses on the estimation of the signalling load imposed by ON management in different ON phases. Additionally some results for the initialization phase (not explicitly mentioned in the previous phases of the project) and security related aspects are also depicted. Section 6 on the other hand is focused on the evaluation of the signalling traffic generated by different ON related algorithms.

Conclusions to the document are drawn in section 7.

Detailed description of the C4MS procedures, implementation options based on IEEE 802.21, DIAMTER and 3GPP are depicted in the appendix to the D3.3 [10]. Additionally, the appendix incorporates the detailed definition of the information data structures and final set of Message Sequence Charts (MSCs) provided for the OneFIT project.

Contributors

First Name	Last Name	Affiliation	Email
Marcin	Filo	EIT+	marcin.filo@eitplus.pl
Tomasz	Wierzbowski	EIT+	tomasz.wierzbowski@eitplus.pl
Jens	Gebert	ALUD	Jens.Gebert@alcatel-lucent.com
Andreas	Wich	ALUD	Andreas.Wich@alcatel-lucent.com
Caroline	Jactat	NTUK	caroline.jactat@nectech.fr
Benoit	Lécroart	NTUK	benoit.lecroart@nectech.fr
Christian	Mouton	NTUK	christian.mouton@nectech.fr
Haeyoung	Lee	UNIS	Haeyoung.lee@surrey.ac.uk
Seiamak	Vahid	UNIS	s.vahid@surrey.ac.uk
Faouzi	Bouali	UPC	faouzi.bouali@tsc.upc.edu
Ramon	Ferrús	UPC	ferrus@tsc.upc.edu
Jordi	Pérez-Romero	UPC	jorperez@tsc.upc.edu
Oriol	Sallent	UPC	sallent@tsc.upc.edu
Panagiotis	Demestichas	UPRC	pdemest@unipi.gr
Andreas	Georgakopoulos	UPRC	andgeorg@unipi.gr
Dimitrios	Karvounas	UPRC	dkarvoyn@unipi.gr
Nikos	Koutsouris	UPRC	nkouts@unipi.gr
Vera	Stavroulaki	UPRC	veras@unipi.gr
Kostas	Tsagkaris	UPRC	ktsagk@unipi.gr
Marja	Matinmikko	VTT	Marja.matinmikko@vtt.fi
Heli	Sarvanko	VTT	heli.sarvanko@vtt.fi

Table of Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AP	Access Point
BS	Base Station
BSS	Basic Service Set
C4MS	Control Channels for the Cooperation of the Cognitive Management System
CCC	Common Control Channel
CCR	Cognitive Controlled Radio
CID	Connection Identifier
CMON	Cognitive systems for Managing the Opportunistic Network
CPC	Cognitive Pilot Channel
CSCI	Cognitive management Systems for Coordinating the Infrastructure
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DL	Downlink
DL-MAP	Downlink Medium Access Protocol
FID	Flow Identifier
FQDN	Fully Qualified Domain Name
HARQ	Hybrid Automatic Request
HIP	Host Identity Protocol
IBSS	Independet Basic Service Set
IEEE	Institute of Electronical and Electronics Engineers
IMSI	International Mobile Subscriber Number
INA	Information Answer
INI	Information Indication
INR	Information Request
LTE	Long Term Evolution
MAP	Medium Access Protocol
NAI	Network Acess Identifier
ONCA	ON Creation Answer
ONCR	ON Creation Request
OneFIT	Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future InterneT
ONMA	ON Modification Answer

ONMR	ON Modification Request
ONNA	ON Negotiation Answer
ONNR	ON Negotiation Request
ONRA	ON Release Answer
ONRR	ON Release Request
ONSI	ON Suitability Indication
ONSN	ON Status Notification
PU	Primary User
RAT	Radio Access Technology
RF	Radio Frequency
SINR	Signal to Interference and Noise Ratio
SSID	Service Set Identification
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
MIH	Media Independent Handover
SLF	Subscriber Location Function
NAF	Network Application Function
BSF	Bootstraping server Function
HSS	Home Subscriber System

Table of Contents

List of Figures

List of Tables

1. Introduction

An Opportunistic Network (ON) should be capable to operate dynamically as a part of an infrastructure without interfering with other traffic and operation in the infrastructure. In addition, it should be able to extend the resources and capabilities of the infastructure by utilizing excisting resources in the network as efficiently as possible. For these reasons, nodes have to be able to exchange between each other information related to policies, node capabilities, environment etc.. In order to distribute this information and avoid excessive signaling, efficient information provisioning procedures provided by the C4MS (Cognitive Control Channels for Cognitive Management) are introduced.

As mentioned in [2], C4MS integrates and extends three concepts, namely: Cognitive Pilot Channel (CPC) [23], Cognitive Control Radio (CCR) [29] and Cognitive Control Channel (CCC) [29]. The CPC, CCR and CCC are intended for supporting terminals in their start-up phase, supporting spectrum scanning and spectrum sensing procedures, provisioning some context information from the infrastructure, as well as for enabling the coexistence and coordination between networks and devices. C4MS integrates these concepts by supporting all of the above mentioned functionalities and enables information provision between heterogeneous network nodes (terminals or infrastructure nodes) as well as between terminals and infrastructure (see Figure 1). In addition, C4MS extends the CPC, CCR and CCC concepts by introducing new procedures, thus enabling new features related to Opportunistic Network management. The following document intends to further elaborate on the C4MS concept and provides the necessary basis for implementation of the complete solution within in the scope of the WP5.

A number of C4MS implementation options, subdivided as RAT/System independent and RAT/System dependent, were identified in the scope of the OneFIT project. The analysis provided in [2] and [28] highlighted different advantages and drawbacks of these approaches and indicated the need of building on a combination of several options. In this document, we provide a detailed description of C4MS protocol and a detailed description of a subset of C4MS implementation options which are reckoned to be the most appropriate are presented in the Appendix to the D3.3 [10].

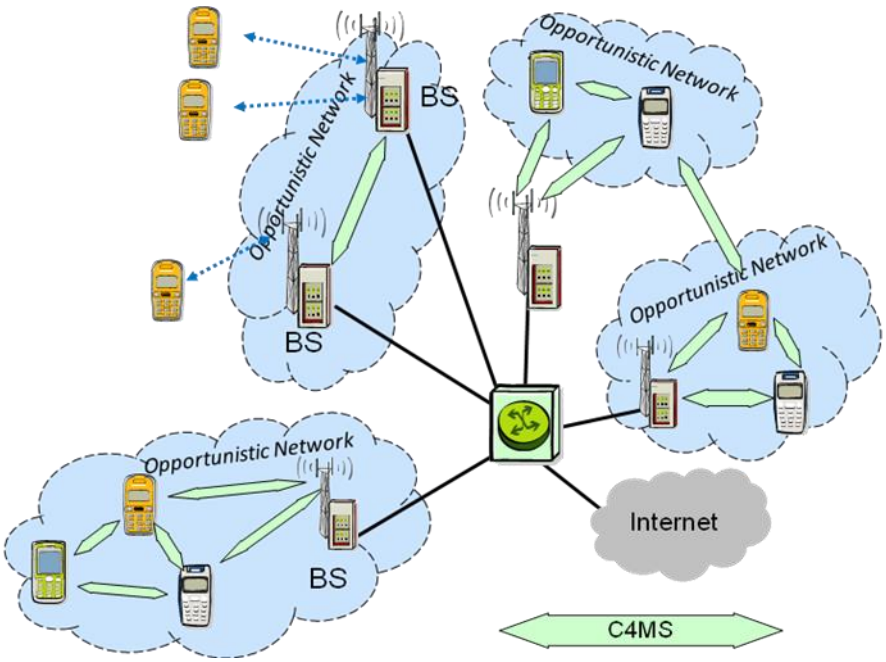

Figure 1: C4MS – general view.

The structure and encoding of information carried by messages is an integral part of a protocol specification. In this document, the high level structure of information to be exchanged between cognitive management systems for management of ONs is examined, and in-depth descritption of data structues and aspects related to the management of information in OneFIT system are given in [10]. The C4MS information considered for encoding and structuring is based on the set of information identified in [3], required by the algorithms described in [4]. Similarly to [3] the considered information is divided into policy information, context information, decisions, profiles and knowledge. Determination of encoding for information carried by the C4MS messages as well as possible information management strategies enables to estimate the control traffic overhead generated by the ON management algorithms, developed within the scope of WP4. Additionally, this will be used to determine the theoretical upper bound of the bandwidth requirements related to the ON management, when realized by C4MS. The outcome of this work will be further used as an input for additional C4MS protocol evaluation, which is to be carried out in the last step of the OneFIT project.

The rest of the document is organized as follows. Section 2 provides a detailed description of the C4MS protocol and is based on the initial contributions provided in [3] and [4]. The section incorporates the protocol overview, message format and identifiers definition, describes the procedures, state machines designed for the OneFIT project. The section ends with a description of security related aspects. Section 3 provides a high level description of the data structures dedicated to the OneFIT system. Structures are categorized into 1) profiles, capabilities and requirements, 2) context, 3) knowledge, 4) decisions and 5) policies). Please refer to the Appendix to D3.3 (Section 3) [10], where the detailed definitions of data structures of the information to be exchanged in the OneFIT system are provided. Section 4 introduces the evaluation methodology proposed for the protocols performance evaluation. Assumptions made in section 4 are enforced in subsequent sections: 5 and 6. Section 5 is dedicated to the general, analytical ON performance evaluation. Opportunistic Network phases (i.e. Suitability Determination, Creation, Maintenance and Termination) are independently analyzed with additional focus on the initialization phase. Security considerations for the OneFIT system are also depicted. Section 6 on the other hand analyzes the performance of the ON-related algorithms and their impact on the overall ON signalling. Finally, conclusions are drawn in Section 7 and references are shown in section 8.

2. C4MS protocol

The following section provides a detail description of the C4MS protocol and is organized as follows. After the C4MS protocol overview presented in Section 2.1, Section 2.2 discusses different C4MS protocol identifiers. Section 2.3 presents a detailed description of C4MS message header, parameter encoding and message structure and format. Section 2.4 gives a description of security aspects related to the C4MS protocol operation.

2.1 C4MS protocol overview

As already stated in the introduction, C4MS provides a common framework enabling integration of CPC, CCR and CCC concepts, thus allowing exchange of variety of information (ON operation related, coexistence information, node capabilities etc.) between nodes residing on the terminal side as well as on the infrastructure side. In order to enable that, C4MS defines a basic set of common services, procedures (operations) and messages (see Section 2.2).

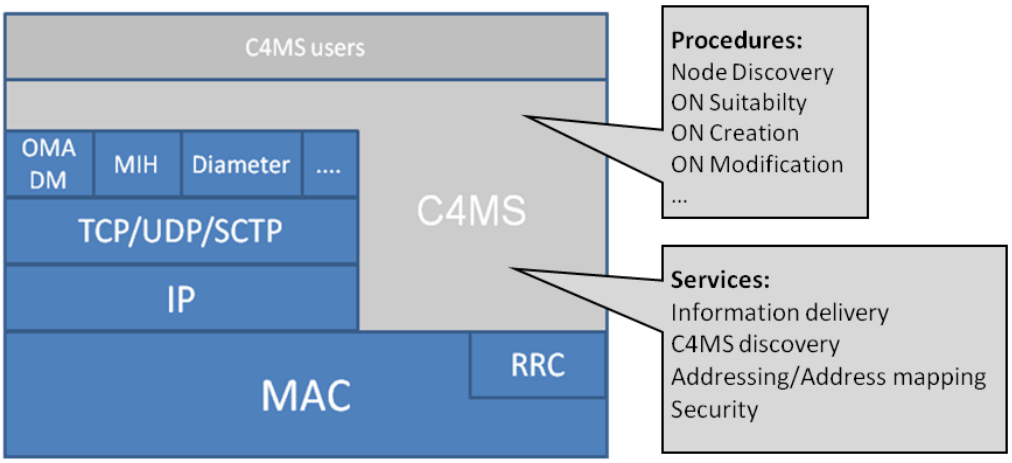

Figure 2: C4MS framework – general view

In general, the C4MS can be seen as an intermediate layer between C4MS users and the network protocol stack (see Figure 5) whose main role is to enable and coordinate the exchange of information between C4MS users located in different nodes. It is worth to underline here that C4MS is not limited to any type of access network and may be adapted to wireless as well as wired domains.

More specifically, the C4MS can be classified as a transaction-based, connectionless protocol. It defines message formats (including a message header and message parameters) and is envisioned to provide sufficient flexibility to enable C4MS information to be transported over different transport mechanisms (e.g. 3GPP RRC, OMA DM, IEEE MIH protocol) and over different layers (L2, L3 and above). The C4MS messages, for example, can be transported over IP in order to be radio access technology independent or directly over MAC or RRC messages in order to enable efficient discovery and communication before an IP connection is established (see [2] and [28]). Although C4MS data can be routed between networks (e.g. in case C4MS is transported over IP), C4MS itself is not a routable protocol[2].

A functional entity defined as C4MS user exploits the services provided by the C4MS in order to exchange information with remote C4MS users. The two main users considered for the C4MS are CMON and CSCI. Other functional entities however (e.g. JRRM) can also make use of the C4MS. In order to enable a proper operation of the protocol, C4MS users shall be capable of:

[2] It needs to be noted however, that C4MS related data may provide additional information for routing protocols.

- Determination and indication to the lower layers of the transportation mechanism to be used (e.g. RRC, MIH, DIAMETER),
- Establishment and maintenance of multicast groups, thus enabling reachability of multiple destinations (e.g. ON participants) with a single transmission

In order to enable the exchange of information between different C4MS users, four basic services have been identified as necessary:

Information delivery: encompasses mechanisms for the information exchange between C4MS users. It supports information pull and push modes (requests/response and notification). It allows different types of information to be exchanged (e.g. ON management related data, coexistence related data). It allows for the delivery of information in a unicast, multicast and broadcast manner.

C4MS discovery: provides mechanisms for discovering other C4MS users (on the terminal and network side) in case the necessary information is not provided by the lower layers (e.g. no extra information enabling discovery is transmitted over beacons).

Addressing/Address mapping: enables the determination of the correct underlying layer address of the remote C4MS user (e.g. IP address and port number). This mechanism is necessary as different transport mechanism can be employed for the transmission of C4MS data. The mechanism also maintains a list that links C4MS specific IDs and corresponding lower layer addresses of remote C4MS users (along with their underlying layer addresses).

Security: provides means for establishing a secure connection between C4MS users belonging to the same ON. It supports mechanisms for encrypting and authenticating the exchanged messages as well as establishing a mutual authentication along with cryptographic key negotiation between C4MS users.

Depending on the underlying transport mechanism, services related to acknowledgements, flow control, congestion control and message fragmentation/reassembly may also be required (e.g. in case available transport protocols are not able to provide them). These services are however not covered in this document.

As mentioned, the C4MS protocol is designed to be RAT agnostic and applicable to various existing standards, thus possible C4MS implementation options based on the IEEE 802.21 standard, RRC and DIAMETER protocols are presented in the Appendixes to D3.3, Sections: 2.1, 2.2 and 2.3 respectively.

TheC4MS messages consist of a message header and parameters. Each message may have mandatory parameters (“required”) and optional parameters.

The Messages are specified in this document using the ABNF specification. For more details on the ABNF specification, see IETF RFC 3588 [12], Section 3.2. As a short summary, the following syntax is used to define fixed, required and optional parameters (the parameters are called Attribute-Value-Pairs (AVPs) as in [12]):

```
message = header  [ *fixed] [ *required] [ *optional][ *fixed]

fixed       = [qual] "<" avp-spec ">"
              ; Defines the fixed position of an AVP

required    = [qual] "{" avp-spec "}"
              ; The AVP MUST be present and can appear
              ; anywhere in the message (mandatory parameter)
```

```
optional    = [qual] "[" avp-name "]"
              ; The avp-name in the 'optional' rule cannot
              ; evaluate to any AVP Name which is included
              ; in a fixed or required rule.  The AVP can
              ; appear anywhere in the message.

qual        = [min] "*" [max]
              ; See ABNF conventions, RFC 2234 Section 6.6.
              ; The absence of any qualifiers depends on whether
              ; it precedes a fixed, required, or optional rule.
              ; If a fixed or required rule has no qualifier,
              ; then exactly one such AVP MUST be present.
              ; If an optional rule has no qualifier,
              ; then 0 or 1 such AVP may be present.
              ;
              ; NOTE:  "[" and "]" have a different meaning than in ABNF
              ; (see the optional rule, above).
              ; These braces cannot be used to express optional fixed
              ; rules (such as an optional ICV at the end).
              ; To do this, the convention is '0*1fixed'.
```

2.2 C4MS message format

A C4MS message consists of a header and parameters.

2.2.1 Header format

The C4MS header can have a structure as shown below. Please note that this header structure is similar to those used in IEEE 802.21 [18]. The Diameter protocol [12] header has similar fields, but in a different order and of different sizes.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Flags |   Reserved    | MessageID (= MsgType + Opcode)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Transaction ID        |    Variable Payload Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: Example of C4MS Message header format

The following table describes fields that are used in C4MS protocol header with indication of their sizes and a brief description. In some situation, a set of possible values were also identified.

Field name	Size (bits)	Description
Version	4	This field is used to specify the version of C4MS protocol used. 0: Not to be used 1: First version 2–15: (Reserved) The version number will be incremented only when a fundamental incompatibility exists between a new revision and the prior edition of

		the standard. A C4MS capable node that receives a C4MS message with a higher version number than it supports will discard the frame without indication to the sending C4MS node.
Flags	4	This field is reserved for future usage.
Reserved	8	This bits are reserved for future use and when not used must be set to value '0'
Message Id	16	The Message Id consists of a Message Type (14 bit) and an OpCode (2bit) as described in detail in section 2.2.3
Transaction ID	16	The field is used for matching request and response type of messages. For more details regarding transactions in C4MS protocol please refer to section 2.2.4
Variable Payload Length	N	Indicates the total length of the variable payload embedded in this C4MS protocol frame. The length of the C4MS protocol header is not included.

Table 1: Description of C4MS protocol header fields

2.2.2 Parameter Format

The parameters in C4MS message are "Type-Length-Value" (TLV) encoded as shown below:

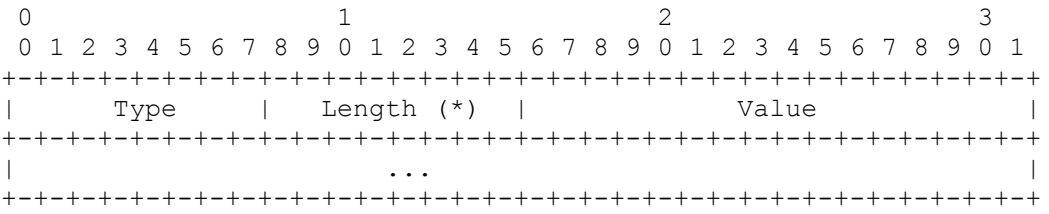

Figure 4: Example of a C4MS Parameter Format

The following table describes fields that are used in C4MS TLVs with an indication of the fields' sizes and a brief description[3].

Field name	Size (bits)	Description
Type	8	Type of the parameter
Length	variable	Length of the value field of this parameter (i.e. length without header)
Value	N	The actual value of the parameter

Table 2: Description of TLV encoding fields

2.2.3 MessageID

As shown in Figure 5, the MessageID consists of a MessageType and an Opcode (Op).

The OpCode can have the following values:

- request – OpCode value equals 1;
- response – OpCode value equals 2;
- indication – OpCode value equals 3.

[3] For more information regarding the Type-Length-Values encoding please refer to [18], section 8.5.

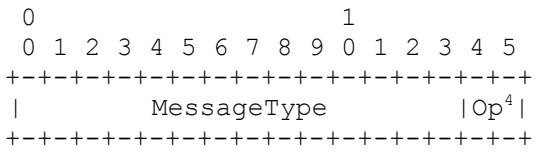

Figure 5: Structure of the MessageID

The following MessageIDs are defined:

Message name	Message Type + Opcode (binary)	MessageID (decimal)
Information Request (INR)	00000000000001 + 01	5
Information Answer (INA)	00000000000001 + 10	6
Information Indication (INA)	00000000000001 + 11	7
ON Suitability Indication (ONSI)	00000000000010 + 11	11
ON Negotiation Request (ONNR)	00000000000100 + 01	17
ON Negotiation Answer (ONNA)	00000000000100 + 10	18
ON Creation Request (ONCR)	00000000000101 + 01	21
ON Creation Answer (ONCA)	00000000000101 + 10	22
ON Modification Request (ONMR)	00000000000110 + 01	25
ON Modification Answer (ONMA)	00000000000110 + 10	26
ON Release Request (ONNR)	00000000000111 + 01	29
ON Release Answer (ONRA)	00000000000111 + 10	30
ON Status Notification Ind. (ONSN)	00000000001000 + 11	35

Table 3: C4MS MessageIDs

Please note that request/response messages shall be used whenever information is required to be exchanged between a pair of nodes (single request is followed by a single response). Indication messages are used in case a message needs to be addressed to more than one recipient or in case a response is not required. It is worth to underline here that the Indication type maybe used to realize a communication model in which a single request is followed by multiple responses (e.g. ON negotiation procedure).

It needs to be noted, that the values assigned to Message ID and OpCodes are presented for reference only and such encoding may not be strictly followed in the validation activities.

2.2.4 Transaction ID

In order to match requests with responses, the protocol header has a Transaction ID (TID) field.

The TID shall be generated by the node initiating a request. A response shall have the same TID as the corresponding request. An indication message may have the TID set to 0 or to a random number or – in case the indication provides further information related to a previous transaction, reuse the corresponding TID.

The following message sequence chart provide a brief example of the TID generation and handling.

[4] Op is used as an abbreviation of Operation code (Opcode)

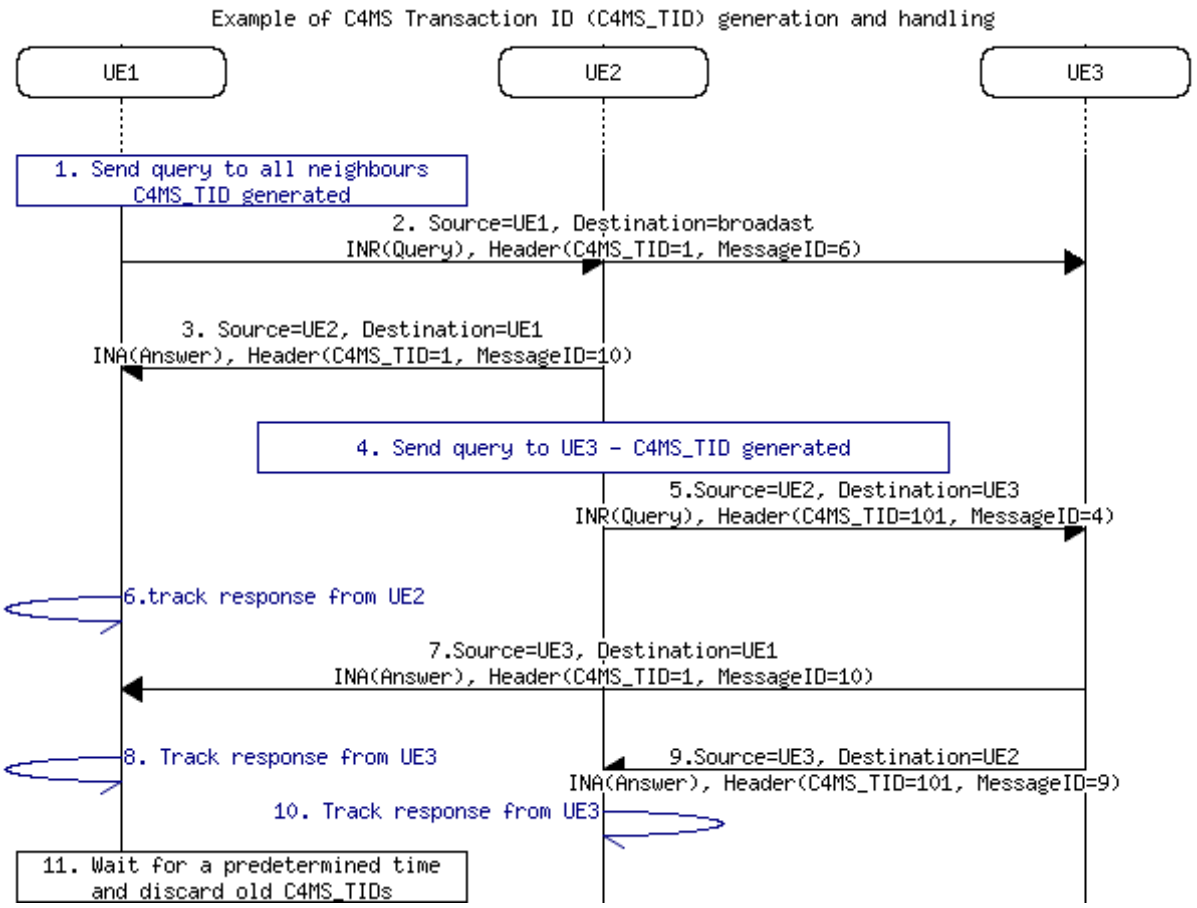

Figure 6: C4MS messages exchange with CTID values

2.3 C4MS ID (C4MS_ID)

In addition to identifiers used in the message header (i.e. MessageID, TransactionID), the C4MS protocol may use an additional node-identifier: the C4MS-ID.

The C4MS ID is thought to be a RAT agnostic network identifier which uniquely identifies a node. Dependent on the selected C4MS implementation option, the C4MS ID may be based on concepts as proposed below[5]:

- Host Identity as defined in Host Identity Protocol [X.2]
- Home Address (in case of Mobile IP usage)
- IEEE 802.21 Media Independent Handover ID (MIHF_ID)
- NAI as specified in IETF RFC 4282
- Hostname, including FQDN (Fully Qualified Domain Name)
- IMSI (International Mobile Subscriber Number)

The concept of the C4MS_ID is presented in the Figure 7, where the node identity is used as a communication endpoint and translates into one or more IP addresses. In this case, a node that is communicating using more than one network interface (using more than one IP address) would be discoverable by a single identity. This enables to separate host's identity from its present topological

[5] It needs to be underlined here that OneFIT does not intend to develop any new addressing scheme; instead we decided to combine or reuse existing addressing schemes for the purpose of the C4MS ID.

location in the Internet (and implicitly its current IP, or other local address), thus maintaining service provisioning despite user mobility [32]. Additionally by providing a unique naming scheme in the Opportunistic Networks environment, a node's behaviour may be linked to a given ID and taken into consideration in future operation, as well as may be used as an input to learning algorithms.

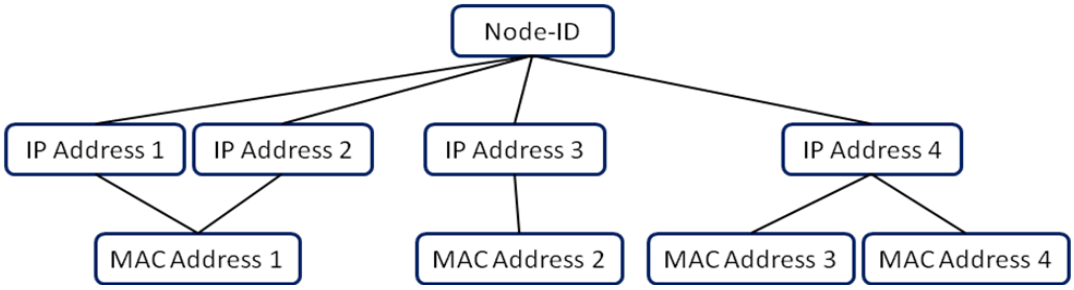

Figure 7: Separating location and identity of Internet hosts.

Whichever approach is chosen from the predefined, non-exhaustive list, the solution shall focus on preserving several key issues that facilitate the Opportunistic Network operation:

- C4MS_ID may applied to a mobile terminal or an infrastructure node and identify a source or a destination of a message. Additionally, C4MS_ID may be used as a identity/address that corresponds to a broadcast or a multicast address.
- As a devices may be equipped with multiple radio interfaces, proper mechanisms for address resolution are required (C4MS_ID of a remote node may need to be translated to a corresponding address of the underlying layers (e.g. MAC or RNTI), please refer to Figure 8 depicting a possible approach for C4MS addressing and address mapping[6].
- The envisaged solution should be also scalable and empower a persistent transport-layer connectivity (e.g. in case the underlying IP address is modified, a node is identified by the same, static C4MS_ID).
- The solution shall also consider global roaming and thus may not be bounded to a limited geographical area.

[6] Our approach would require an address resolution service which enables resolution between: link layer (e.g. MAC address), network layer (e.g. IP address) and upper layers addresses (e.g. C4MS_IDs).

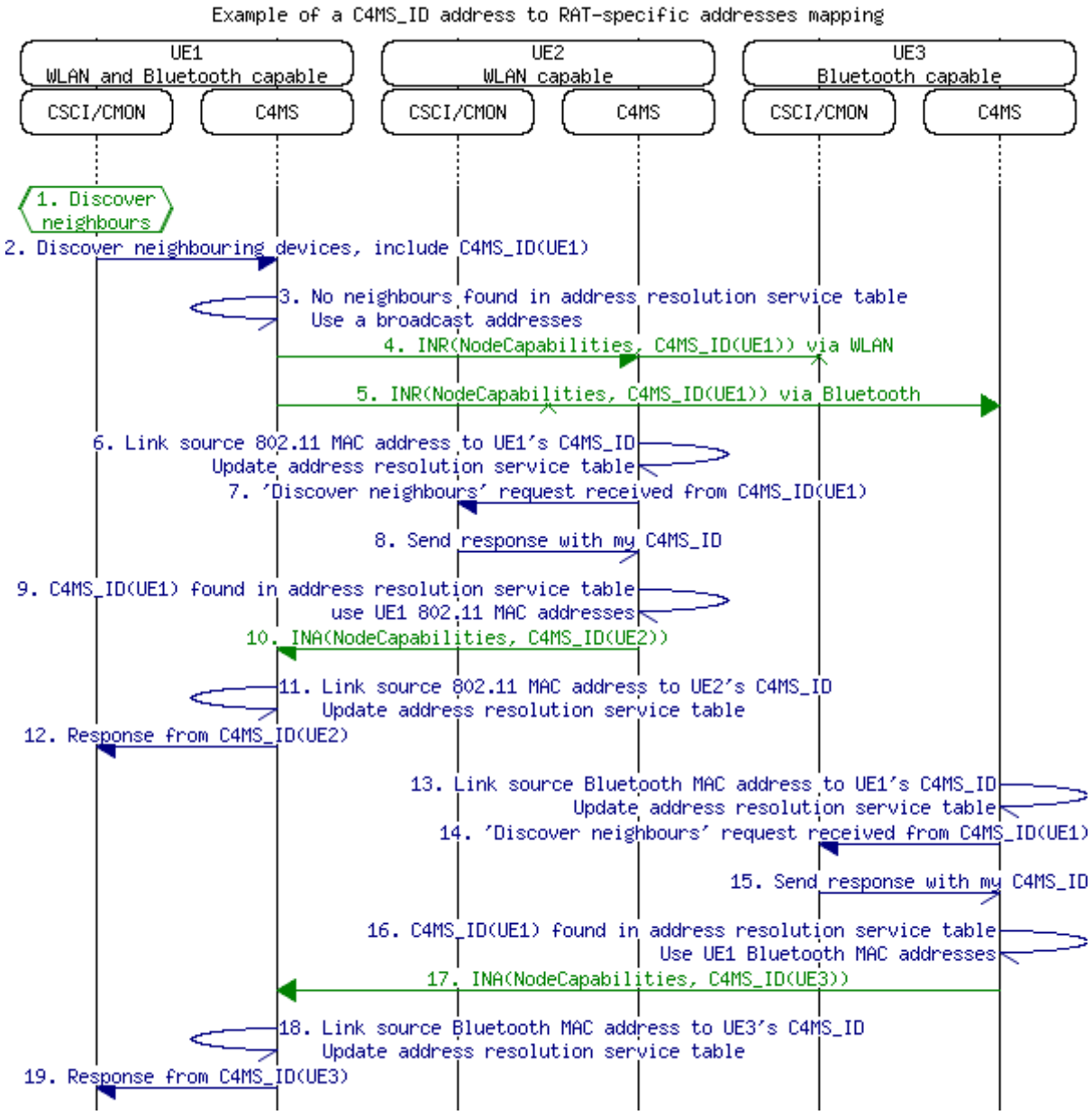

Figure 8: C4MS ID to RAT-specific address mapping

The message sequence chart presented in Figure 8 is designated to improve the readability of the C4MS concept and considers a situation as follows. In a given location three users are deployed. Each support opportunistic networking. UE1 is equipped with both WLAN and Bluetooth interface; UE2 and U3 are equipped with WLAN and Bluetooth respectively. Due to some condition, UE1 decides that ON creation would be beneficial and decides to discover any adjacent nodes via its short range radio interfaces.

The message sequence chart consists of the following steps:

1. At start UE1 does not know its neighbours and decides to scan its surroundings using all available short range radio interfaces.
2. Request to scan is send to C4MS layer.
3. As the C4MS does not know any neighbour it will use broadcast addressed for distribution of the request.

4. Information Request (INR) is send via the WLAN interface. The C4MS message conveys the UE1's C4MS_ID, the Ethernet (WLAN) header has the UE1's IP and MAC addresses of the WLAN interface.
5. INR is also send with the Bluetooth interface and as before the C4MS message conveys the UE1's C4MS_ID, the UE1's Bluetooth Device Address (BD_ADDR) is in the Bluetooth header message.
6. After message reception, the C4MS layer updates the address resolution service's table and links the UE1's source MAC address (and potentially also the IP address) to the UE1's C4MS ID. Based on that action, UE2's C4MS layer will be able to determine on which interfaces UE1 (denoted by the C4MS_ID of UE1) may be reached.
7. The message containing the 'discover request' is transported to CSCI/CMON. With such operation, CSCI/CMON does not need to decide which interface shall be used to reach UE1, it just indicates that a message to a given C4MS_ID shall be delivered and the C4MS layer is responsible for choosing the most appropriate technology and addresses in given time and under current communication conditions.
8. The CSCI/CMON decides to respond to the INR by sending an INA to UE1's C4MS_ID.
9. C4MS layer is able to locate the C4MS_ID of UE1 is in its address resolution service's table, and assigns the current WLAN MAC address.
10. The response is send via the WLAN interface and is addressed to UE1.
11. The INA from UE2 is received and UE1's address resolution service's table is updated (the INR message conveys UE2's C4MS_ID in C4MS header, and UE2's MAC address in Ethernet (WLAN) header).
12. The notification of the response - with only the C4MS_ID of UE2 send to CSCI/CMON.

13-19: Analogical step to those presented in steps 6 – 12 are repeated; the only difference is that the messages are transported with the use of Bluetooth radio interface.

Based on the properties of the Host Identity Protocol [14] and the fact that the operation of Opportunistic Networks is envisaged in an untrusted/public environment, a robust mechanism needs to be applied for providing secure host identification among untrustworthy users. It also needs to be noted that although mutual user identification is inevitable for providing services among communicating parties, the actual user identity needs to be protected and a reasonable level of anonymity shall be empowered (e.g. in case of traffic forwarding the relaying node shall be given enough information to be assured that some incentives/kick-back would be given, however persistent node identity knowledge may not be required).

It shall be also stressed that that the validation platforms which are being developed in the scope of WP5 enforces some modification on the proposal of the C4MS_ID (and the protocol itself) presented in WP3. Thus, the C4MS_ID or identification of nodes supporting ONs in the validation platform is based on different assumptions/mechanisms compared to the WP3's version as the implementation/validation intents to show some possibilities that the ONs provide and does not intent to implement the whole working system.

2.4 C4MS Timers

Communication between peer nodes in opportunistic network relies on request and response type of messages enabling parameter selection, negotiation and decision taking. The time between transmitting a request and receiving an answer message depends on the wireless, unreliable in

nature environment and underlying radio access technology. Following timers provide method for an efficient C4MS data exchange:

- RetransmissionIntervalTimer, indicating the interval between consecutive message retransmission in case an acknowledgment or response has not been received.
- TransactionTimer, indicating the duration in milliseconds of a given transaction, if the timer expires and no response/acknowledgment is received, the transaction is marked as finished and no further retransmission are required.

The following message sequence chart provides an example of C4MS message handling based on timers.

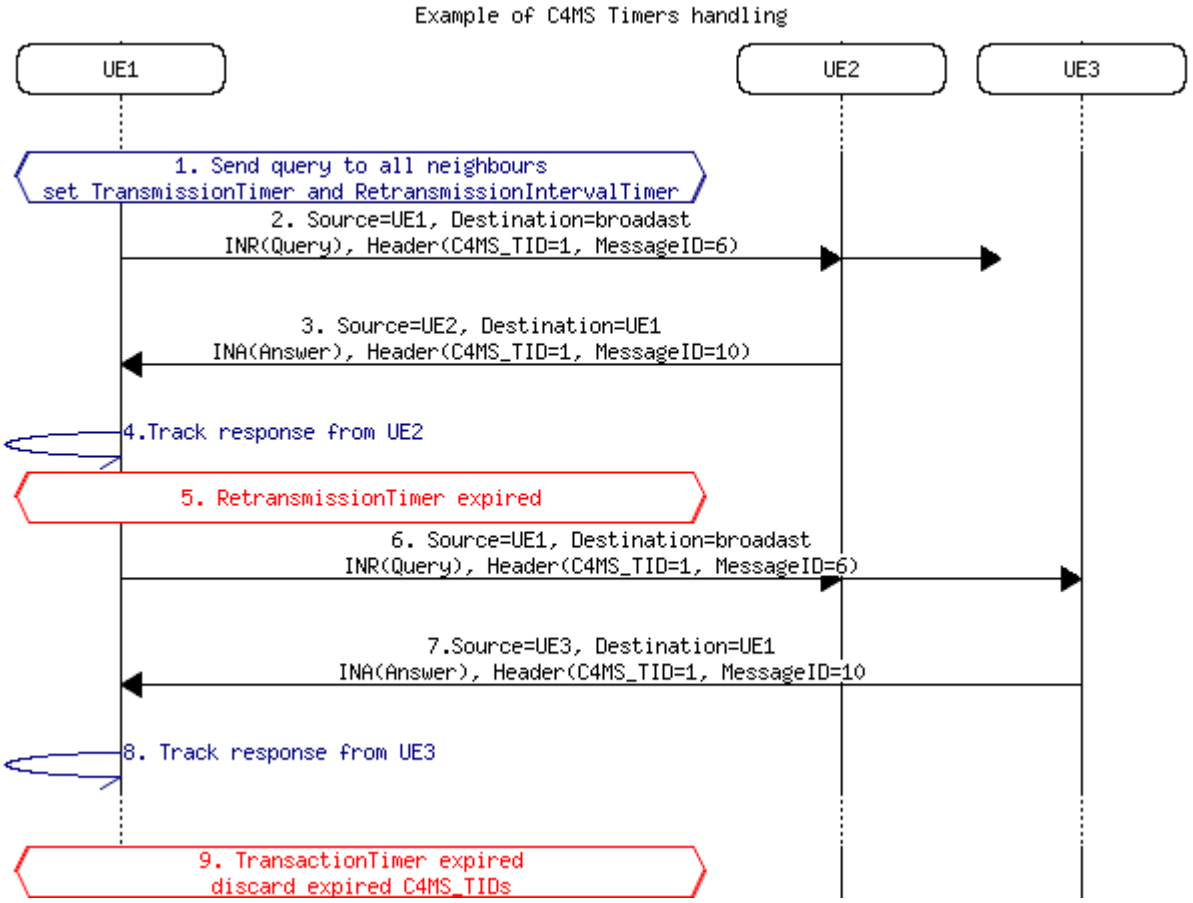

Figure 9: C4MS timers example

2.5 Procedures

The following list of elementary ON management procedures and messages is required to be supported over C4MS (detailed specification of messages and procedures can be found in the Appendixes to D3.3, Section 3 [10]).

- Information Provisioning (specified messages: Information.Request, Information.Answer, Information.Indication)
- ON Suitability (specified messages: ON_Suitability.Indication)
- ON Negotiation (specified messages: ON_Negotiation.Request, ON_Negotiation.Answer)
- ON Creation (specified messages: ON_Creation.Request, ON_Creation.Answer)
- ON Modification (specified messages: ON_Modification.Request, ON_Modification.Answer)

- ON Release (specified messages: ON_Release.Request, ON_Release.Answer)
- ON Status Notification (specified messages: ON_Status.Notification)

2.6 State machines in the OneFIT system

Each node includes typically several state machines. Figure 10 shows the location of some selected state machines.

In each node potentially participating in an ON, the CMON must have information if a node is participating in an ON or not. Further on, status information must also be stored on which other nodes are participating in the ON, especially for those nodes which have a direct link to the own node. Therefore, as shown in Figure 10 and as described in more detail in D3.2 [3], each node maintains an ON-Node-State as well as for every active link towards another node an ON-Link-State.

Similarly, the other building blocks like JRRM and CCM contain also one more state machines.

Also most protocols include state machines.

TCP [11] for example has the following states: LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT, and the fictional state CLOSED.

The IPv4 protocol as described in IETF RFC 0791 [8] maintains only minimal state information between datagram transmissions.

However, some protocols like UDP are stateless and thus do not include a state machine.

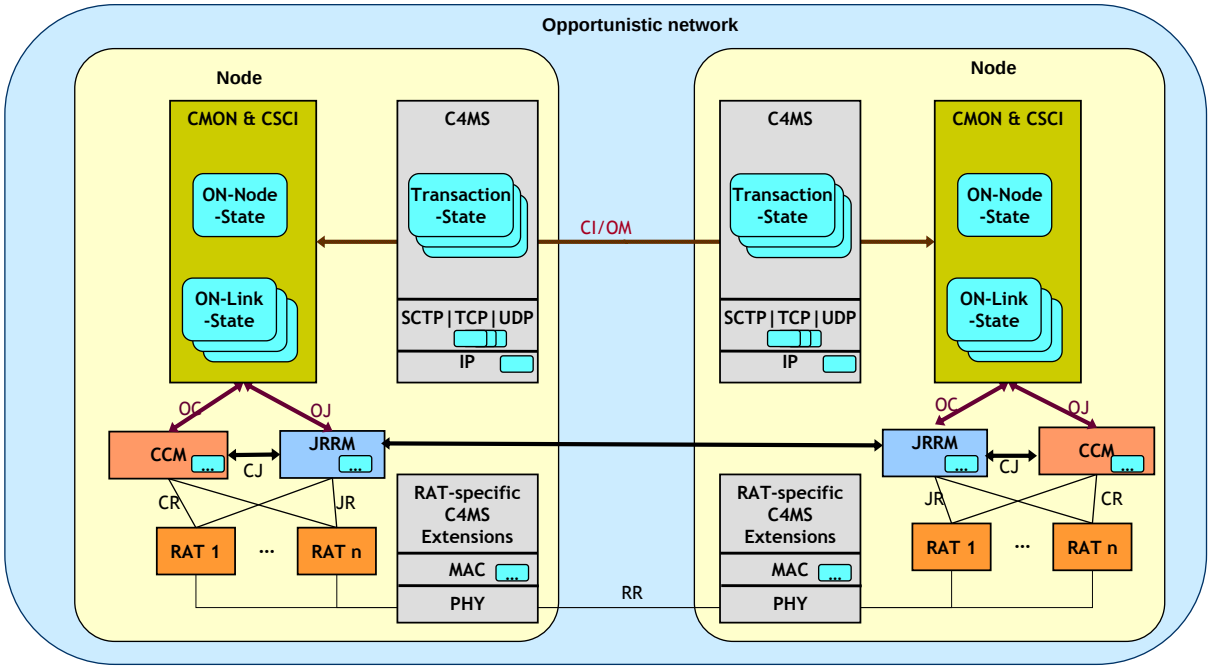

Figure 10: Location of some state machines in the nodes

2.6.1 C4MS Protocol state machine

The C4MS protocol uses three categories of messages:

- Request
- Answer
- Indication

When a Request is sent from a Node 1 to a Node 2, then an Answer shall be sent back from Node 2 to Node 1. If the Node 1 does not receive an answer in a certain time frame, then the message shall

be retransmitted until a defined number of maximum retries is reached. An indication can be sent from one Node to another Node (There is no Answer message sent in response to an indication).

This behaviour is shown in the C4MS Protocol State Machine below:

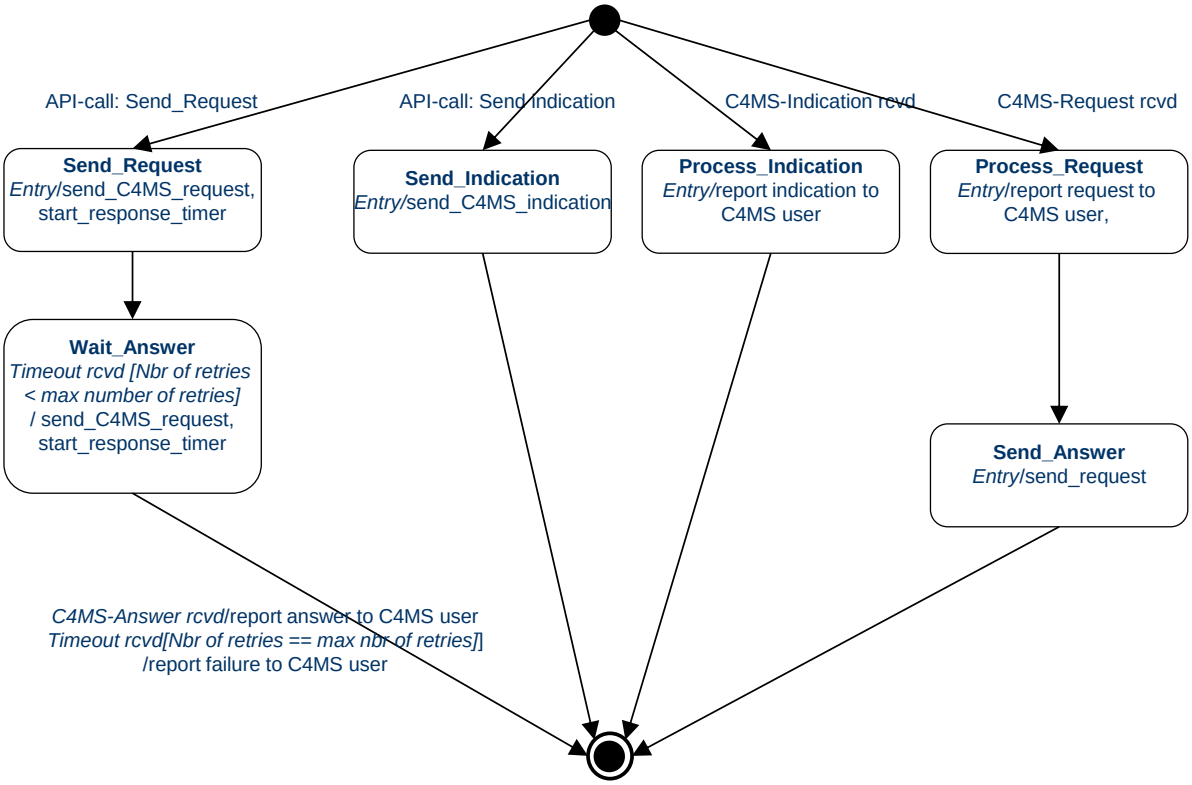

Figure 11: C4MS Protocol state machine

As an example, when Node 1 sends a request, then the state machine in Node 1 is first in the state "Send_Request" and then in the state "Wait_Answer". After receiving the request in Node 2, the state machine in Node 2 will be first in "Process_Request" and then in the state "Send_Answer".

2.7 C4MS security related aspects

As mentioned in D3.2 [3], a principle for designing C4MS security is to ensure an easy integration in the legacy 3GPP security framework for e-UTRAN/EPC, i.e. the latest generation of cellular networks. This implies to re-use as much as possible of key management principles (key hierarchy, key separation, key derivation and key provision) and authentication procedures. As both 3GPP and IEEE radio technologies are considered, a reuse of the 3GPP and the IEEE procedure is expected for reaching the same level of security as the current 3GPP network.

It was identified that Data integrity and confidentiality needs to be provided not only between end-to-end devices but also between relay devices residing in the path. Two types of data have been identified to be protected: the C4MS signalling messages and the user traffic. This have also to be protected over the new paths introduced for ON such as the UE relay and the UE-to-UE direct communication.

Regarding the ON signalling message, the end to end protection of the messages can be realised differently depending on the protocol used to transport the ON signalling. If the ON signalling messages are transported by IP messages, then the security scheme can be similar to the UE-ANDSF security scheme. If the ON signalling messages are transported over PDCP as for the 3GPP signalling, then a new key derivation has to be defined. For the new particular case of ON signalisation message exchanged over UE-to-UE direct communication, a specific protection based on a group key

utilisation is defined. For the particular cases of relay, several solutions based on existing 3GPP solutions have been defined. Solutions are either IPsec or 3GPP based.

Regarding the User plane messages, the new user plane for direct UE to UE communication has to be considered. In this case, a specific protection based on a pair-wise or group key utilisation has been defined.

2.7.1 Securing UE-to-UE direct communication

Most of the OneFIT scenarios are characterized by the existence of multiple mobile terminals which may spontaneously set up ad hoc networks between each other. It needs to be stressed, that no trust relationship is granted between communication parties.

In order to provide security in such scenarios we decided to propose security mechanisms that make use of public key certificates which enable mutual authentication and establishment of an encrypted connection between a pair of nodes without the need for a pre-shared secret[7]. The common problem of the solutions based on public key certificates is related to certificate generation, delivery, revocation, etc. In order to address these problems and at the same time enable simple integration with the legacy 3GPP security framework we decided to reuse the Generic Authentication Architecture (GAA) [21] which was standardized by 3GPP.

In general the GAA can be defined as an authentication service which can be provided by a network operator to allow mutual authentication between a client and a server. GAA reuses the existing authentication and key management procedures used in the 3GPP based cellular networks thus allowing its simple integration with the already deployed systems. One of the possible applications of the GAA is related to the authentication of clients/subscribers to the Public Key Infrastructure to enable signing their certificates [22]. This specific application of GAA is in a particular interest of OneFIT as it can be directly applied to our scenarios.

It needs to be underlined that in order to enable application of the abovementioned solution a Network Application Function (NAF) server dedicated for authentication of client's/subscriber's requests for signing their certificates needs to be deployed by the network operator. The following figure depicts the necessary system components.

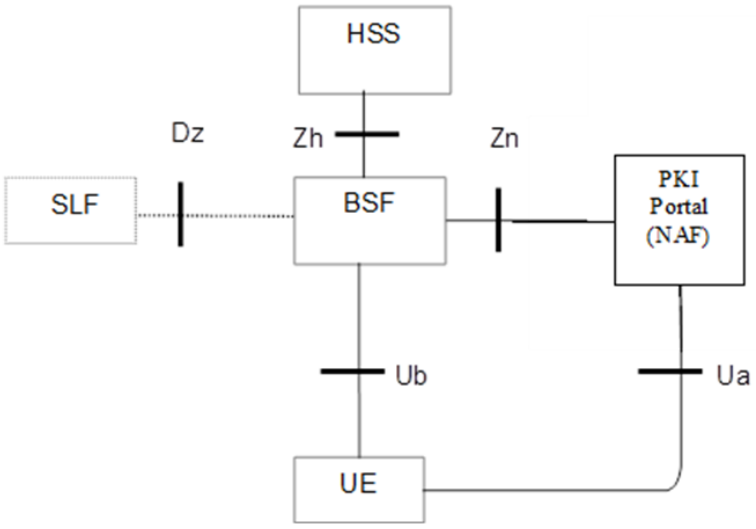

Figure 12: Necessary system components for securing UE to UE communication, borrowed from [22]

[7] Pre-shared secret is not likely to be present in our scenarios

Using the obtained subscriber certificates, UE-to-UE communication in our scenarios can be secured, depending on the C4MS implementation option, using transport layer (e.g. TLS), network layer (e.g. IPsec) or link layer (e.g. 802.1X-EAP-TLS[8]) based solutions.

Securing the C4MS broadcast traffic

Authentication of broadcast traffic is a common problem for most of the existing ad-hoc networks . A straight forward solution to solve this problem in our scenario would be to directly use the subscriber certificates (delivered using the GAA) to sign each broadcasted message. Signing (and verifying) each message individually is however computationally expensive and may introduce a significant computational overhead (e.g. [35]). This is especially visible in case of small messages which fit into a single packet (in such a case we would end-up signing each packet). In order to address this problem we decided to propose a scheme which is based on symmetric cryptography and was originally proposed for the Wireless Sensor Networks in [36]. The basic idea of the proposed scheme is to enable message authentication and ensure message integrity by adding to each broadcasted message a set of Message Authentication Codes (MAC). MACs are generated by transmitter for each potential receiver using keys shared between transmitter and receivers. The following figure depicts the proposed message format for the secured C4MS broadcast message and is based on the message format proposed in [36].

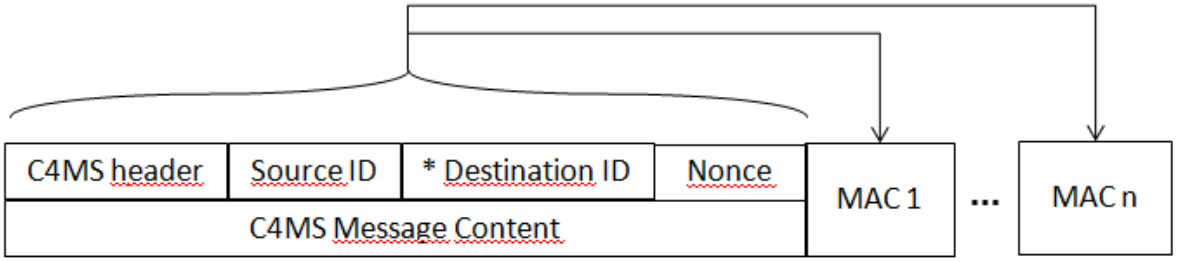

Figure 13:C4MS message frame with Medium Authentication Codes (MACs) appended.

It needs to be underlined here that in order to establish a shared key between each pair of terminals in the network (what is necessary for the scheme to work), we reuse the security procedures proposed in the previous subsection.

It needs to be noted that as message authentication and integrity for the C4MS broadcast traffic may consume significant amount of resources, the solution may be applied on demand, if determined to be necessary.

It needs to be also noted that the proposed security scheme for the C4MS broadcast traffic is applicable for different C4MS implementation options which are used for the implementation of terminal to terminal connectivity (we assume that the infrastructure to terminal link is already employed with the proper mechanisms[9]).

2.7.2 Securing UE-to-Infrastructure communication

In order to enable secured connection between UE and the infrastructure for the C4MS traffic we intend to reuse the security solution which was applied to enable secured communication between UE and ANDSF [23]. The solution is based on the GAA and PSK TLS. In contrast to the UE-to-UE communication, GAA in this case is used for the establishment of a shared secret between UE and

[8] Although IEEE 802.1X and EAP-TLS are not commonly used for enabling authentication in ad-hoc networks, they can be used for that purpose (e.g. [37])

[9] In case of IEEE 802.11, the security mechanisms for the broadcast traffic are not provided and the proposed security mechanisms may need to be applied.

NAF (which in our case is CMON/CSCI). As mentioned in [23], the solution enables mutual authentication, integrity protection and confidentiality.

It is worth to underline here that the solution is necessary to secure the communication only for the RAT independent implementation of C4MS. In case of a RAT dependent implementation, security of the C4MS traffic is guaranteed by the underlying RAT.

It is worth to underline here that as the proposed solution provides end-to-end security, and thus it is applicable in case the communication takes place over a set of relaying UEs. The set of system components which enable application of such a solution is almost identical to the set presented in Figure 12. However, in this case the PKI portal is replaced with a component which realizes CMON/CSCI functionalities.

3. C4MS data structures

This section provides information on the data structures that have been defined from OneFIT. Initially, information on the profiles is described. Contextual information and decisions follow. Knowledge-related and policies information are finally described. The following figure provides a high-level description of data structures.

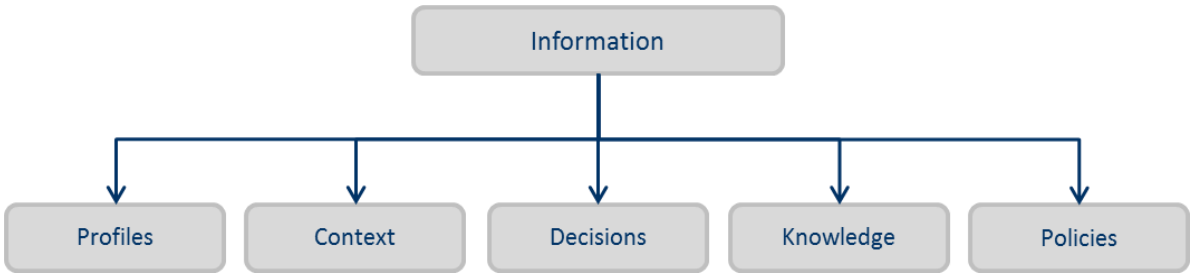

Figure 14: High-level description of data structures

3.1 Profiles, capabilities, requirements data structure

This section analyses the "Profiles" data structure. High-level description of this data structure is provided through Figure 15. Profiles are divided into terminal, base station, user and operator profiles. Terminal and BS profiles include:

- General capabilities, e.g. Node ID, Node Type etc.;
- Communication capabilities, e.g. Network interface capabilities, supported spectrum sensing techniques etc.;
- Computing capabilities, e.g. CPU, memory size etc.;
- Storage capabilities, e.g. caching size etc.;
- Energy capabilities, e.g. battery capacity etc.;
- Opportunistic Network capabilities, e.g. does the terminal/BS support ONs, incentives, how many times has the terminal participated in an ON etc.

Additionally, user profile provides information on the subscribed applications of a user, the user class of an application (i.e., the quality levels that the application can be provided to this user class. E.g. for streaming or browsing application type, a user that belongs to the 'High' user class the possible qualities of service shall be e.g., 2Mbps, 1Mbps or 512Kbps etc.). Also, the behaviour aspects of the user are taken into account. These aspects indicate the number of requests from a user in order to use an application and the usage characteristics. Usage characteristics include the estimated session duration and the estimated data volume transfer. For example a user may need to use an ON for 5 minutes or may need to download a small (e.g. 1-2MB) or a large file (e.g. 20MB). We would like to determine if an ON can support a user with these usage characteristics. Finally, operator profile shall include information on the elements (e.g. BSs) that the operator owns/ manages, its subscribers etc.

Figure 16 and Figure 17 provide a detailed view of the terminal profile and user profile data structures respectively.

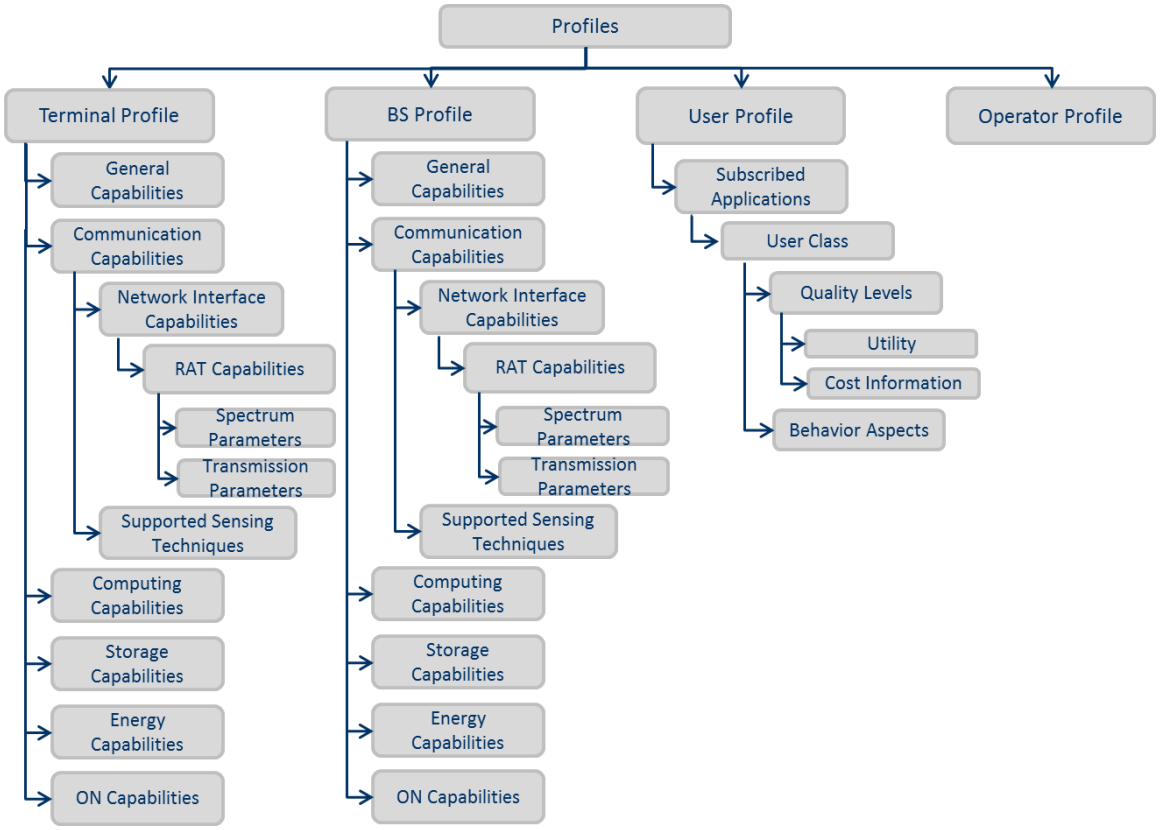

Figure 15: 'Profiles' data structure

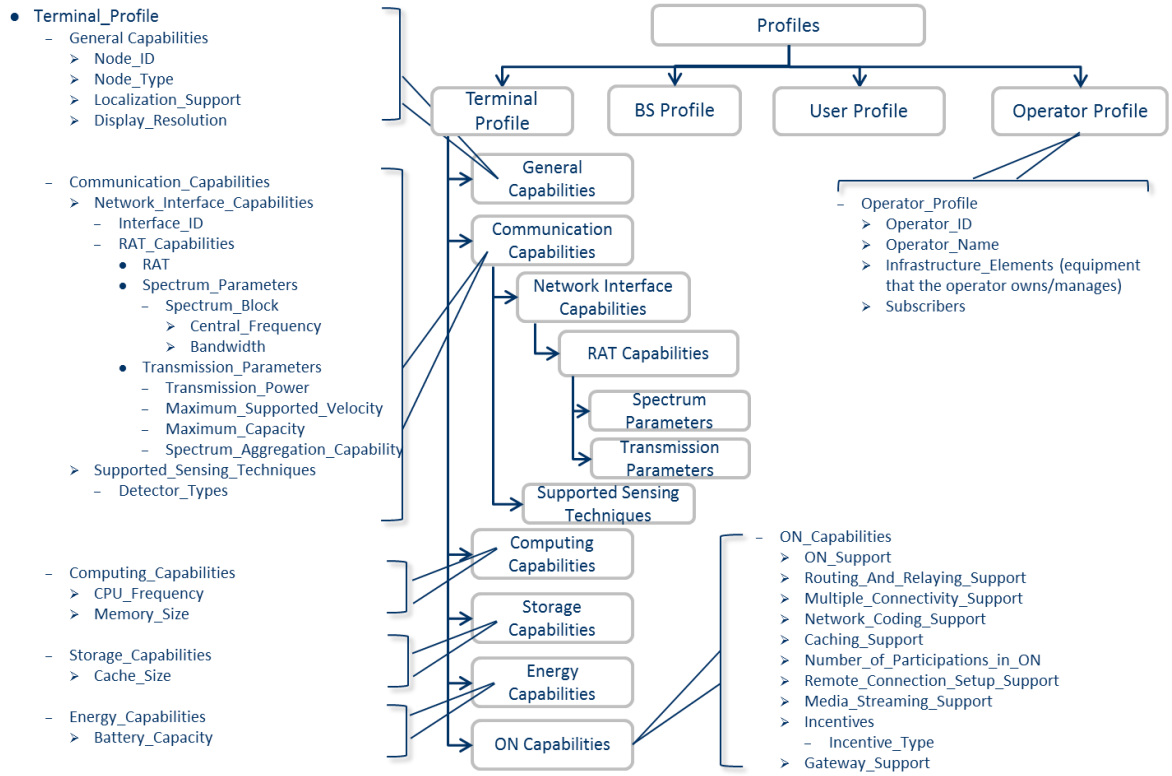

Figure 16: 'Terminal Profile' and 'Operator Profile' detailed data structure

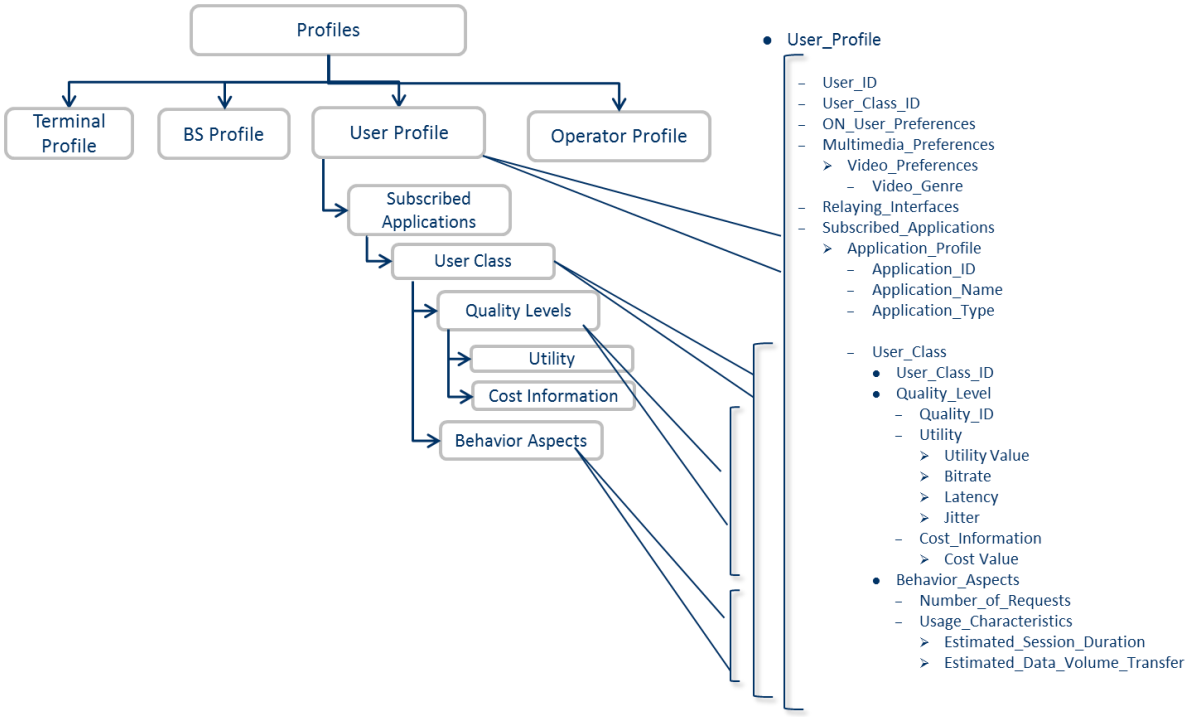

Figure 17: 'User Profile' detailed data structure

3.2 Context information data structure

This section analyses the "Context" data structure. High-level description of this data structure is provided through Figure 18. Contextual information is divided into terminal and base station context. Terminal and BS context include:

- General status, e.g. Node location, Context timestamp, Node mobility (in case of a terminal) etc.;
- Communication status, e.g. interface status, RAT operated, demand and QoS offered per application, user class etc.;
- Computing status, e.g. current CPU/memory usage;
- Storage status, e.g. current cache usage;
- Energy status, e.g. current battery level;
- Opportunistic Network specific context, e.g. ON services offered, Supported ONs (ON paths from terminals to BSs –set of nodes and links), Potential ONs (neighboring terminals that support ON) etc.

Also, Figure 19 and Figure 20 illustrate the detailed data structure of the BS Context and Terminal Context respectively.

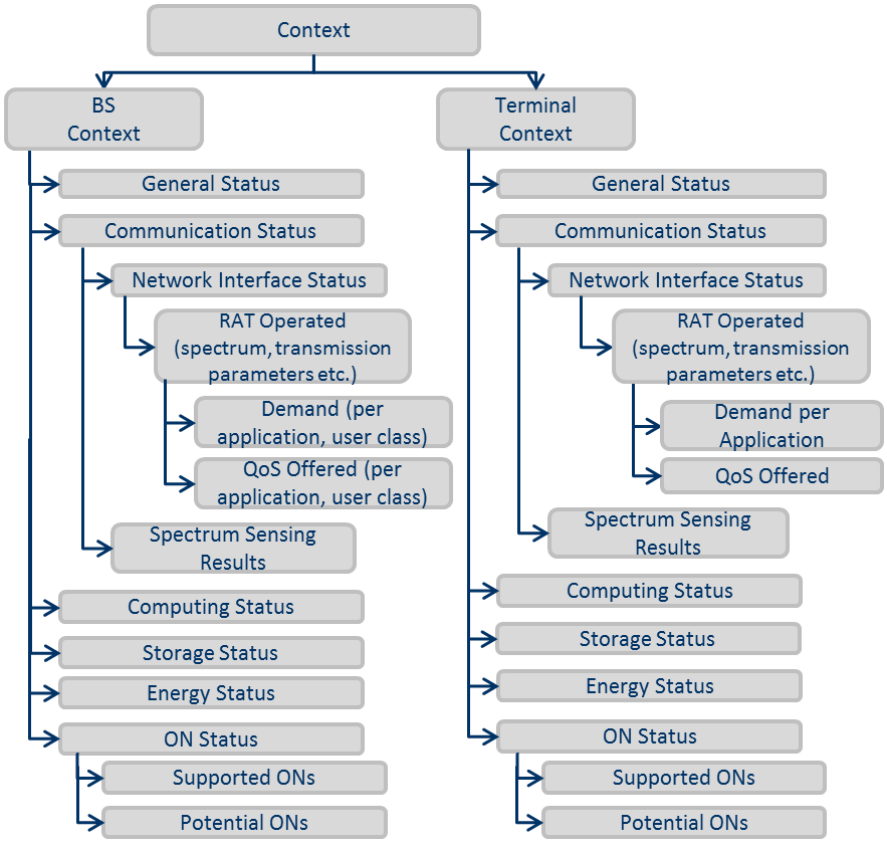

Figure 18: 'Context' data structure

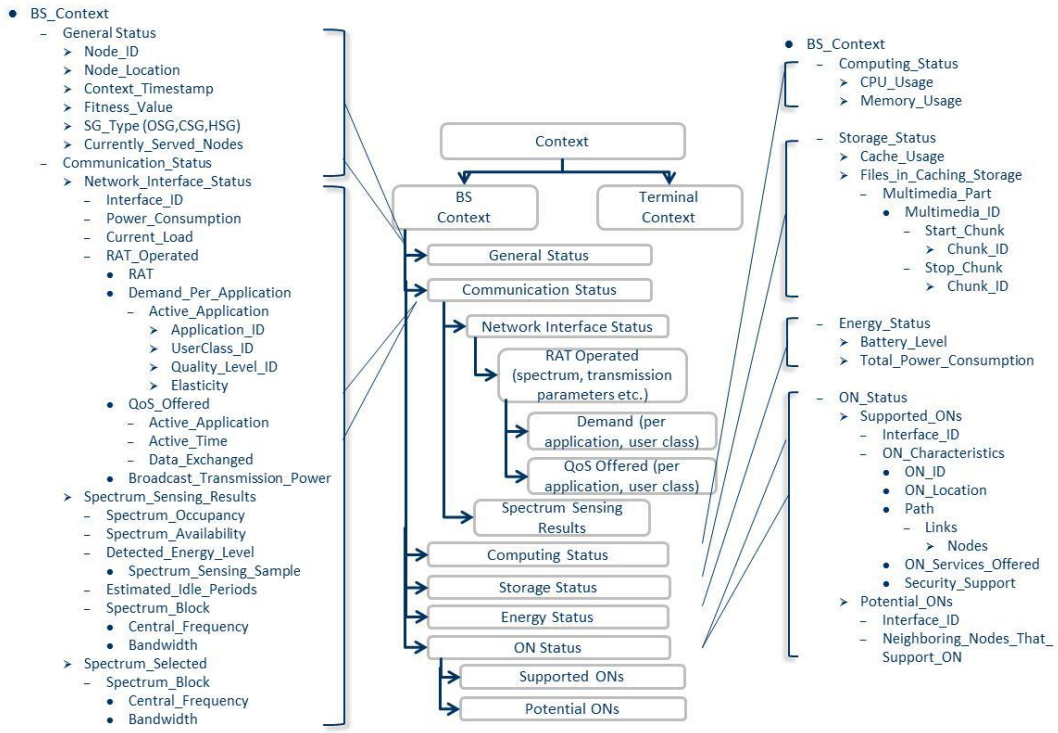

Figure 19: 'BS Context' detailed data structure

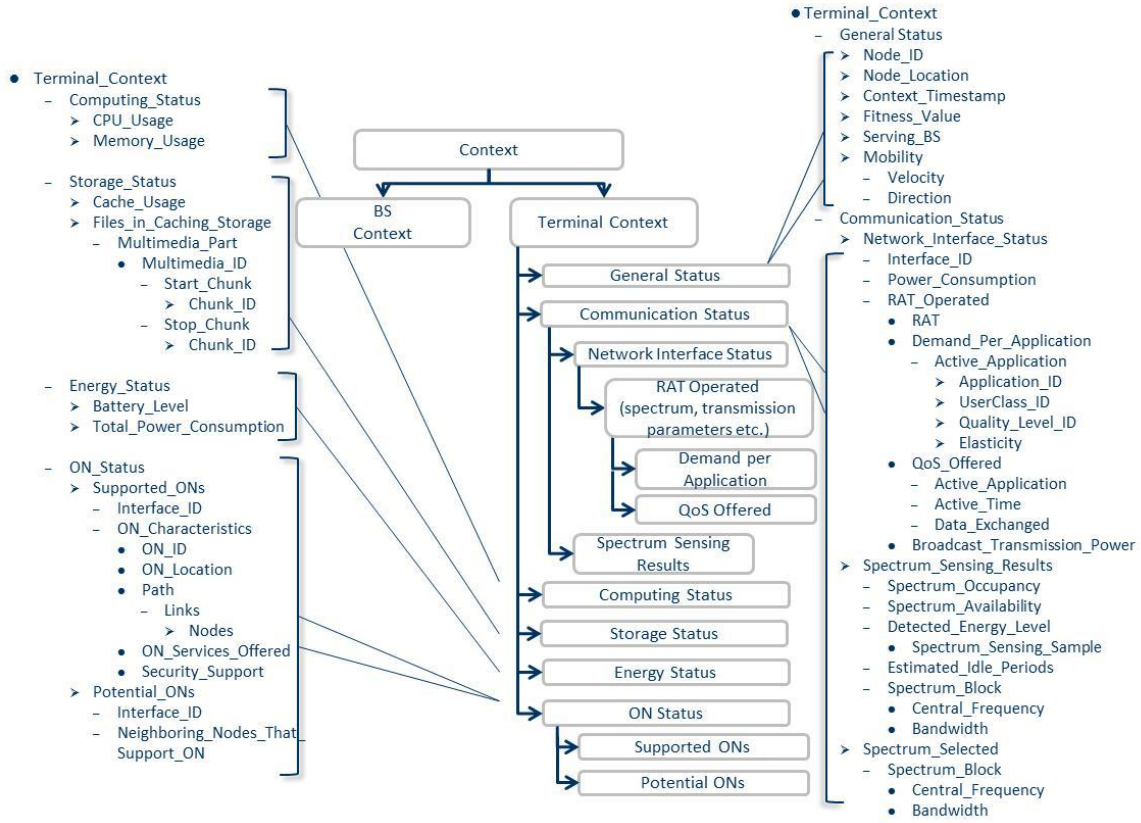

Figure 20: 'Terminal Context' detailed data structure

3.3 Decisions data structure

This section analyses the "Decisions" data structure. High-level description of this data structure is provided through Figure 21. Information on decisions is divided into ON decisions, infrastructure decisions and terminal decisions. Specifically, ON decisions include:

- Path selection (covering selected nodes and links);
- Spectrum selection e.g. selected spectrum block such as central frequency, bandwidth, selected sensing technique (e.g. sensing detectors etc.) and transmission constraints (e.g. maximum allowed transmit power etc.).

Additionally, infrastructure and terminal decisions cover aspects on communication, storage and computing.

- Communication Decisions, e.g. RAT to be operated (including assigned demand per application and user class, assigned terminals)
- Storage Decisions, e.g. amount of cache to be used etc.
- Computing Decisions, e.g. CPU or memory amount to be used etc.

Also, Figure 22 and Figure 23 illustrate the detailed data structure of the ON and Infrastructure decisions respectively.

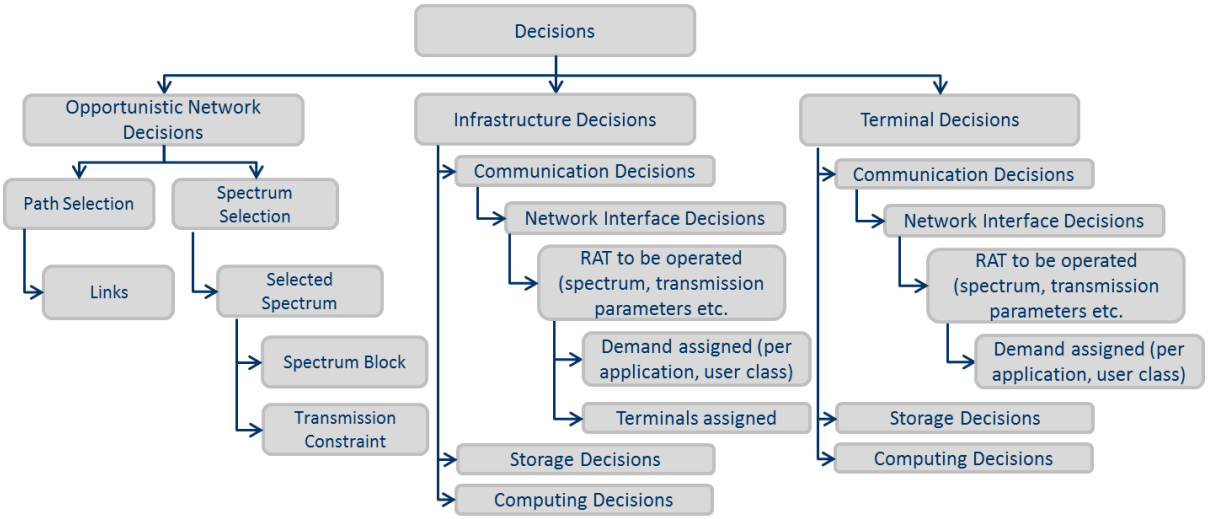

Figure 21: 'Decisions' data structure

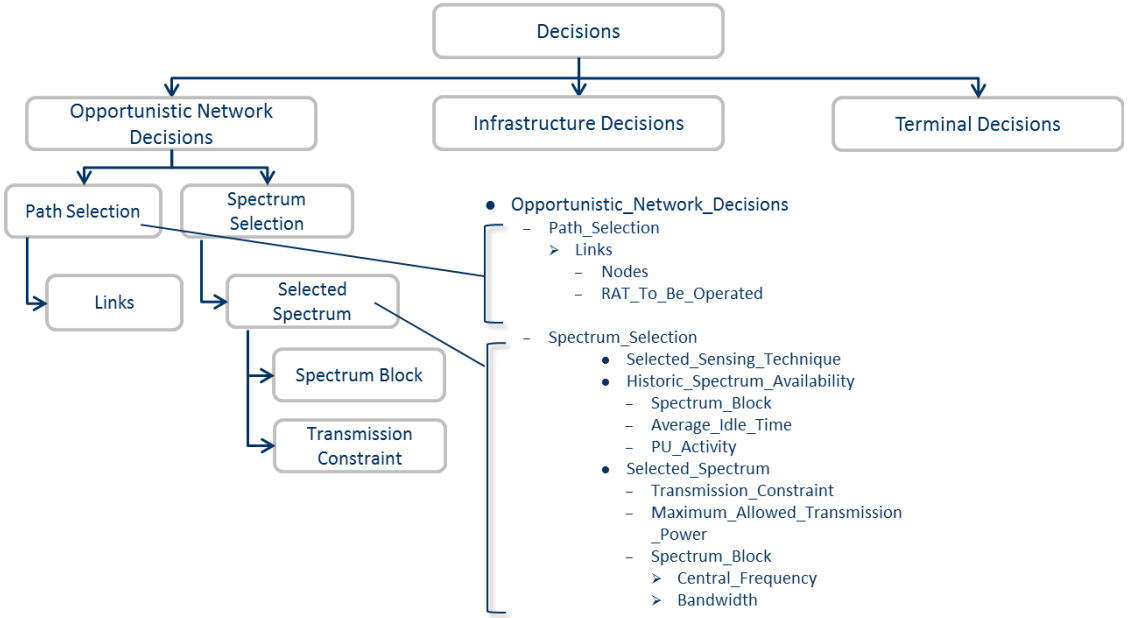

Figure 22: 'Opportunistic Network Decisions' data structure

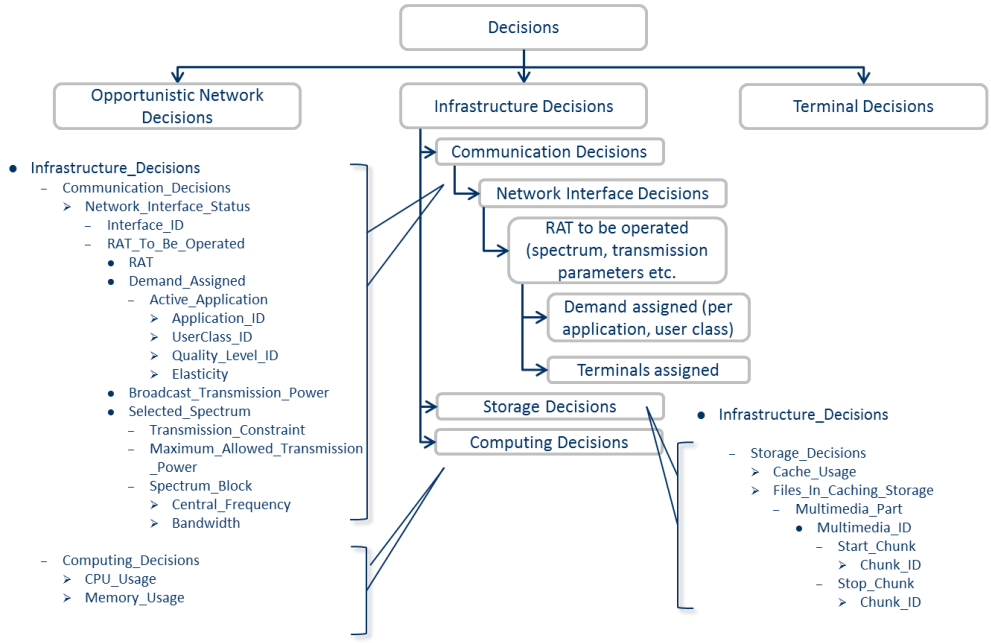

Figure 23: 'Infrastructure Decisions' data structure

3.4 Knowledge data structure

This section analyses the "Knowledge" data structure. High-level description of this data structure is provided through Figure 24. Knowledge is focused on acquired context and decisions made. For example, ON knowledge information is focused on the selected path, selected spectrum etc. (e.g., nodes and links used, spectrum used, QoS achieved etc.). Infrastructure-related knowledge includes: communication decisions (such as RAT operated, assigned demand per application and user class, assigned terminals etc.); storage decisions (such as amount of cache used etc.) and computing decisions (such as CPU/memory used etc.). Accordingly, terminal-related decisions include communication decisions (such as RAT operated, applications served, QoS offered etc.); storage decisions (such as amount of cache used by the terminal etc.) and computing decisions (such as CPU, memory used etc.).

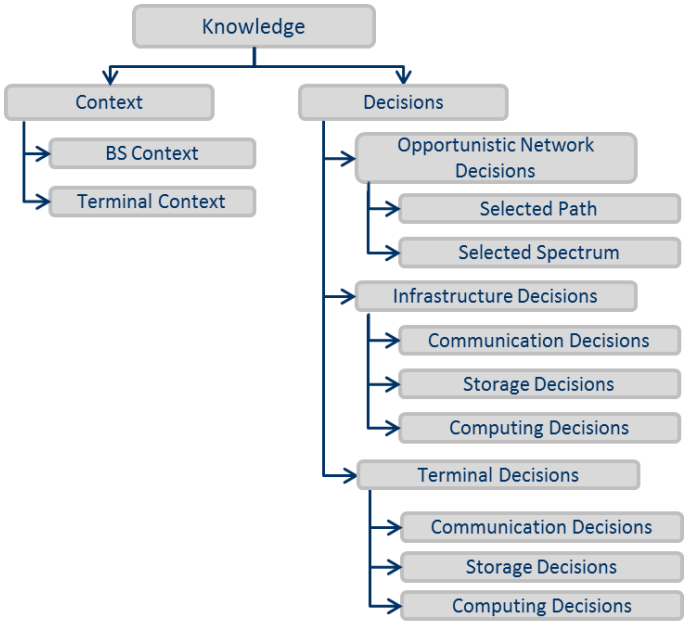

Figure 24: 'Knowledge' data structure

3.5 Policy data structure

Policies represent rules of the network operator that are imposed for certain reasons. To that respect network operator policies shall include:

- Communication related policies (such as allowed interfaces, allowed relaying capacity etc.);
- Computing related policies (such as allowed CPU usage, allowed memory usage etc.);
- Storage related policies (such as allowed caching size etc.);
- Energy related policies (such as allowed consumption etc.);
- Opportunistic Network related policies (such as maximum number of nodes in an ON, maximum time to live, allowed applications and quality levels etc.);

The following figure illustrates the aforementioned data structure.

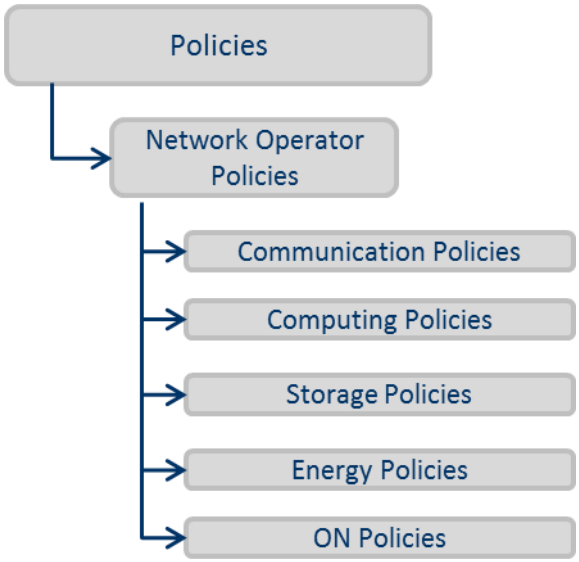

Figure 25: 'Policies' data structure

4. Signalling evaluation methodology

To enable opportunistic networking, additional traffic is created for the ON-related signalling in addition to the normal signalling for the legacy procedures. In order to determine the cost of operator governed opportunistic networking, the implementation of the ON concept needs to be then preceded by a proper estimation of the amount of the signalling traffic generated by management algorithms. It needs to be noted that signalling load assessment will take into consideration not only information transported within the C4MS messages but also information that is utilized by the ON management algorithms and conveyed via RAT specific messages. Additionally, it is also desirable to analyse the convergence time of different ON phases to determine the feasibility of Opportunistic Networks in different scenarios, given the proposed signalling procedures. The following section describes the methodology which will be followed for the purpose of signalling evaluation. It is worth to underline here that, in contrast to the approach taken in WP4 [7], the evaluation in WP3 is intended to be based mainly on the analytical analysis[10].

In general, the evaluation plan for the C4MS signalling assessment can be divided into four main steps:

1. **Determination of evaluation scenarios**: the evaluation scenarios to conduct analysis in the third step will be defined based on the set of OneFIT scenarios. The evaluation scenarios to conduct analysis in the last step will be based on the scenarios proposed by the WP4 partners. A first set of possible scenarios for the last step, which is to be used as a basis for the purpose of the signalling analysis, was proposed in M4.2 [7].
2. **Estimation of the ON related message sizes for different scenarios**: estimation of the protocol message sizes[11] which are to be exchanged to enable proper operation of the ON related algorithms in different ON phases and different scenarios. Message format definitions and data structures are provided in Section 2.2 and the Appendix to D3.3, Section 3 [10] respectively and will be used as basis during this step.
3. **Analytical analysis of ON related signalling for different scenarios**: analytical analysis conducted in this step aims to provide a general view on the signalling generated by the operation of ON in different scenarios. The analysis aims to cover the evaluation of the signalling for joint operation of different ON related algorithms in different ON phases.
4. **Analysis of signalling for ON related algorithms in different scenarios:** The main aim of this step is to provide insight into an impact of a specific ON algorithm on the overall signalling. This step includes the analysis of possible information management strategies (based on the information provided in the Appendix to D3.3, Section 7 [10]) which could affect the amount of signalling traffic generated by different algorithms in different ON phases.

The reference model illustrated in Figure 26 is considered as a common framework for conducting the signalling evaluation. On the left-hand side, the proposed information management strategies to be evaluated are depicted. The proposed strategies will be analysed for different WP4 algorithms to assess the signalling load. The analysis will be conducted on the identified set of evaluation scenarios, through well-defined metrics (see next paragraph).

[10] Evaluation based on simulations as well as experimental test-beds are not excluded from the proposed methodology

[11] The estimation will be provided for C4MS messages as well as RAT specific messages exchanged for the purpose of ON management.

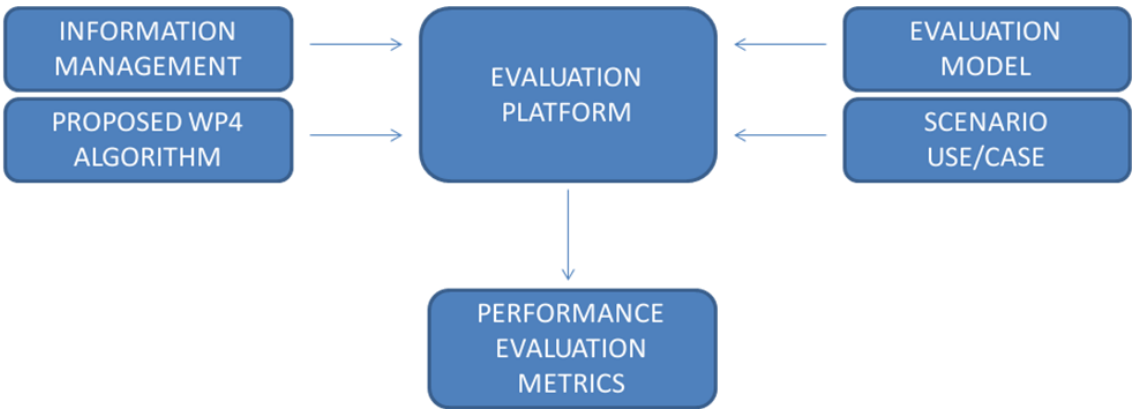

Figure 26: Reference model for signalling evaluation

The methodology is sustained on the following considerations:

- The exact set of data structures (see the Appendix to D3.3, Section 3 [10] for data structure definition) to be exchanged for the ON related algorithms, based on their final implementation, will be identified by the involved partners.
- Partners shall take into account ON related management information transported via C4MS messages and RAT specific messages. However, it needs to be noted that RAT specific messages that are transmitted to support the legacy network operation (e.g. measurement reports for mobility management in cellular networks) are not accounted to the ON related signalling traffic.
- The evaluation model to be used for the analysis will be described by each partner, thus enabling to assess the conditions on which the signalling load has been tested by other partners.
- Partners will be open to receive suggestions to conduct further analysis and will support other partners to the possible extent. This can be particularly useful to enable joint analysis of different algorithms.

The following paragraph provides an overview of the evaluation metrics which are intended to be used for the purpose of the signalling evaluation. It is worth to underline here that, if necessary, the described set of metrics may be further extended.

- Signalling load – the cumulative size of control data exchanged or the average size of signalling data transmitted per time unit by a node. The metric is an indication of the bandwidth resources that are consumed by the signalling for the purpose of ON management (the metric takes into account data transmitted via C4MS messages and via RAT specific messages);
- Signalling message rate – number of C4MS and RAT specific messages related to ON management transmitted per second by a node;

5. Analytical ON signalling evaluation

The following section focuses on estimation of the signalling load imposed by ON management in different ON phases (i.e.: Suitability determination, Creation, Maintenance and Termination). In general, the section provides joint analytical analysis of signalling traffic generated by multiple ON related algorithms operating in different ON phases (the allocation of algorithms to the ON phases is based on M4.2,see Figure 27). Although the initialization phase is not specified as a distinct ON phase in earlier stages of the project, signalling evaluation respective to this phase is also presented hereinafter. Additionally, evaluation of signalling generated by the mechanisms related to security is also introduced in this section.

		Discovery of terminals supporting ONs	Modular decision flow for selecting frequency, bandwidth and RAT	Fittingness-factor based spectrum selection	Machine Learning based knowledge acq. On spectrum usage	Techniques for aggr. Of available spectrum bands/fragments	Knowledge based suitability determination	UE to UE Trusted paths	Selection of Nodes and Routes	Route pattern selection in ad-hoc network	QoS and Spectrum aware routing techniques	Application cognitive multipath routing in wireless mesh networks	Multi-flow routes co-determination	Techniques for network reconfiguration-topology design	Content conditioning and distributed storage virtualization
Technical challenge	Node discovery	X													
	Node selection						X		X						X
	Route selection						X	X	X	X	X	X	X	X	
	Spectrum identification		X	X	X										
	Spectrum selection		X	X	X	X					X				
ON Management stage	Suitability	X	X	X	X		X			X	X	X			X
	Creation	X	X	X	X	X		X	X		X	X	X	X	X
	Maintenance & Termination	X	X	X	X	X				X	X	X	X	X	X
Scenario	Scenario 1	X	X	X	X	X	X	X	X	X	X		X	X	
	Scenario 2	X	X	X	X	X	X		X	X	X		X	X	
	Scenario 3	X	X	X	X	X	X	X	X	X	X		X	X	
	Scenario 4	X	X	X	X	X	X	X	X					X	
	Scenario 5		X	X	X	X	X		X			X			X

Figure 27: Identification of commonalities among algorithms, borrowed from [7].

5.1 Suitability, Creation, Maintenance and Termination phase signalling evaluation

The following section focuses on the analytical evaluations of the control traffic generated during different ON phases, in different OneFIT scenarios. The evaluations conducted in this section are based on the final set of Message Sequence Charts (MSCs) originally proposed in D3.2 [3] (see Appendix to D3.3, Section 4 [10]), proposed C4MS data structures (see Section 3 and the Appendix to D3.3, Section 3 for more detail [10]) and C4MS message format definitions (See Section 2.2 and the Appendix to D3.3, Section 5 [10]). Results provided in the subsequent sections present the overhead introduced by the joint operation of multiple algorithms, thus indicating the theoretical upper bound of the signalling overhead introduced by the application of C4MS for ON management.

5.1.1 Evaluation model

Analytical evaluations are based on the Message Sequence Charts (MSCs), proposed C4MS data structures and C4MS message format definitions (see the Appendix to D3.3 [10]). In order to simplify the analysis it is assumed that: 1) each procedure presented in the MSC is successful unless stated otherwise (for example, each ON Negotiation Request is replied with ON Negotiation Answer with an agreement to create an ON), 2) overhead introduced by the lower layers is not considered, 3) an links between terminals and terminals and infrastructure are error-free and have equal capacity. Additionally, in order to determine the upper bound of the signalling overhead it is assumed that no information is reused from the RAT-specific procedures (i.e. all the necessary information needs to be exchanged over C4MS), and that terminals encounter themselves for the first time (i.e. exchange of full profiles is necessary).

5.1.2 Verification scenario

The following scenario parameters are considered for the purpose of **scenarios #1 and #5** verification:

- Each node is equipped with 2 radio interfaces (in case of an infrastructure node both interfaces are used for the purpose of cellular connectivity provisioning, in case of mobile terminals, one radio interface is used for cellular connectivity, whereas the seconds is a short range radio interface).
- Each terminal is subscribed to a single application, and only requirements of a single application are manifested in the Terminal Profile.
- Each node supports three application quality levels
- Up to 2 links parameters are described in terminal context information.
- No multimedia parts are considered to be stored in the node's cache.
- At start, nodes do not have any ON-capable neighbors
- An ON is composed from 3 nodes at most

5.1.3 Information management strategies

The information management strategies are not explicitly evaluated in this section. For the purpose of this section it is assumed that the considered procedures are triggered based on some events related to e.g. QoS degradation, congestion indication, terminal arrival. This means, that as soon as some event occurs (e.g. congestion identification) the respective functional entities will be informed in order to initiate appropriate procedure (e.g. establishment of an ON).

5.1.4 Signalling message size estimations

Sizes of C4MS messages and parameters are estimated based on the assumptions presented in the verification scenario section (5.1.2). The following section firstly presents the minimum sizes of C4MS parameters sizes and afterwards specifies the sizes of exemplary C4MS messages used for the purpose of signalling evaluation.

The minimum sizes of the basic data types follow the 802.21 specification and are given in the following figure.

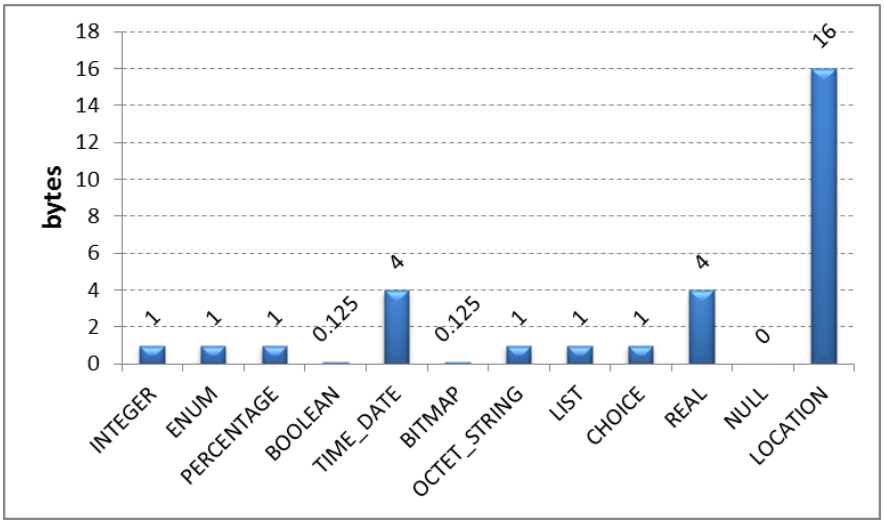

Figure 28: Minimum sizes of each data type according to the 802.21 specification

According to the specification, minimum sizes of data types of "Integer", "Enumeration", "Percentage", "Octet_String" are 1 byte (unless mentioned differently –e.g. we may use an "Integer" of 4 bytes, an "Octet_String" of 10 bytes etc.). Also, definitions of "List" and "Choice" add 1 extra byte to the contents of the "List" or the "Choice". "Boolean" and "Bitmap" data types are having minimum sizes of 1 bit (i.e., 0.125 byte). Finally, "Time_Date" and "Real" data types are having a size of 4 bytes each, while the "Location" data type is considered to be 16 bytes. Of course, "Null" requires zero bytes.

The "Profiles" data structure has been assessed according to the calculations that follow. Figure 29 provides the estimated sizes of Terminal and BS profile according to the 802.21 specification. Sizes may vary according to the number of interfaces and number of RATs per interface. It is calculated according to the following formula:

$$\text{BS/Terminal\_Profile} = 35 + \sum_{i=1}^{a}(18 \cdot x_i + 1) \quad (1)$$

where

$a = \text{number of interfaces}, a \geq 1$

$x = \text{number of RATs (per interface)}, x \geq 1$

Table 4 presents the considered cases for the evaluation of the BS/Terminal_Profile. Each case is distinguished by the considered number of available interfaces and the considered number of available RATs per interface.

Table 4: Considered cases for BS/Terminal_Profile evaluation

Case	1	2	3	4	5	6	7	8	9
# Interfaces	1	1	1	2	2	2	3	3	3
# RATs per interface	1	2	3	1	2	3	1	2	3

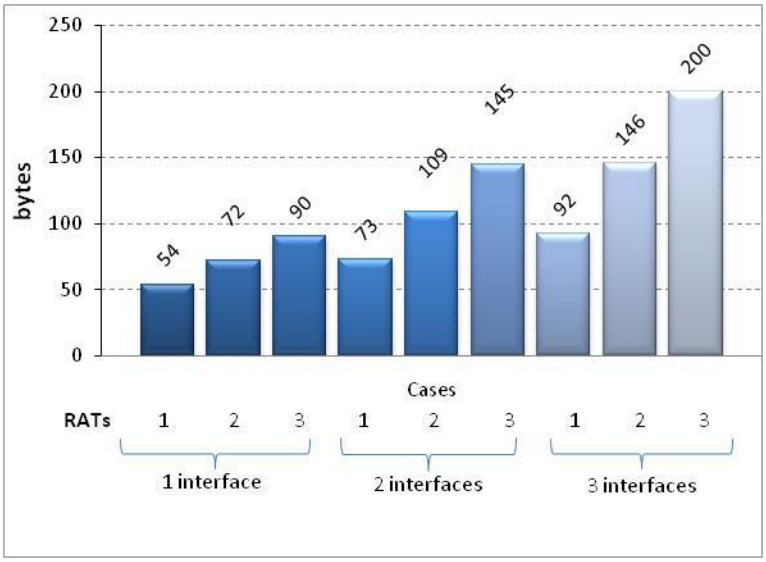

Figure 29: Estimated sizes of Terminal and BS profile according to the 802.21 specification

The "User_Profile" data structure uses as arguments the number of available interfaces that could be potentially used for relaying, the number of subscribed applications, the user classes of each application and the number of available quality levels for each user class. It is calculated through the following formula:

$$\text{User\_Profile} = 26 + a + \sum_{i=1}^{app_s} (9 + 12 \cdot q_i) \qquad (2)$$

where

$a = \text{number of interfaces},\ a \geq 1$

$app_s = \text{number of subscribed applications}, app_s \geq 1$

$q = \text{number of quality levels}, q \geq 1$

Table 5 presents the considered cases for the evaluation of the User_Profile. Each case is distinguished by the considered number of available interfaces, the considered number of subscribed applications and the considered number of the available quality levels.

Table 5: Considered cases for User_Profile evaluation

Case	1	2	3	4	5	6	7	8	9
# Interfaces	1	1	1	1	1	1	2	2	2
#Subscribed Applications	1	1	2	2	3	3	1	1	2
# Quality levels	1	2	1	2	1	2	1	2	1
Case	10	11	12	13	14	15	16	17	18
# Interfaces	2	2	2	3	3	3	3	3	3
#Subscribed Applications	2	3	3	1	1	2	2	3	3
# Quality levels	2	1	2	1	2	1	2	1	2

Figure 30 provides the estimated sizes of User_Profile according to the 802.21 specification. Sizes may vary according to the number of interfaces, the number of subscribed applications and the number of available user classes and quality levels.

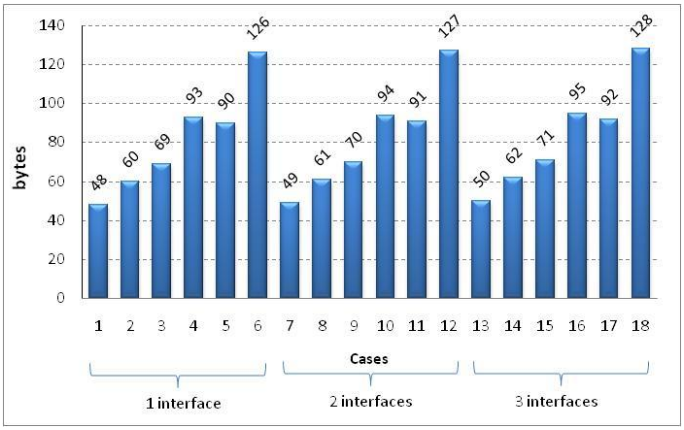

Figure 30: Estimated sizes of User_Profile according to the 802.21 specification

The "Terminal_Context" data structure uses as arguments the number of active applications, the number of multimedia parts that are available in the storage, the number of links of each terminal and the number of ON-capable neighbouring terminals. It is calculated through the following formula:

$$\text{Terminal\_Context} = 105 + \sum_{i=1}^{a_{act}} (28 + 4 \cdot app_{act}) + 6 \cdot m + 44 \cdot l + 4 \cdot t_n \qquad (3)$$

where

a_{act} = number of active interfaces

app_{act} = number of active applications, $app_{act} \geq 1$

l = number of links of terminal, $l \geq 1$

m = number of multimedia parts, $m \geq 0$

t_n = number of ON-capable, neighboring terminals, $t_n \geq 0$

Table 6 presents the considered cases for the evaluation of the Terminal_Context. Each case is distinguished by the considered number of active applications, the considered number of links of each terminal and the considered number of multimedia parts in the storage (files in caching storage).

Table 6: Considered cases for Terminal_Context evaluation

Case	1	2	3	4	5	6	7	8	9
# Active Applications	1	1	1	1	1	1	2	2	2
# Links	1	1	2	2	3	3	1	1	2
# Multimedia Parts	10	20	10	20	10	20	10	20	10
Case	10	11	12	13	14	15	16	17	18
# Active Applications	2	2	2	3	3	3	3	3	3
# Links	2	3	3	1	1	2	2	3	3
# Multimedia Parts	20	10	20	10	20	10	20	10	20

Figure 31 provides the estimated sizes of Terminal_Context according to the 802.21 specification. Sizes may vary according to the number of active applications, the number of links of each terminal and the number of multimedia parts in storage (files in caching storage). In the presented cases, each terminal is considered to have one potential neighbouring terminal to connect to, if needed.

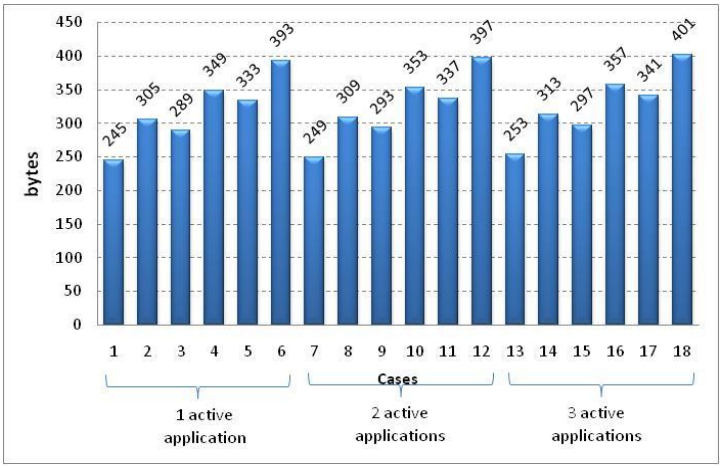

Figure 31: Estimated sizes of Terminal_Context according to the 802.21 specification

The "BS_Context" data structure uses as arguments the number of ONs currently supported by the BS and the Terminal_Context of each terminal currently connected to the BS. It is calculated through the following formula:

$$\text{BS\_Context} = 117 + m \cdot 6 + \sum_{i=0}^{on_s} (22 + 44 \cdot l_i) + \sum_{j=1}^{t_{BS}} \text{Terminal\_Context}_j \qquad (4)$$

where

$on_s = \text{number of supported ONs}, on_s \geq 0$

$l_i = \text{links of each supported ON } i, l_i \geq 1$

$m = \text{number of multimedia parts}, m \geq 0$

$t_{BS} = \text{number of terminals connected to BS}, t_{BS} \geq 1$

Table 7 presents the considered cases for the evaluation of the BS_Context. Each case is distinguished by the terminals connected to the BS, the currently supported ONs and the number of links per ON.

Table 7: Considered cases for BS_Context evaluation

Case	1	2	3	4	5	6	7	8	9
#Terminals connected to BS	10	10	10	10	10	10	10	10	10
# ONs	1	1	1	5	5	5	10	10	10
# Links per ON	1	2	3	1	2	3	1	2	3
Case	10	11	12	13	14	15	16	17	18
#Terminals connected to BS	40	40	40	40	40	40	40	40	40
# ONs	1	1	1	5	5	5	10	10	10
# Links per ON	1	2	3	1	2	3	1	2	3

Figure 32 provides the estimated sizes of BS_Context according to the 802.21 specification. Sizes may vary according to the number of terminals connected to the BS, the number of supported ONs and the number of links per ON. All these cases have been assessed separately for different Terminal_Context cases (as presented in previous Table 6), namely case 3 and case 12. Case 3 corresponds to terminals with 1 active application and 2 links per terminal, while case 12 corresponds to terminals with 2 active applications and 3 links per terminal.

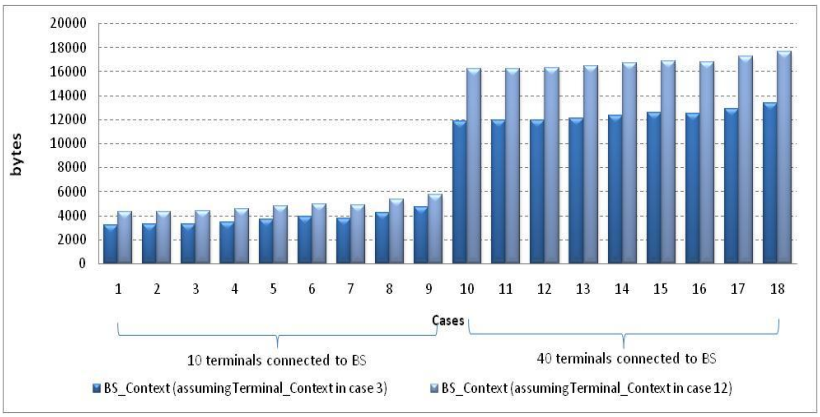

Figure 32: Estimated sizes of BS_Context according to the 802.21 specification

The "ON_Decisions" data structure uses as arguments the number of links in the ON and it is calculated through the following formula:

$$\text{ON\_Decisions} = 32 + 44 \cdot l_{ON} \qquad (5)$$

where

l_{ON} = number of links in the ON, $l_{ON} > 1$

Figure 33 provides the estimated sizes of ON_Decisions according to the 802.21 specification. Sizes may vary according to the number of links in each ON. There have been considered relatively small ONs (having 2 to 4) links per ON due to the fact that ONs are rather limited in size for performance reasons.

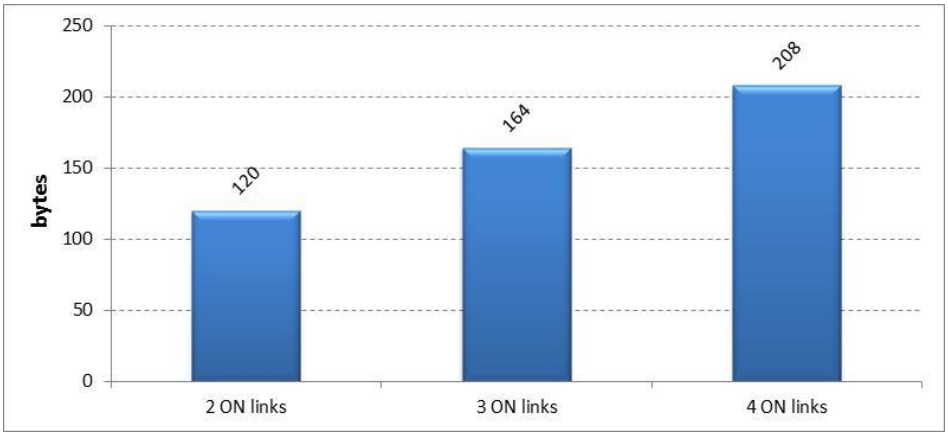

Figure 33: Estimated sizes of ON_Decisions according to the 802.21 specification.

Also, the Infrastructure_Decisions have been calculated according to the following formula:

$$\text{Infrastructure\_Decisions} = 22 + 2 \cdot a + 8 \cdot t_{served} + 6 \cdot m \qquad (6)$$

where

$a = \text{number of interfaces}, a \geq 1$

$t_{served} = \text{number of served terminals}, t_{served} > 0$

$m = \text{number of multimedia parts}, m \geq 0$

Table 8 presents the considered cases for the evaluation of the Infrastructure_Decisions. Each case is distinguished by the number of interfaces, the number of the served terminals and the number of multimedia parts (files in caching storage).

Table 8: Considered cases for Infrastructure_Decisions evaluation

Case	1	2	3	4	5	6	7	8	9
# Interfaces	1	1	1	1	1	1	2	2	2
# Terminals served	5	5	20	20	40	40	5	5	20
# Multimedia_Parts	10	20	10	20	10	20	10	20	10
Case	10	11	12	13	14	15	16	17	18
# Interfaces	2	2	2	3	3	3	3	3	3
# Terminals served	20	40	40	5	5	20	20	40	40
# Multimedia_Parts	20	10	20	10	20	10	20	10	20

Figure 34 provides the estimated sizes of Infrastructure_Decisions according to the 802.21 specification. Sizes may vary according to the considered number of interfaces, the number of served terminals and the files in caching storage.

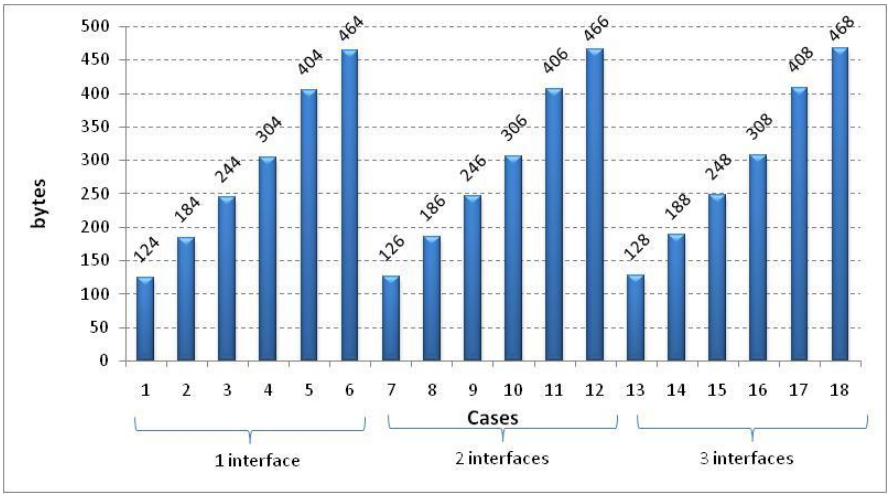

Figure 34: Estimated sizes of Infrastructure_Decisions according to the 802.21 specification.

$$\text{Terminal\_Decisions} = 30 + 2 \cdot a + 6 \cdot m \qquad (7)$$

where

$a = \text{number of interfaces}, a \geq 1$

$m = \text{number of multimedia parts}, m \geq 0$

Table 9 analyzes the considered cases that have been taken into account for the evaluation of the Terminal_Decisions data structure.

Table 9: Considered cases for Terminal_Decisions evaluation

Case	1	2	3	4	5	6	7	8	9
# Interfaces	1	1	1	2	2	2	3	3	3
# Multimedia_Parts	1	10	20	1	10	20	1	10	20

Accordingly, Figure 35 provides the estimated sizes of Terminal_Decisions according to the 802.21 specification. Sizes may vary according to the considered number of interfaces and the number of multimedia parts (files in caching storage).

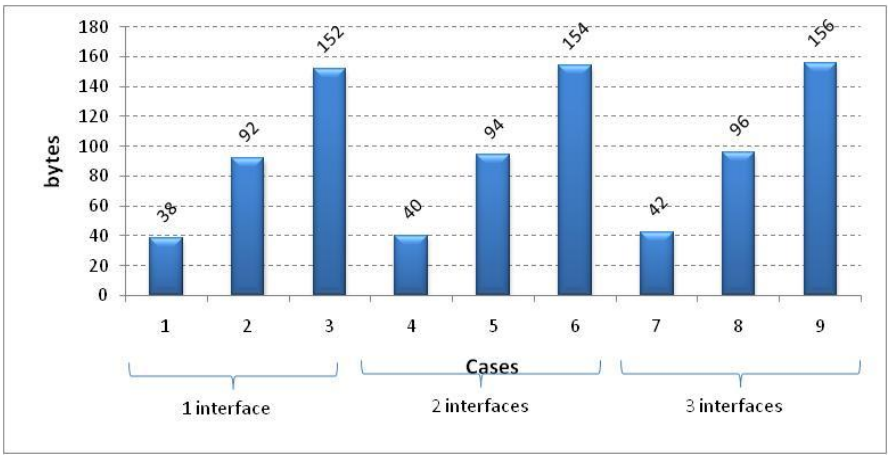

Figure 35: Estimated sizes of Terminal_Decisions according to the 802.21 specification.

Finally, ON_Knowledge data structure conveys selected information from the BS_Context, Terminal_Context, ON_Decisions, Infrastructure_Decisions or Terminal_Decisions. To that respect, the size of this data structure is linked to the sizes of the aforementioned context or decision structures. The aforementioned data structures will be conveyed through the messages defined in the MSCs.

As introduced in the C4MS messages format definitions (see section 1 in the Appendix to D3.3 [10]) each message contains mandatory and optional fields. The following table (Table 10) lists some of the considers parameters and estimates sizes of the fields that are used in the C4MS messages.

Table 10: C4MS parameters and their sizes considered in the message size estimation

Parameter	Remarks	Size (bytes)
Requested_Information	N/A	4
Reason	N/A	2
Result_Code	N/A	2
ON_ID	N/A	8

Negotiation_ID	N/A	2
single Policy	N/A	170
Notification_Event_Type	N/A	1
Termial/BS_Profile	2 radio interfaces	71
User profile	2 radio interfaces 1 supported application 3 quality levels supported	73
Terminal_Context	1 supported application 2 links for a terminal 0 multimedia parts 0 ON-Capable neighbours	224
BS_Context	0 supported ONs 0 multimedia parts 1 ON-Capable terminal connected to the BS	341
ON_decisions	2 links in the ON	119
Infrastructure_decisions	2 interfaces 1 served terminal 0 multimedia parts	**33**
Measurement_Report	Size of measurement 15	20

Fields specified in the table above constitute the C4MS messages. The cumulative sizes of messages (with a specification of the content of each message) are presented in Table 11.

Please note that optional parameters that are not included in the message are omitted for clarity. For a comprehensive definition of C4MS messages please examine Appendix to D3.3 [10] section 1. Be advised, that additionally to the conveyed parameters, each message contains a 6B (fixed size) header (for header definition and format please refer to section 2.2.1).

Table 11: Exemplary C4MS message sizes

Message Type	Content	Size (bytes)
INR	[Source C4MS ID] [Destination C4MS ID] { Requested Information }	20
INA	[Source C4MS ID] [Destination C4MS ID] { Result Code } [Information Container -> Terminal Proifle]	85
INI	[Source C4MS ID] [Destination C4MS ID] { Information Container -> Terminal_Context }	242
ONSI	[Source C4MS ID] [Destination C4MS ID] { Reason } [Context -> Terminal_Context]	252
ONNR	[Source C4MS ID] [Destination C4MS ID] { Negotiation_ID } { Reason }	363

	{ Context -> BS_Context }	
ONNA	[Source C4MS ID] [Destination C4MS ID] { Negotiation_ID } { Result_Code } { ON_ID }	28
ONCR	[Source C4MS ID] [Destination C4MS ID] { Creation_Reason } { ON_ID } { Decisions -> Terminal Decisions }	59
ONCA	[Source C4MS ID] [Destination C4MS ID] { ON_ID } { Decisions -> ON_decisions }	139
ONMR	[Source C4MS ID] [Destination C4MS ID] { Reason } { ON_ID }	26
ONMA	[Source C4MS ID] [Destination C4MS ID] { Result_Code } { ON_ID }	26
ONRR	[Source C4MS ID] [Destination C4MS ID] { Reason } { ON_ID }	26
ONRA	[Source C4MS ID] [Destination C4MS ID] { Result_Code } { ON_ID }	26
ONSN	[Source C4MS ID] [Destination C4MS ID] { Notification_Event_Type } [Context -> BS_Context -> Terminal_Context]	584

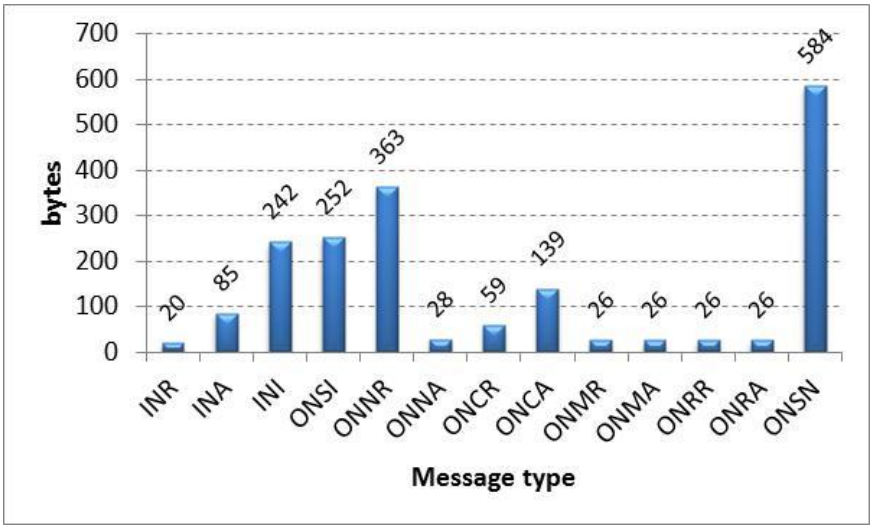

Figure 36: Estimated sizes of exemplary C4MS message types.

5.1.5 Signalling evaluation

The following table summarizes the results of analytical evaluations of the control traffic generated during the ON Suitability determination phase in different OneFIT scenarios based on the final version of the MSCs presented in the Appendix to D3.3 [10].

Table 12: Suitability phase signalling load results

OneFIT scenario	#1			#2a		#2B	#3			#4			#5
Approach	Terminal centric		Network centric	Network centric	Terminal centric	Network centric	Terinal. Centric		Network Centric	Terminal centric		Netw. centric	N/A
Case	network supported	terminal initiated	N/A	N/A	N/A	N/A	terminal initiated	network initiated	N/A	network supported	terminal initiated	N/A	N/A
	Signalling load [B]												
CI interface	679	162	1469	0	1255	24	518	1002	194	795	467	1074	359
OM interface	0	0	0	0	0	0	0	0	0	0	0	0	0
Other interface	0	0	0	1034	0	1028	0	0	0	0	0	0	0
Total	**679**	**162**	**1469**	**1034**	**1255**	**1062**	**518**	**1002**	**194**	**795**	**467**	**1074**	**359**
term-term	467	162	403	0	627	0	160	467	0	467	467	467	0
Term-netw	77	0	463	0	262	24	10	10	36	40	0	501	0
netw-term	135	0	250	0	103	10	348	525	158	288	0	106	0
netw-netw	0	0	347	1034	262	1028	0	0	0	0	0	0	359

The following table summarizes the results of analytical evaluations of the control traffic generated during the ON Creation phase in different OneFIT scenarios.

Table 13: Creation phase signalling load results

OneFIT scenario	**#1/#4**		**#2a**		**#2b**	**#3**		**#5**
approach	**Terminal centric**	**Network centric**	**Network centric**	**Terminal centric**	**Network centric**	**Terminal centric (terminal initiated)**	**Network Centric**	**Network centric**
	Signalling load [B]							
CI interface	0	0	0	0	0	637	841	0
OM interface	1204	1096	587	982	696	430	0	545
Total	**1204**	**1096**	**587**	**982**	**696**	**1067**	**841**	**545**
term-term	428	535	**0**	428	268	430	**0**	**0**
Term-netw	394	34	16	394	34	599	299	0
netw-term	34	511	143	34	394	38	542	0
netw-netw	348	16	428	126	0	0	0	545

The following table summarizes the results of analytical evaluations of the control information which is exchanged during the ON maintenance phase.

Table 14: Maintenance signalling load results

OneFIT Scenario	**#1/#4**					**#2a**	**#2b**	**#3**		**#5**	
approach	**Generic ON paramteres modification**	**Gateway handover**	**BS handover**	**ON participant disconnection**	**Gateway disconnection**	**Network centric approach**	**Network centric approach**	**Terminal centric approach (terminal initiated)**	**Network Centric**	**ON parameters modification**	**ON participant disconnection**
	Signalling load [B]										
CI interface	0	231	1477	253	253	0	0	279	833	348	348
OM interface	816	243	618	40	40	587	159	626	0	159	40
Total	**816**	**474**	**2095**	**293**	**293**	**587**	**159**	**906**	**833**	**508**	**388**
term-term	408	401	697	166	166	0	0	626	0	0	0
Term-netw	378	57	0	126	126	16	16	241	538	0	0
netw-term	30	16	697	0	0	143	143	38	295	0	0
netw-netw	0	0	701	0	0	428	0	0	0	508	388

The following table summarizes the results of analytical evaluations of the control information which is exchanged during an ON termination and after an ON is terminated.

Table 15: Termination phase signalling evaluation

scenario	**#1/#4**	**#2a**	**#2b**	**#3**	**#5**
approach	**N/A**	**Network centric approach**	**Network centric approach**	**Terminal centric approach (terminal initiated)**	**Network centric**

	Signalling load [B]				
CI interface	0	0	0	231	0
OM interface	90	80	40	268	40
Total	**90**	**80**	**40**	**500**	**40**
term-term	50	0	0	268	0
Term-netw	24	16	16	231	0
netw-term	16	24	24	0	0
netw-netw	0	40	0	0	40

5.1.6 Summary

The following section provided analytical analysis of the signalling load generated by different ON related procedures. The analysis was conducted based on the MSCs presented in the Appendix to D3.3 [10] and allowed us to determine the theoretical upper bounds[12] on the signalling overhead for different OneFIT scenarios in different phases. In general the analysis indicates that (for the considered scenario settings) the ON management does not introduce excessive signalling. In order to better understand the scale of the ON management signalling, the overhead introduced by L1/L2 protocols in an LTE cell[13] is presented in Table 16. Considering (for the purpose of comparison) the set of ON related procedures which generate the highest overhead on the interface between network and terminal (see Table 17), and assuming that terminals are on a cell edge (worst case scenario)[14], the average overhead generated in the uplink and downlink would not exceed 2.34% and 2.23% respectively. This simple example shows that the ON related overhead in the worst case scenario is 10 times smaller than the L1/L2 signalling overhead in LTE. Moreover, as the analysis was conducted to determine the upper bound of the signalling overhead, it needs to be underlined that the amount of the exchanged data may significantly decrease for some scenarios (e.g. some information may already be available from the previous encounters or from the RAT-specific procedures running in the background).

Table 16: L1/L2 protocol overhead for LTE FDD Rel. 8 [38]

Uplink		Downlink	
Total number of Resource Elements (10Mhz, 10ms)	84000	Total number of Resource Elements (10Mhz, 10ms)	84000
PUCCH (4 PRB per 10MHz)	8.00%	DL control channels (L=3 OFDM symbols per subframe)	21.42%
DM-RS	14.28%	CRS (1 antenna port)	3.57%
SRS (full-bandwidth, 10ms period)	0.68%	Synchronization signals	0.34%

[12] No information is reused from the RAT-specific procedures, terminals encounter themselves for the first time

[13] The overhead was calculated for typical system settings, over a 10 ms radio frame for a 10 MHz system bandwidth

[14] CQI index 1 - QPSK modulation with ECR (Effective Coding Rate) equal to 0.076 [38]

PRACH (6 PRB, 10ms period)	1.20%	PBCH	0.29%
Total overhead	**24.16%**	**Total overhead**	**25.62%**

Table 17: Estimated ON signalling for a worst case scenario

ON related procedure	Uplink load	Downlink load
Suitability determination	501 B (SCE#4 procedure)	525 B (SCE#3 procedure)
Creation	599 B (SCE#3 procedure)	542 B (SCE#3 procedure)
Maintenance	538 B (SCE#3 procedure)	697 B (SCE#1 procedure)
Release	231 B (SCE#3 procedure)	24 B (SCE#2a procedure)
Total overhead	**14.95 kbps**[15]	**14.30 kbps**[15]

5.2 Initialization phase signalling evaluation

The following subsections cover aspects related to the evaluation of the control information which is required to be exchanged to enable the ON operation. In general the section identifies information which needs to be delivered before the ON suitability determination phase, estimates the size of C4MS or RAT specific messages which carry this information and provides the analysis of the load introduced by the ON management related traffic (given different settings of available information management strategies).

The following evaluations are valid for the OneFIT scenarios 1, 2, 3 and 4 (in case of scenario 5, ON related information exchanged during the initialization phase is assumed to be pre-deployed in the nodes).

5.2.1 Evaluation model

In the following evaluation the number of nodes in the network is not specified, instead we use a Poisson process to model arrival of terminals to the network. Overhead introduced by the lower layers is not considered in the evaluation. An error-free channel with the same capacity for each terminal is assumed.

Additionally, we assume that the information offered by terminal/BS/network does not alter over the evaluation period. This allows us to omit situations in which events related to the information change trigger the information transmission. In our view this is a reasonable assumption as policies, BS profiles, Terminal profiles and User profiles are more likely to change over longer periods of time.

5.2.2 Verification scenario for the initialization phase

As presented in the Message Sequence Chart below (see Figure 37), the initialization phase can be subdivided into three main steps:

[15] Assuming that each ON related procedure is triggered once per second

1. RAT specific procedures which enable a terminal to discover and attach to the network. As these procedures are not triggered by ON related mechanisms, they are not considered to be a part of ON related signalling. It is worth to underline here that information obtained using these procedures (e.g. approximate location of terminals) can be used for the purpose of the ON operation.
2. Delivery of ON related information from the BS to the Terminal. The messages used for this purpose may convey information related to the most important policies, profile of a BS (or profiles of neighbouring BSes), depending on the employed information management strategy.
3. Delivery of Terminal related information (Terminal and User Profile) to the BS. Depending on the information management strategy, information can be pushed by the Terminal or pulled by the BS,

For the purpose of the signalling evaluation it is assumed that in the considered verification scenario the Base Station supports three radio access technologies (e.g. LTE, HSPA, GSM) and is operated by a single network operator (each RAT is assumed to support two distinct radio bands). Additionally, it is assumed that each BS supports two types of spectrum sensing techniques. The terminal, similarly to the BS, is assumed to support three RATs (e.g. LTE, HSPA and GSM) and two sensing techniques. The content and size of messages exchanged during different steps of the initialization phase vary depending on the applied information management strategies.

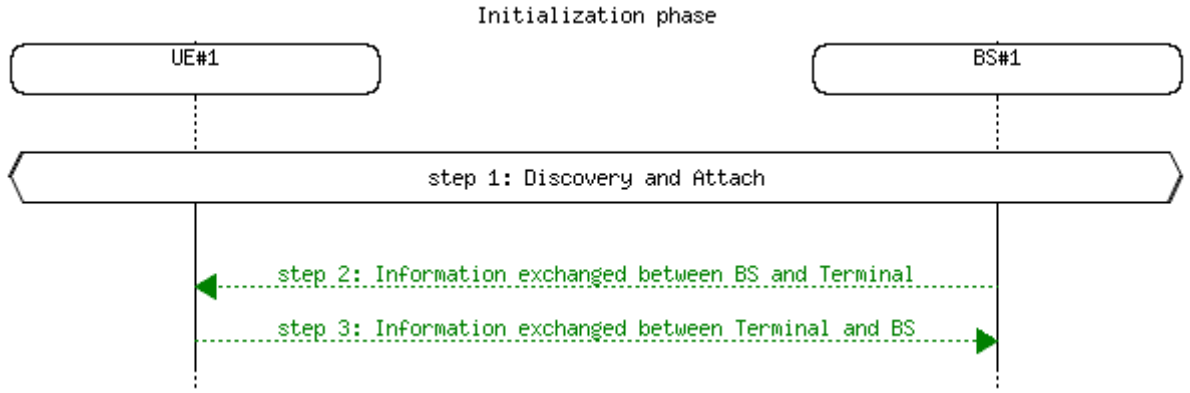

Figure 37: Initial stage, applicable to all scenarios

5.2.3 Information management strategies

The amount of information exchanged between terminals and the infrastructure strongly depends on the information management strategies employed in the network. The following subsection provides details on the strategies which are to be evaluated for the purpose of signalling load estimation for the initialization phase.

The following information management strategies (IMS) shall be considered for the signalling evaluation during the initialization phase for the second step:

- IMS#1 – BS periodically broadcasts the ON related information towards terminals over a broadcast channel – periodical information push
- IMS#2 – BS broadcasts the ON related information at a Terminal arrival or at ON related information update. The information is broadcasted over a broadcast channel in the next broadcast period – event-driven information push.

- IMS#3 – BS periodically broadcasts meta-data generated based on the currently possessed information[16]. If new piece of information is available, terminal determines it by examining the meta-data and it informs the BS to include the missing pieces of information in the next broadcast period.
- IMS#4 – Terminal requests the ON related information from the BS on its arrival by sending meta-data generated based on its currently possessed information. The information is delivered to the Terminal over a dedicated (unicast) channel – event-driven information pull.

The following information management strategies shall be considered for the signalling evaluation during the initialization phase for the third step:

- IMS#5 – BS requests the ON related information (e.g. User or Terminal Profile) from a terminal on its arrival by sending meta-data generated based on currently possessed information. The information is exchanged over a dedicated channel – event-driven information pull.
- IMS#6 – Terminal delivers the ON related information to the BS on its arrival to the network. The information is exchanged over a dedicated channel – event-driven information push.
- IMS#7 – Terminal delivers meta-data generated based on the possessed ON related information to the BS. The BS requests the ON related information, if new information is available. The information is exchanged over a dedicated channel – publish and pull.

The signalling load for the discussed methods of information exchange will be presented in the subsequent section. It is worth to underline here that as the first step of the initialization phase (i.e. network discovery and network attachment) is RAT specific and that it is not triggered by ON related algorithms/mechanisms, it is not considered for further evaluation.

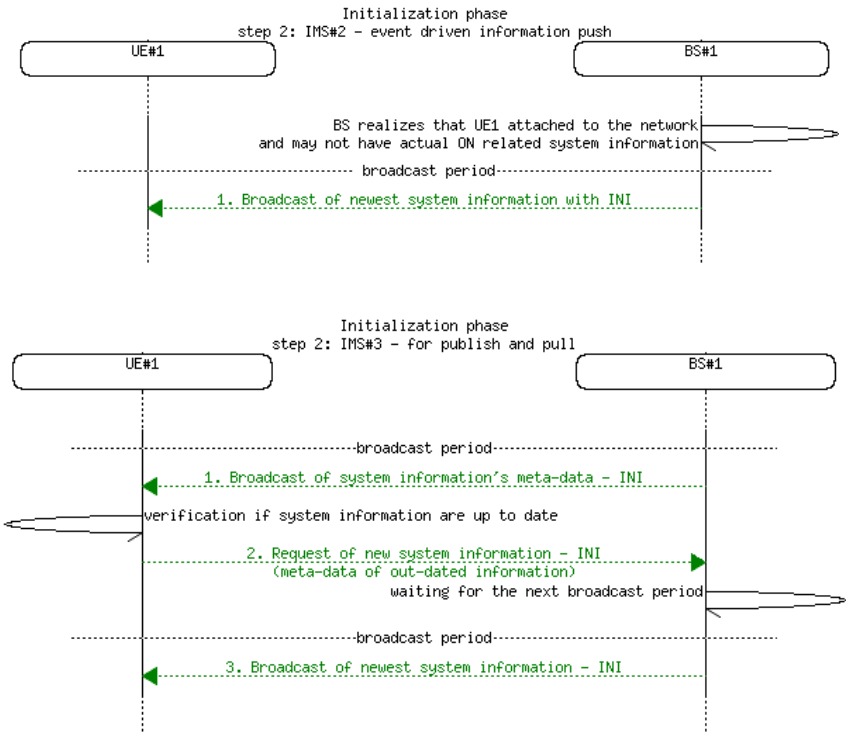

Figure 38: Example Information management strategies for initialization

[16] Meta-data is an extract of a data that unequally describes it, however has substantially smaller size.

5.2.4 Signalling message size estimations

The sizes of messages (and thus the amount of information) exchanged between terminals and BSes strongly depend on the actual context and network configuration and thus differs on the scenario basis. Some possible message sizes for INI, INR and INA are presented in Table 18.

It is worth to underline here that the estimated sizes do not include the overhead introduced by the lower layers and are based on the C4MS data structures introduced in Section 3 (and depicted in detail in the Appendix document (see Section 3)). In order to estimate the sizes of the messages the following assumptions are made: 1) three distinct ON related policies needs to be delivered to terminals, 2) BS and terminals are employed with the same number of RATs, 3) BS and terminals support two spectrum sensing techniques.

Table 18: Estimated average message size

C4MS Message Type	Message size [B]
IMS#1 and IMS#2	
Information Indication (INI)	138 + 510
IMS#3	
1. Information Indication (INI)	120
2. Information Indication (INI)	0/30/60/90/120
3. Information Indication (INI)	0/138 + 0/170/340/510
IMS#4	
Information Request (INR)	120
Information Answer (INA) (in case no new information is available)	120

5.2.5 Signalling load evaluation

The following section focuses on the evaluation of signalling introduced by the procedures conducted during the initialization phase. The section focuses on the last two steps of the initialization phase (see Section 5.2.2 for more detail), evaluating different schemes for delivering the necessary information.

5.2.5.1 Downlink overhead evaluation for the second step of the initialization phase

In the first test we consider evaluation of IMS#1 and IMS#2 (see Section 5.2.3 for more details on IMS#1 and IMS#2). To simplify, we assume that the information offered by the BS/network does not alter over the simulation time (this allows us to omit situations in which events related to the information change trigger the information broadcast). In our view this is a reasonable assumption as policies and BS profiles are more likely to change over longer periods of time rather than short. The results obtained for the first test are depicted in Figure 39.

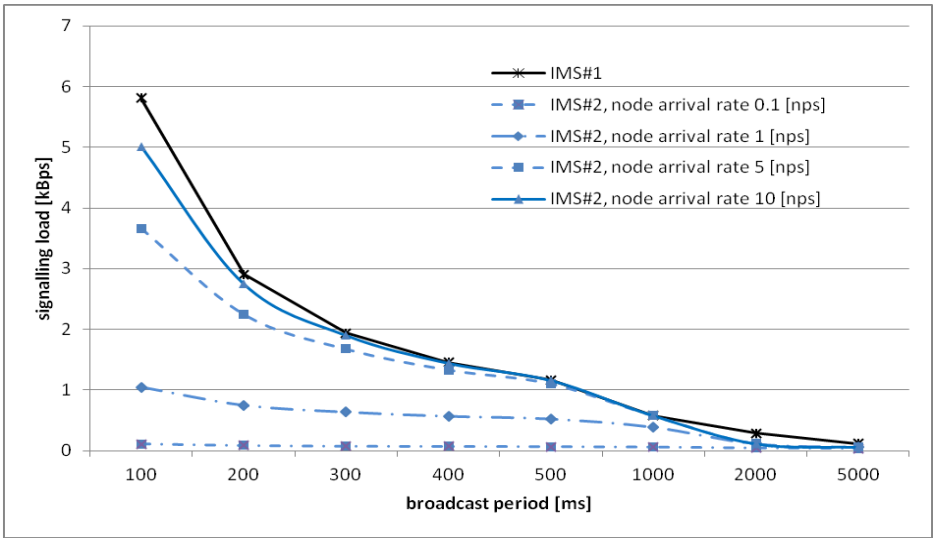

Figure 39: Signalling load generated during the initial stage for step 2 by IMS#1 and IMS#2.

As expected, signalling load for both schemes decreased with the increase of the broadcast period. What is worth noting is that the level of signalling load for IMS#2 increases with the node arrival rate and tends to the signalling level introduced by the periodical broadcast (i.e. IMS#1). This indicates that for a certain node arrival rate the ON related information is broadcasted every broadcast period. Although the results obtained in this experiment suggest that IMS#2 is at least as good as the periodical broadcast, it needs to be underlined that the usage of IMS#2 may cause some terminals in the network to have inconsistent/invalid information for significantly longer periods of time than in case of IMS#1. This can be especially seen in scenarios with a low node arrival rate. In such scenarios terminals which failed to receive the necessary information at their arrival to the network (e.g. due to different random transmission errors) could be forced to operate without valid ON related system information, until arrival of a new node.

In the second test, similarly to the first test, two distinct information management strategies are considered for evaluation, namely IMS#2 and IMS#3 (see Section 5.2.3 for more details on IMS#2 and IMS#3). As in the previous test, the evaluation is conducted for a scenario in which information offered by the BS/network does not alter over the simulation time.

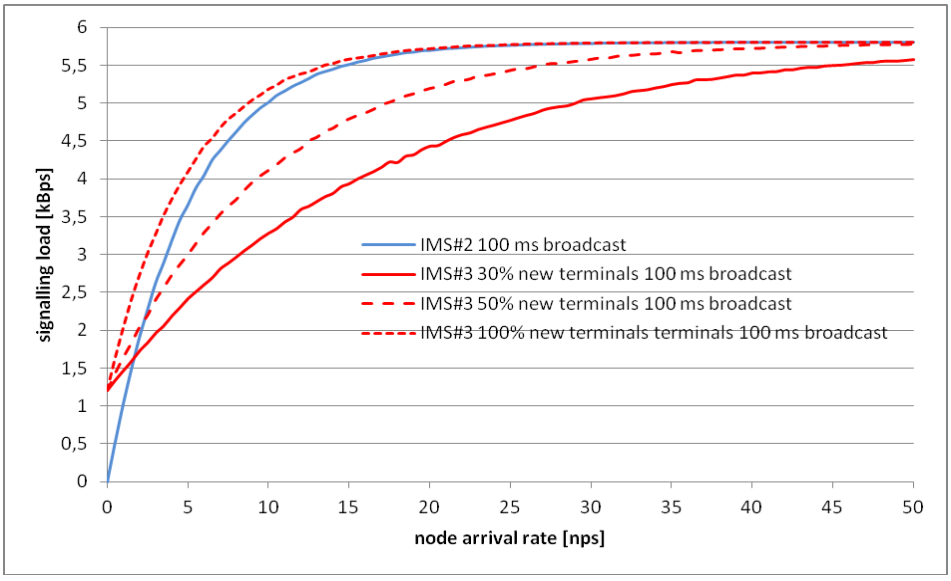

Figure 40: Signalling load generated during the initial stage for step 2 by IMS#2 and IMS#3.

As seen in the figure, the performance of the IMS#3 strongly depends on the arrival rate of “new terminals” (i.e. terminals with the out-dated information). Assuming that there are finite numbers of

terminals and that the information offered by the BS/network does not alter very often, the arrival rate of "new terminals" should decrease over time. This indicates that although IMS#3 shows worse performance for some scenarios (due to the additional overhead related to the periodical transmission of meta-data), it may provide better overall results in terms of the signalling load than IMS#2. Additionally, it is worth noting that unlike IMS#2, IMS#3 does not suffer from the reliability problem, as indicated in the previous test. It is also worth to underline here that the results for IMS#3 may differ depending on the difference between the actual size of the information which needs to be transmitted and the size of the meta-data[17] which is generated based on this information (the larger the difference the better the results).

In the third test we evaluate IMS#3 and IMS#4. Similarly to the previous tests, in order to simplify we assume that the information offered by the network does not change over the simulation time. Figure 41 depicts the results obtained for the third test.

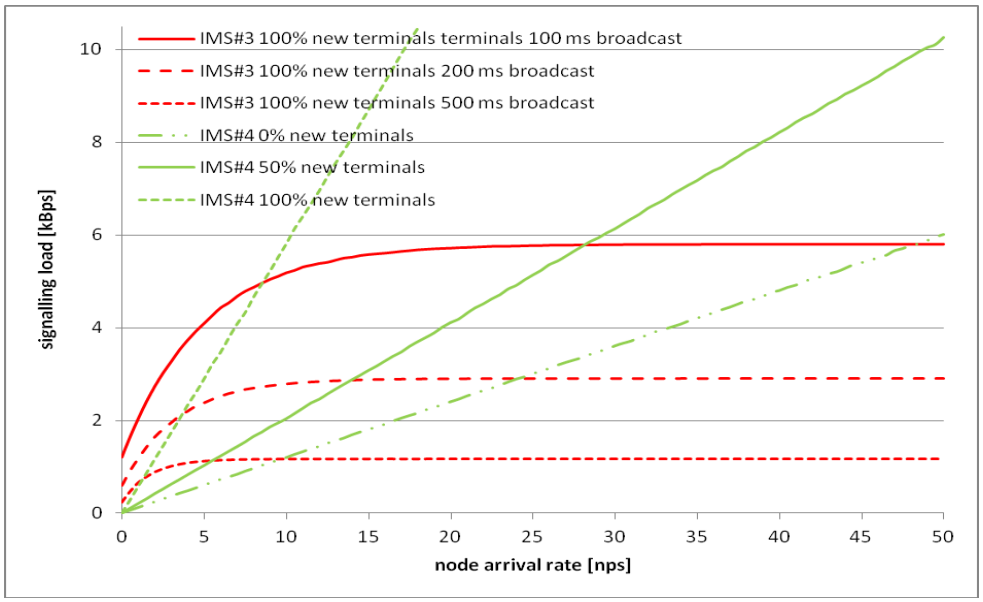

Figure 41: Signalling load generated during the initial stage for step 2 by IMS#3 and IMS#4

As seen in the figure, the signalling load introduced by IMS#4 increases with the node arrival rate and unlike the other schemes it does not have an upper bound. This is mainly caused by the fact that the information is exchanged over a dedicated channel (BS responds to every request received form terminals)[18]. The obtained results show that, depending on the node arrival rates, either IMS#4 or IMS#3 performs better. This indicates that both IMSes could be potentially employed in the network and could be dynamically selected based on the node arrival rate experienced in the network. It is worth to underline here that the threshold value of the node arrival rate which is used to select the most appropriate IMS depends on the size of the ON related information to be transmitted, the information update period and thus may be different for different scenarios.

5.2.5.2 Uplink overhead evaluation for the second step of the initialization phase

In the last test related to the second step of the initialization phase the signalling overhead introduced in the uplink direction was evaluated. As IMS#1 and IMS#2 do not introduce any uplink overhead, they were not considered during this test.

[17] For the purpose of this evaluation the meta-data was assumed to be about 20% of the size of the actual data.

[18] It was assumed that even if a terminal has up-to-date information, it receives a confirmation which includes the meta-data

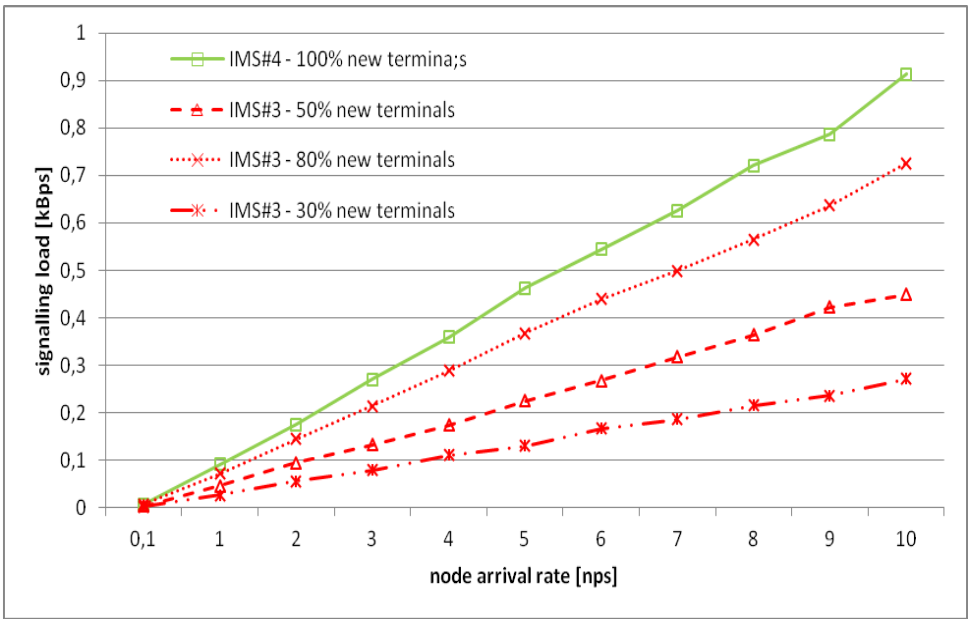

Figure 42: Uplink signalling load during the initial stage for step 2

As seen, the overhead in case of IMS#3 depends on two parameters, i.e., the node arrival rate and the arrival rate of "new terminals" (i.e. terminals with the out-dated information), whilst IMS#4 depends solely on the node arrival rate. This is basically caused by the fact that, in case of IMS#4, terminals are not aware of the information which is in the possession of the network and thus need to send requests each time after they join the network. This is not the case with IMS#3 in which the BS periodically broadcasts meta-data which is generated based on the possessed information.

It is worth to underline here that, although not shown in the test, the uplink overhead depends also on the number of pieces of information which needs to be delivered to the terminal. In case of IMS#3 the size of the request messages changes then depending on the number of new pieces of information which could be requested from the network. Although IMS#3 is at least as good as IMS#4 in terms of uplink overhead and thus seems to outperform IMS#4, it needs to be underlined that the usage of IMS#3 may potentially cause a temporal overload in the network. Such a situation may appear in case multiple "new terminals" join the network in the same broadcast period. In such a case requests will be sent by terminals almost at the same time instant, potentially causing an overload.

5.2.5.3 Downlink overhead evaluation for the third step of the initialization chase

In the first test related to the third step of the initialization phase evaluation of IMS#5 and IMS#7 in the downlink direction is considered (see Section 5.2.3 for more details on IMS#5 and IMS#7). As IMS#6 does not introduce any downlink overhead, it was not evaluated during this test. The obtained results are depicted in figure below.

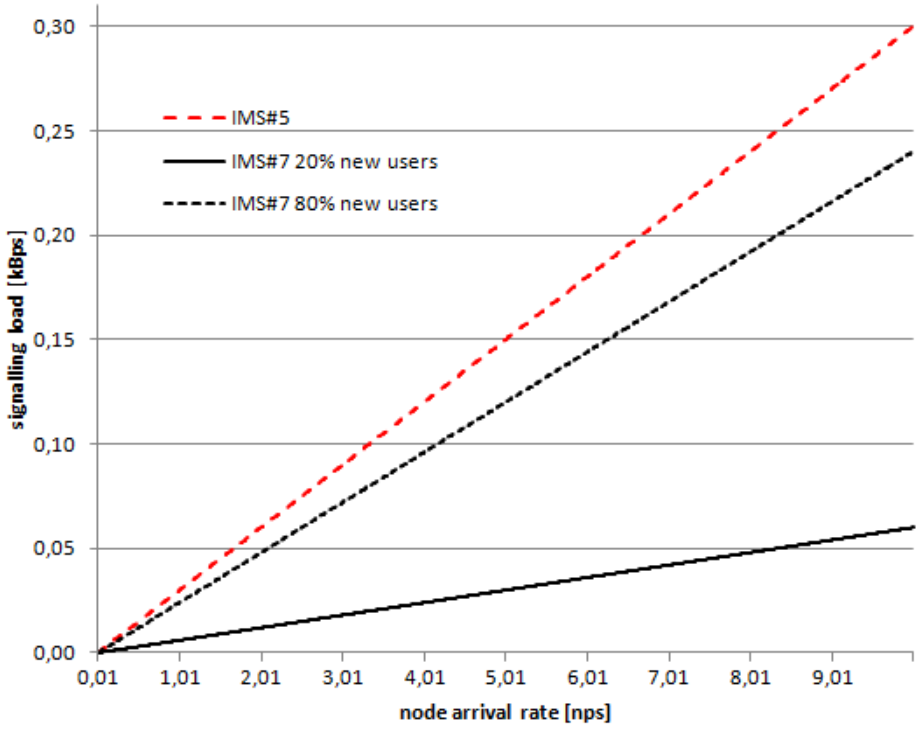

Figure 43: Downlink signalling load for the third step

As seen, the overhead increases linearly with the node arrival rate. Such dependency is specific to strategies which employ dedicated channels for information exchange. The difference between IMS#5 and IMS#7 which can be observed in the Figure is related to the fact that in IMS#5 the network is not informed whether it has the up-to-date information on User and Terminal Profiles. Upon terminal arrival the network requests then all potentially required information by piggybacking meta-data generated based on the already possessed information. In contrast to IMS#5, in case of IMS#7 the network receives (upon terminal arrival) information about the Profiles possessed by terminals and thus is capable to determine which pieces of Profile information are missing or are out-dated and need to be requested.

Similarly to the previous tests, it is worth to underline that the overhead in case of IMS#7 depends also on the number of pieces of information which needs to be delivered to the terminal (the size of the request message may change depending on the number of new pieces of information which could be requested from the network).

5.2.5.4 Uplink overhead evaluation for the third step of the initialization phase

In the second test related to the third step of the Initialization phase evaluation of IMS#5, IMS#6 and IMS#7 (see Section 5.2.3 for more details on IMS#5, IMS#6 and IMS#7) was considered. The obtained results are presented in the figure below (see Figure 44).

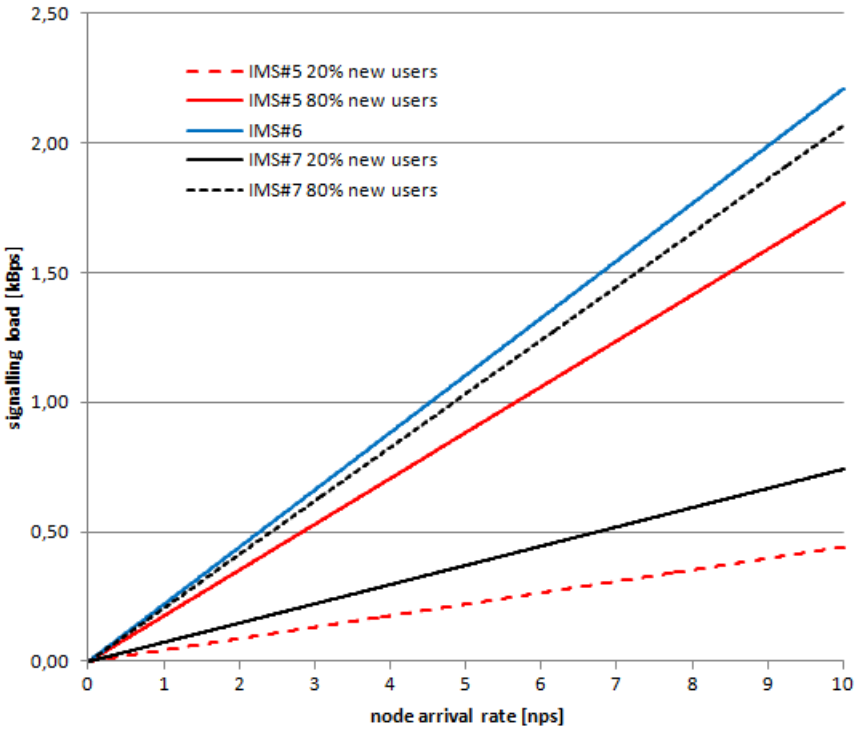

Figure 44: Uplink signalling load for the third step

Similarly to the overhead in downlink direction, the overhead in the uplink direction increases linearly with the node arrival rate. Additionally, in case of IMS#5 and IMS#7, overhead depends also on the arrival rate of "new terminals" (i.e. terminals with the out-dated information). This is not the case with IMS#6 in which terminals are not aware of the information which is in the possession of the network and thus send all the necessary information after they join the network. In contrast to IMS#6, in IMS#5 the network informs terminals (upon their arrival) about the possessed information (meta-data generated based on the possessed information). This allows terminals to determine which pieces of information need to be delivered. Similarly, in case of IMS#7, terminals (upon their arrival) inform BS about the version of information which is currently in their possession (meta-data generated based on the possessed information). This allows the BS to request only the missing or out-dated pieces of information from the terminal.

Similarly to the previous tests, the overhead in case of IMS#7 depends also on the number of pieces of information which needs to be delivered by the terminal (the size of the request message may change depending on the number of new pieces of information which could be requested from the network).

5.2.5.5 Signalling delay considerations for the initialization phase

Although the signaling delay is not explicitly evaluated in this section, the following upper bounds were determined:

- The maximum delay of the "second step" procedures for IMS#1 and IMS#2 is not greater than the broadcast period + the time necessary to transmit the necessary information over a broadcast channel,
- In case of IMS#3 the delay is not greater than two broadcast periods + the time necessary to transmit the necessary information over a broadcast channel and not shorter than a single broadcast period + the time necessary to transmit the necessary information over a broadcast channel,
- In case of IMS#4 (as well as IMS#5 for the "third step"), the delay was estimated not to be shorter than the RTT of the C4MS INR/INA procedure,

- In case of IMS#6 the delay was estimated not to be shorter than the time which is necessary to transmit required information over a dedicated channel using the C4MS INI procedure,
- In case of IMS#7 the delay was estimated to be not shorter than the time which is necessary to transmit meta-data information over a dedicated channel using the C4MS INI procedure and the RTT of the C4MS INR/INA procedure.

5.2.6 Summary

The following section provided a general analysis of signalling overhead related to provision of information during the Initialization phase which is necessary to enable Opportunistic Networking (i.e. policies and profiles). The analysis was conducted for the interface between terminal and infrastructure and included evaluation of different Information Management strategies. In general, the obtained results indicate that the overhead introduced by the transmission of information depends on the size of information to be transmitted, transmission period and rate of terminal arrival in the network. It was also shown that for some strategies the signalling overhead can be reduced by enabling system to distinguish between nodes which have up-to-date and out-of-date information (such differentiation can be achieved by introducing additional constant signalling overhead in uplink [in case of step 2] and downlink [in case of step 3]).

In order to better understand the scale of the signalling overhead introduced by the transmission of information during the initialization phase, the overhead generated by the transmission of System Information[19] in an LTE cell is presented in the following table[20].

Table 19: System Information Block overhead calculated over 20ms and for a 10 MHz system bandwidth for LTE FDD Rel. 8 [26]

	MIB	SIB1	SI-1 (SIB2 and SIB3)	SI-2 (SIB4)
Transmission period	10ms	20ms	20ms	20ms
Estimated message size	14 bits	26 bytes	43 bytes	63 bytes
Default MCS	n/a (72 subcarriers, 4 OFDM symbols)	5	5	5
Partial overhead	0.29%	0.3%	0.5%	0.6%
Total overhead	1.69%			

Assuming that: 1) the default MCS for ON related information is also equal to 5, 2) the amount of information which needs to be delivered to the terminal in a worst case scenario for step 2 (i.e. terminal requires all policies and profiles to be delivered) is equal to 648 Bytes, 3) ON related information is not as critical as delivery of System Information in LTE networks and thus can be transmitted with higher transmission period, the ON related overhead equals 6% for 20ms period, 2.4% for 50ms period, 1.2% for 100ms period. This simple example shows that (for higher

[19] Information transmitted during the initialization phase seem to have a similar purpose as System Information in LTE

[20] The overhead was determined for an example configuration and may vary depending on various parameters

transmission periods) transmission of information during the second step of Initialization phase could be potentially possible over the BCCH channel in an LTE network[21].

5.3 Security related signalling evaluation

The following subsection covers aspects related to the evaluation of the traffic load which is generated by the security mechanisms employed during different phases of the ON operation. The section identifies pieces of information which are to be exchanged, estimates the size of messages that carry these sets of information and provides the analysis of the traffic introduced by the messages (given different possible information management strategies).

5.3.1 Evaluation model

The evaluation of C4MS security related signalling focuses on the evaluation of signalling related to the subscriber certificate enrolment and the evaluation of IEEE 802.1X (EAPOL) based solutions in the context of security provisioning between nodes in the OneFIT scenarios (two EAP methods, namely EAP-IKEv2 and EAP-TLS, are evaluated).

The signalling evaluation is mainly based on the analytical calculations of the overhead of the protocols specified as EAPOL [20], EAP-IKEv2 [13], and EAP-TLS [15] and GAA related mechanisms [21] and [22]. An example configuration of the underlying security protocols is considered in section 5.3.4 .

In our evaluation we assume that the secured connection needs to be set up between users which belong to the same operator. In such a case (and assuming that users use the subscriber certificates signed by the operator), we consider the operator to be an acceptable Certificate Authority for both users (the intermediate CA are not involved thus the exchange of additional certificates between the involved users is not required). For the purpose of signalling evaluation between terminals we also assume that the root certificate (i.e. certificate used by the operator to sign subscriber certificates) is already deployed in all terminals (root certificates usually have a long validity period [e.g. 1 year], thus their impact on the signalling can be neglected).

In order to accurately evaluate the signalling load incurring with different security mechanisms we use two signalling load metrics: average system signalling cost, and total expected node signalling cost. The first metric is used to quantify the signalling cost that occurs on a system-level, when nodes need to obtain subscriber certificates from the infrastructure. While, the second metric quantifies the signalling cost that is generated by a node that creates ONs with other Onefit nodes.

It is worth highlighting that in this section we do not take into consideration the overhead introduced by the link layer (this includes TCP/IP connection setup required for issuing subscriber certificates). Furthermore, in the following section we do not consider overhead introduced by exceptional cases (e.g. mutual authentication failure). .

5.3.2 Verification scenario

Two verification scenarios are considered for the evaluation of the security related signalling. The first scenario focuses on the aspects related to the certificate enrolment procedure, i.e. terminal requesting from the operator certification of its public key). The scenario is composed of mobile terminals which communicate with a BSF and a PKI portal via a Base Station, over a long range interface (e.g. LTE). The second scenario focuses on the aspects related to the establishment of a secured connection between mobile terminals (particularly it relates to the handshake procedures).

[21] Assuming a special case of IMS#3 in which only the first INI message is transmitted over the BCCH, the overhead could be further reduced

The scenario is composed of mobile terminals which are equipped with short range radio interfaces (e.g. WiFi) and which are in each other's vicinity.

5.3.3 Information exchange strategies

As the overhead of the procedure related to obtaining a subscriber certificate by a user from the infrastructure can be considered as constant[22], the overall overhead depends on the subscriber certificate validity period. Depending on the employed information management strategy, the subscriber certificate is required to be obtained either 1) at the expiration of its validity period (IMS#1) or 2) when a secured connection needs to be established and the available certificate is out-dated (IMS#2).

For the purpose of the certificate distribution and key establishment (i.e. handshake procedure) two additional information management/exchange strategies could be proposed. In the first strategy (IMS#3), terminals are required to initiate the handshake procedures as soon as they detect a new ON capable terminal in their neighbourhood. In case of the second strategy (IMS#4), terminals initiate the handshake procedures only if a secured connection is required (e.g. before the ON negotiation procedure). The rationale behind IMS#3 is based on the assumption that at some point in time neighbouring terminals may be willing to establish an ON and certificate/key distribution would have a negative impact on the ON creation delay. It is worth highlighting that in order to enable the application of IMS#3, the solutions considered for the purpose of securing the C4MS information exchange are required to support session resumption mechanisms (i.e. IKEv2 Fast Reconnect [13] and TLS session resumption [15]) which enable re-establishment of a secured connection using simplified handshake procedures thus limiting the number of messages to be exchanged.

Summarizing, in case of IMS#3 nodes initiate the full handshake procedure exchange at the first encounter, and then continuously (at the end of each resumption period) initiate the simplified procedure to restart the resumption counter. According to IMS#4 the handshake procedure is initiated only upon ON creation and the simplified procedure is not used to reset the resumption timer (nodes are not able to re-establish connection using the simplified procedure after the resumption timer expires).

5.3.4 Signalling message size estimations

The following section focuses on the estimation of message sizes of the existing/proposed security solutions. The following configuration parameters for the underlying security mechanisms are considered for the evaluation:

- Public key certificate: Certificate size[23] – 712 Bytes; Public-key length – 128 Bytes,
- EAP-IKEv2: Nonce size – 136 Bytes; Considered cryptographic algorithms – AES-CBC, HMAC-SHA-96, Diffie-Hellman group 2, PRF-HMAC-SHA1; Number of cryptographic algorithm proposals – 1 (4 transforms); Identification – based on a fully qualified domain name string (30 Bytes); Fast-reconnect Id size – 30 Bytes
- EAP-TLS: Ciphersuit considered – TLS_RSA_WITH_AES_256_CBC_SHA; Number of Ciphersuits considered for selection – 1; Extensions and compression methods – not considered;

Based on the configuration parameters as well as EAP-IKEv2 and EAP-TLS specifications, message sizes as in Table 20 and Table 21are considered.

[22] Assuming constant size of the certificate

[23] A certificate example generated using openssl

Table 20: Example message size for the bootstrapping procedure in EAP-IKEv2

Message	EAP-IKEv2 Message size	EAP-IKEv2 message size for Fast Reconnect
EAP IKE_SA_INIT_Request	370 B	424 B
EAP IKE_SA_INIT_Response	455 B	392 B
EAP_IKE_AUTH_Request	998 B	N/A
EAP_IKE_AUTH_Response	950 B	N/A

Table 21: Example message size for the bootstrapping procedure in EAP-TLS

Message	TLS Message size	TLS Message size for session resumption
Client Hello	43 B	75 B
Server Hello	72 B	72 B
Server Certificate	716 B	N/A
Certificate Request	40 B	N/A
Server Hello Done	4 B	N/A
Client Certificate	716 B	N/A
Client Key Exchange	134 B	N/A
Certificate_Verify	40 B	N/A
Change_Cipher_Spec	1 B	1 B
Finished	16 B	16 B

In order to obtain the subscriber certificate two procedures need to be conducted, namely Bootstrapping procedure and Subscriber Certificate enrolment procedure [22]. The following tables list all messages (along with their estimated sizes) which need to be exchanged between the UE and the infrastructure. Message sizes are computed using examples taken from TS 24.109 [21].

Table 22: Exemplary message sizes for the bootstrapping procedure, based on [21]

Message	Message size
Initial GET request (UE to BSF) – HTTP request	257 B
401 Unauthorized response (BSF to UE) – HTTP response	270 B
GET request (UE to BSF) – HTTP request	449 B
200 OK response (BSF to UE) – HTTP response	590 B

Table 23: Exemplary message sizes for the subscriber certificate enrolment procedure, based on [21]

Message	Message size
Initial enrolment request (UE to PKI portal) - HTTP request	898 B (including PKCS#10 Certification Request[24] – 540 B)
401 Unauthorized response (PKI portal to UE) - HTTP response	300 B
Authenticated enrolment request (UE to PKI portal) - HTTP request	1209 B (including PKCS#10 Certification Request – 540 Bytes)
Delivery of subscriber certificate (PKI portal to UE) - HTTP response	1141 B (including Certificate – 712 B)

5.3.5 Signalling load evaluation

The following table summarizes the total load introduced by the bootstrapping procedure and the subscriber certificate enrolment procedure which are necessary to be conducted in order to issue and deliver the subscriber certificate to the end user.

Table 24: Subscriber certificate enrolment related signalling load for a single request

	Bootstrapping procedure	Subscriber certificate enrolment procedure
HTTP message sizes [B]	1566	3548
number of messages to be exchanged	4	4
Overhead related to IP and TCP [B]	416	416
Total [B]	**5946**	

As mentioned in the previous section, the overhead of the certificate enrolment procedure can be considered as constant. The overall signalling load depends then on the subscriber certificate validity period and is presented in the figure below.

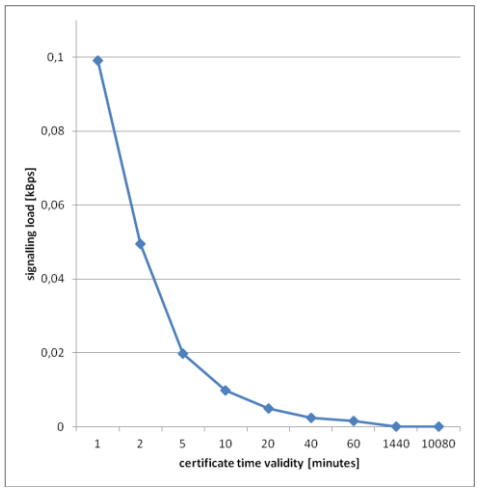

Figure 45: Signalling load generated by a single terminal for different certificate time validity

[24] A certification request example was generated using openssl

As mentioned (see Section 5.3.3), two possible Information Management Strategies could be considered for the subscriber certificate enrolment procedure (i.e. IMS#1 and IMS#2). In order to evaluate the two strategies we calculate signalling cost as an average system cost, which describes the average signalling cost for the whole system consisting of N terminals, each requiring valid certificate. For our system we assume exponential distribution of the probabilities of certificate enrolment (this could correspond to the Poisson distribution of ON creation inter-arrivals), then the probability that the time between the two consecutive ON creations is equal or lower than the certificate validity period takes the form:

$$p_n(\tau \le T_v) = 1 - e^{-\lambda_n T_v}$$

Taking this into account and assuming that nodes in the system will have the same probability distribution functions for ON creation, the expected average system cost criterion for each of the information exchange strategies can be denoted as follows:

$$\gamma_S^{\#1} = NC\lambda_v \qquad \gamma_S^{\#2} = NC\lambda_v(1 - e^{-\lambda_n T_v})$$

Where:

$\gamma_S^{\#1}$, $\gamma_S^{\#2}$ – average system cost for IMS#1 and IMS#2 respecitvely,

N – number of nodes in the system,

C – cost of a single certificate enrolment procedure (see Table 24),

T_v – certificate validity period,

T_n – expected inter-arrival time between any two consecutive ON creations.

The following figure shows the differences in terms of signalling load in kbps between the considered strategies.

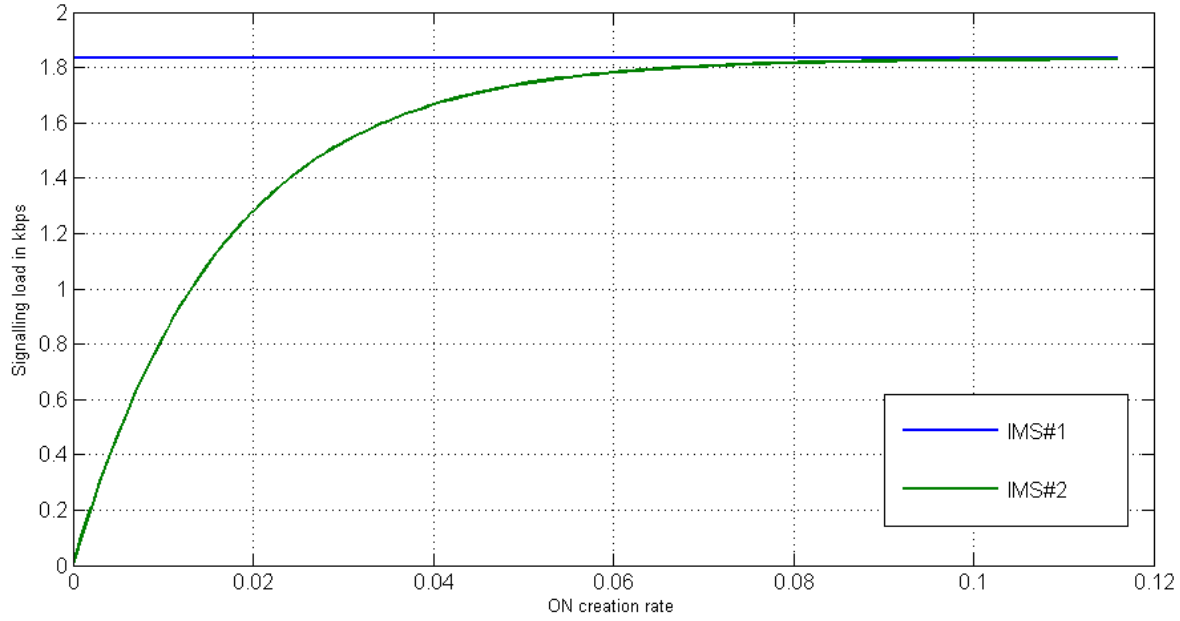

Figure 46: Certificate enrolment related signalling overhead for IMS#1 and IMS#2 for N=20, T_v=60min and C=5.946kB

Although IMS#1 generally leads to higher signalling loads (some terminals may not require the certificate during its validity period), it needs to be stressed that IMS#2 may introduce additional delay to the ON creation, if terminals happen to have invalid certificates. This in turn may result in a

lower probability of successful ON creation[25]. Additionally, usage of IMS#2 may result in short-term peaks in the transmitted traffic (whenever multiple terminals involved in the connection setup require their certificates to be renewed).

Given that all terminals are in the possession of their subscriber certificates, signalling load introduced by the security mechanisms solely depends on the underlying security solutions (in our case 802.1X-EAP-TLS and 802.1X-EAP-IKEv2). Table 25 presents the overhead generated by the considered solutions for the scenario with two terminals during the handshake phase. The calculations are based on the estimated message sizes provided in the previous section as well as sequence charts specified in [13] and [15].

Table 25: IKEv2 and TLS signalling overhead comparison

	EAP-IKEv2	EAP-IKEv2 Fast Reconnect	EAP-TLS	EAP-TLS session resumption
Protocol specific payload (including digital certificates if required) [B]	2717	816	1783	155
number of messages to be exchanged	8	6	10	8
Overhead related to EAPOL and EAP [B]	143	105	150	123
Total	**2860**	**921**	**1933**	**276**

Similarly to the subscriber certificate enrolment procedure, two possible Information Management Strategies could be considered for the establishment of a secured connection between any two terminals (i.e. IMS#3 and IMS#4). In order to compare IMS#3 and IMS#4 let us define the total expected discounted signaling cost for a node in the system, which is based on the total expected discounted cost [39]. The choice of the metric is driven by the need for quantification of the signalling cost reduction that occurs whenever during the resumption time a simplified handshake procedure is conducted instead of the full procedure (see Table 25). The total expected discounted node cost for our system is denoted as a sum of discounted costs at each consecutive time epoch[26] until some indefinite future, the cost at single time epoch will be a sum of the expected costs for handshake procedure with each neighbouring node:

$$\delta_s = \sum_{n=1}^{N} E[C\lambda_n] + \beta \sum_{n=1}^{N} E[C\lambda_n] + \beta^2 \sum_{n=1}^{N} E[C\lambda_n] + \mathrm{L} \ , \beta \in <0,1)$$

Where:

β – the discount factor, that accounts for the stability of the current network neighbourhood, i.e. the probability that the nodes will be stationary after a time epoch

N – number of nodes in the system

[25] Delay related to certificate enrolment as well as probability of successful ON creation were not explicitly analysed in this evaluation

[26] Time period between two system state updates (in our system each time epoch is constant size and is equal to the resumption time)

C – cost of a single full handshake procedure (see Table 25)

λ_n – expected rate of ON creations

For the purpose of the IMS evaluation it is assumed that each ON creation is preceded by a security handshake procedure and ONs are created whenever an application available on one of the nodes requests connectivity. As no assumption is taken about the number of available applications, or the number of connections that each application can generate, the "calling population" is assumed to be infinite (although the number of neighbouring nodes is finite). This in turn allows us to assume that the ON duration has no effect on the ON creation rate. Furthermore, we omit the impact of the ON duration time on the signalling cost[27]. All nodes considered in the scenario are in the range of each other (i.e. they can exchange messages between each other) and their mobility is emulated through β factor, which accounts for the future signalling cost.

Assuming that the ON creation rate does not change from epoch to epoch (with the exception of the zero epoch), the following equation for the total expected discounted node cost in case of IMS#3 can be denoted as:

$$\delta_s^{\#3} = \delta^{\#3}(T_0) + \beta\delta^{\#3}(T_1) + \beta^2\delta^{\#3}(T_2) + \mathrm{L} \ , \beta \in <0,1)$$

$$\delta_s^{\#3}(T_i) = \sum_{n=1}^{N} C_n = fC\sum_{n=1}^{N}(\lambda_n p_n(\tau \le T_r) + p(\tau > T_r)\lambda_r), i \in N^+ , \ \delta_s^{\#3}(T_0) = NC\lambda_r$$

Where:

T_r – resumption period

f – signalling cost reduction factor (ratio between the simplified handshake procedure cost and the full handshake procedure cost)

The expected node cost in any time epoch for IMS#4 is a sum of three factors: 1) the full handshake procedure cost which occurs whenever nodes create an ON for the first time, 2) the full handshake procedure cost which occurs whenever nodes create an ON, and the resumption timer has expired, 3) the simplified handshake procedure cost which occurs whenever nodes create an ON, during the ongoing resumption timer after prior ON creation. Taking into account all the factors, the expected cost for the neighbouring node "n" will have the following form:

$$C_n = C\lambda_r p_n(n = 0, kT_r \mid n > 0, T_r) + C\lambda_n p_n(n > 0, kT_r \mid n > 0, T_r) p_n(\tau > T_r) + fC\lambda_n p_n(n > 0, kT_r \mid n > 0, T_r) p_n(\tau \le T_r)$$

Since in IMS#4 the handshake procedure is initiated only at the creation of ON, the total expected discounted node cost during a time epoch is the same for each time epoch. Assuming that the probabilities do not change in different time epochs, the total expected discounted node cost can be denoted as follows:

$$\delta_s^{\#4} = \sum_{n=1}^{N} C_n + \beta\sum_{n=1}^{N} C_n + \beta^2 \sum_{n=1}^{N} C_n + \mathrm{L} \ , \beta \in <0,1)$$

Assuming further that the probability of creating an ON with any of the neighboring nodes is uniformly distributed (i.e. the ON creation rate is the same for each neighbour and it equal to

[27] ON duration can be perceived as an increase to the resumption time, which leads to the reduction in the total signalling cost but does not affect the difference in signalling costs between the two strategies

$\lambda = \frac{\lambda_n}{N}$) and that ON creation interarrival times have Poisson distribution, the probabilities which are used in the calculation of the expected cost take the following forms:

- $p_n(n>0,T_r) = 1 - e^{-\lambda T_r}$ – the probability that at least one ON will be created during a time epoch,
- $p_n(n=0,kT_r \mid n>0,T_r) = e^{-\lambda k T_r}(1-e^{-\lambda T_r})$ – the probability that the ON is created for the first time with the neigbouring node "n" during the "k-th" time epoch (in case of IMS#4),
- $p_n(n>0,kT_r \mid n>0,T_r)p_n(\tau > T_r) = (1-e^{-\lambda k T_r})(1-e^{-\lambda T_r})e^{-\lambda T_r}$ – the probability that an ON with the neighbouring node "n" will be created after resumption time expires,
- $p_n(n>0,kT_r \mid n>0,T_r)p_n(\tau \le T_r) = (1-e^{-\lambda k T_r})(1-e^{-\lambda T_r})^2$ – the probability that any subsequent ON with the neighbouring node "n" will be created before resumption time expires,

Assuming that the ON creation rate for every neighbouring node "n" is equal, we obtain the formulas for the total expected discounted node cost which (after calculation of the sum of geometric series) take the following forms:

$$\delta_s^{\#3} = NC(\lambda_r + f\frac{1}{1-\beta}(\lambda_r e^{-\lambda T_r} + \lambda(1-e^{-\lambda T_r}))),\ \beta \in <0,1)$$

$$\delta_s^{\#4} = NC(1-e^{-\lambda T_r})\left(\frac{p_f}{1-\beta} + \frac{\lambda_r - p_f}{1-\beta e^{-\lambda T_r}}\right),\ \beta \in <0,1),\ p_f = f\lambda - f\lambda e^{-\lambda T} + \lambda e^{-\lambda T}$$

The following figure shows the difference in terms of signalling load between the considered strategies for f=0.14 which corresponds to EAP-TLS simplification, i.e. 276 bytes of the resumption procedure vs. 1933 bytes of the full handshake procedure.

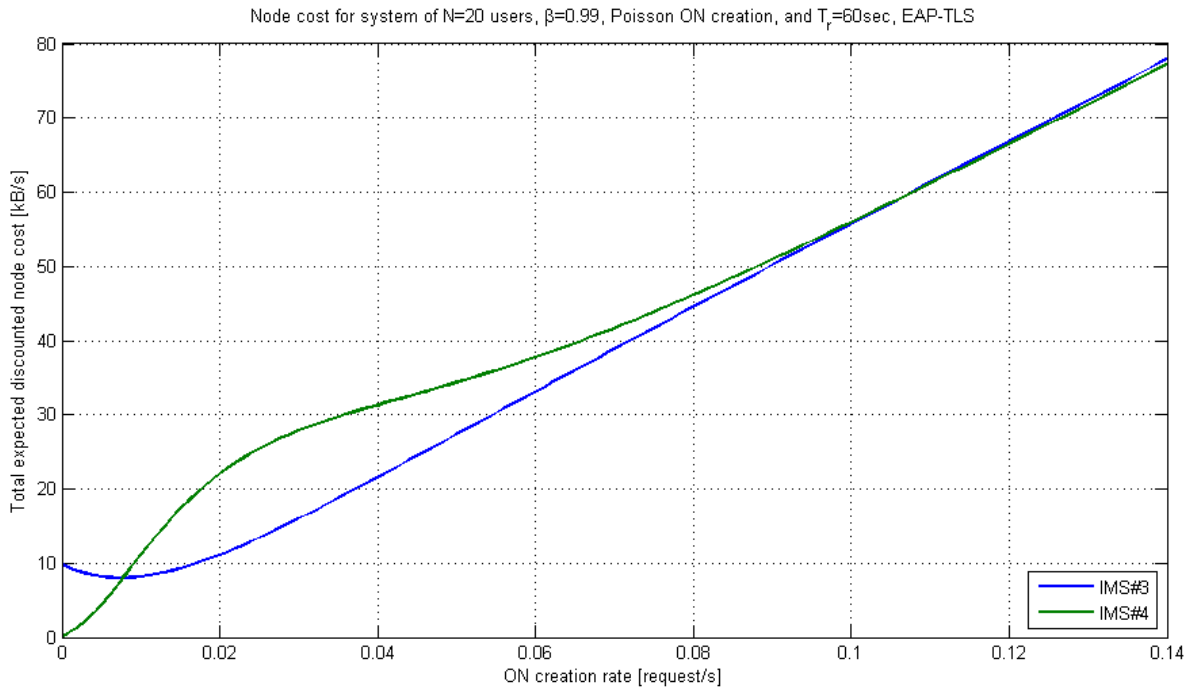

Figure 47: Security related signalling overhead for IMS#3 and IMS#4 for stationary neighbourhood

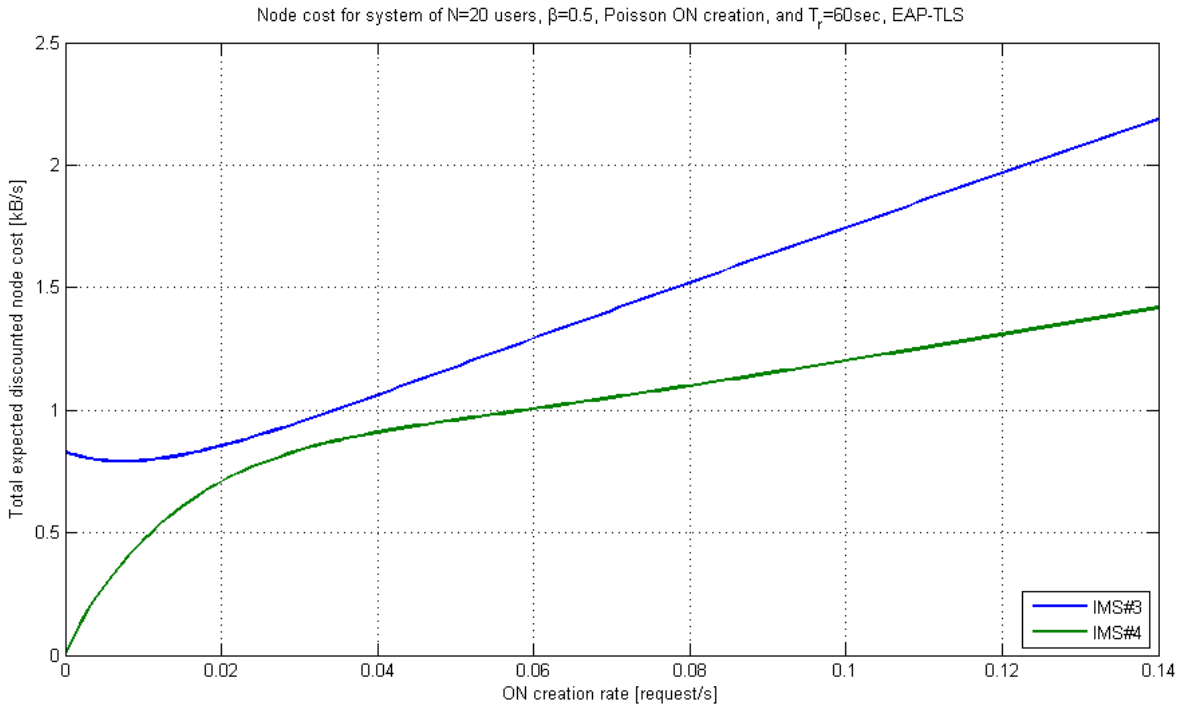

Figure 48: Security related signalling overhead for IMS#3 and IMS#4 for non-stationary neighbourhood

As seen in Figure 47 and Figure 48, the signalling load performance of each method is highly dependent on the ON creation rate and the stationarity of the wireless neighbourhood. In the case of low ON creation rate (<0.01 requests/s) IMS#4 provides better performance in terms of signalling load than IMS#3, however as the ON creation rate grows the performance of IMS#4 degrades and overcomes the performance of IMS#3. This seemingly counterintuitive result can be explained with the mechanism of IMS#4, which expects that full handshake procedure is performed whenever there is no resumption timer ongoing. Now, if there is relatively low number of ON requests then the cost of aperiodic handshake procedures (even full ones!) cannot out-match the periodical IMS#3. However, as the ON creation rate increases and more handshake procedures are required, high number of them are full handshake procedures, which bear higher cost that eventually out-matches the cost of periodical simplified handshake procedure. Nevertheless, as the ON creation rate becomes large enough (>0.1 requests/) the cost of both procedures stabilizes and tends to a difference, which is a cost of a single simplified handshake procedure. In the case of non-stationary neighbourhood (see Figure 48) IMS#4 always bears costs lower than IMS#3, because the nodes account very little for future costs and thus periodic procedure which requires immediate full handshake procedure bears the highest signalling cost.

However, it needs to be highlighted that IMS#4 introduces additional delay during the ON creation (full handshake procedure requires exchange of additional information), what in turn in some scenarios may result in a lower probability of a successful ON creation. For this is reason (as well as potentially lower signalling overhead) in some cases (especially related to stationary, low mobility neighbourhood) it may be beneficial to employ IMS#3 instead of IMS#4. It also needs to be stressed that the size of interval for which the IMS#3 shows better performance than IMS#4 depends on the signalling cost reduction factor and thus IMS#3 could perform even better if the simplified procedures would impose smaller reduction factor.

5.3.6 Summary

The following section focused on the overhead analysis of a subset of procedures essential for providing security in the context of Opportunistic Networks (i.e. certificate enrolment and mobile terminal handshake). The main factors which affects the signalling overhead (i.e. ON creation rate and Certificate validity) were identified and studied. The analysis showed also that security related signalling load can be tuned by employing different Information Management Strategies. Additionally, although it was not explicitly presented and analysed, the selected Information Management Strategy affects the ON setup delay, which in turn affects the probability of successful ON creation.

It is worth to remind here that (in general) the employed solutions are based on the existing and commonly used protocols/frameworks (e.g. EAP-TLS [15], EAP-IKEv2 [13], Untrusted non-3GPP IP access [25], GAA [22]). The main advantage of such approach is related to small standardization costs (e.g. thorough evaluation of such solutions is not always strictly necessary) and simplified integration with existing systems.

6. Signalling analysis for different algorithms

The following section focuses on estimation of the signalling traffic generated by various ON related algorithms which cover main technical challenges identified within the OneFIT project (i.e. spectrum opportunity identification and selection, route and node selection). It needs to be underlined here, that information exchanged over RAT specific messages to enable legacy procedures may be often used by ON management algorithms. Depending on the context, such information can be either considered as related or unrelated to ON management. Whenever the RAT specific messages are carried independently from the management algorithm, the conveyed information is not accounted as ON related signalling. As an example, such messages may be related to the measurements performed by a UE for mobility in LTE E-UTRAN[28] e.g.:

- Intra-frequency E-UTRAN measurements;
- Inter-frequency E-UTRAN measurements;
- Inter-RAT measurements for UTRAN and GERAN;
- Inter-RAT measurements of CDMA2000 HRPD or 1xRTT frequencies.

Whenever the RAT specific messages are transmitted for the purpose of (or are triggered by) ON management algorithms, they shall be incorporated into the overall signalling traffic load estimation.

6.1 Opportunistic coverage extension with relaying device

6.1.1 Evaluation model

The evaluation of the opportunistic coverage extension scenario consists of three parts:

A. An estimation on how often the situation of a device is getting out of coverage occurs and in how many cases this can be solved by creating an Opportunistic Network. This estimation is done by simulations as described in D4.2 [5] where the probability of solving an out of coverage situation with an Opportunistic Network is evaluated with the ONE-simulator [30] as show in Figure 49. The result depends on parameters like coverage range of the infrastructure, range of the direct interface, number of devices per km^2, speed of the users [31].

B. Measurements of the amount of signalling (number of messages, number of bytes) in a concrete scenario in an opportunistic network demonstrator (testbed) [8] which uses an IEEE 802.21 based C4MS implementation. The basic setup of this demonstrator is shown in Figure 50:

C. Analytical evaluation of the signalling load based on the C4MS design and taking into account the results from the simulation and the testbed.

[28] Futher information regarding the measurements may be found in [24].

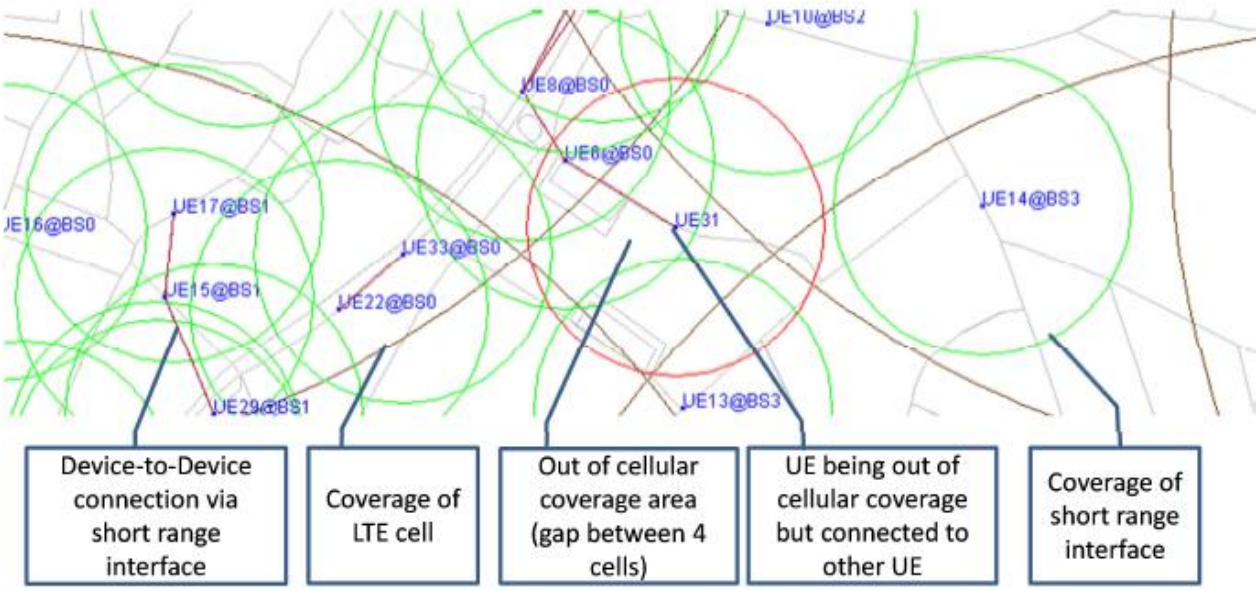

Figure 49: Simulation of out-of-coverage scenario with the ONE-simulator [30],[31]

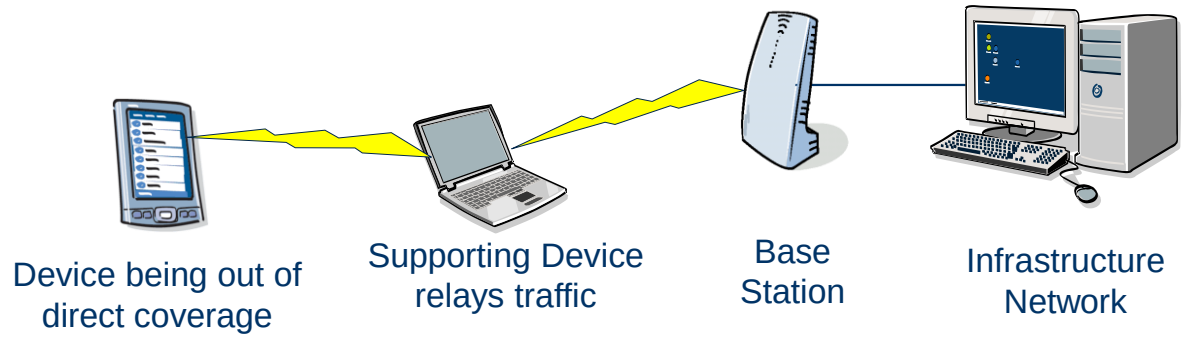

Figure 50: Opportunist Networking Testbed

6.1.2 Verification scenario for the coverage extension

A typical message exchange for the coverage extension scenario is shown in Figure 51.

In general, each base station or access points registers to the Cognitive Radio System Management (CRSM) on infrastructure side, which hosts the JRRM, DSM and a combined CSCI and CMON. Dependent on the configuration of a base station, the base station may first ask the DSM on which spectrum to use (Spectrum Assignment Request/Response) before registering to the JRRM-part of the CRSM (Register Cell Request/Response).

Each connected terminal sends measurements reports to the CRSM (e.g. via MIH_Link_up/down indications or MIH_Link_Parameter_Report). The infrastructure evaluates these measurements and then decides upon the situation if a device shall be reconfigured e.g. to provide a relaying service for another terminal or if a direct device-to-device connection shall be established for a communication session.

In the example shown in Figure 43, UE#1 is getting out of coverage of the infrastructure, thus a MIH_Link_Going_Down.indication is sent to the infrastructure. Alternatively, the infrastructure can also already react on then information transmitted e.g. in the MIH_Link_Parameters_Report. During

the suitability determination, the CRSM decides that an ON shall be created. Therefore, the CRSM negotiates with UE#2 if it can act as relay for UE#1. After successful negotiation, the JRRM inside the CRSM asks the DSM on which spectrum to use for the relay in UE#2 and then an ON_Creation.Request is sent to UE#2 to create the relay. After creation of the relay, the relaying access point is registered in the CRSM and then UE#1 is informed with an ON_Suitability.indication message that is recommended to handover to the relaying access point created by UE#2.
After the handover,UE#1 uses the ON created by UE#2.
Both UEs still report measurements to the infrastructure. Update-Cell-Information messages are used to report the cell status and cell load towards the infrastructure.

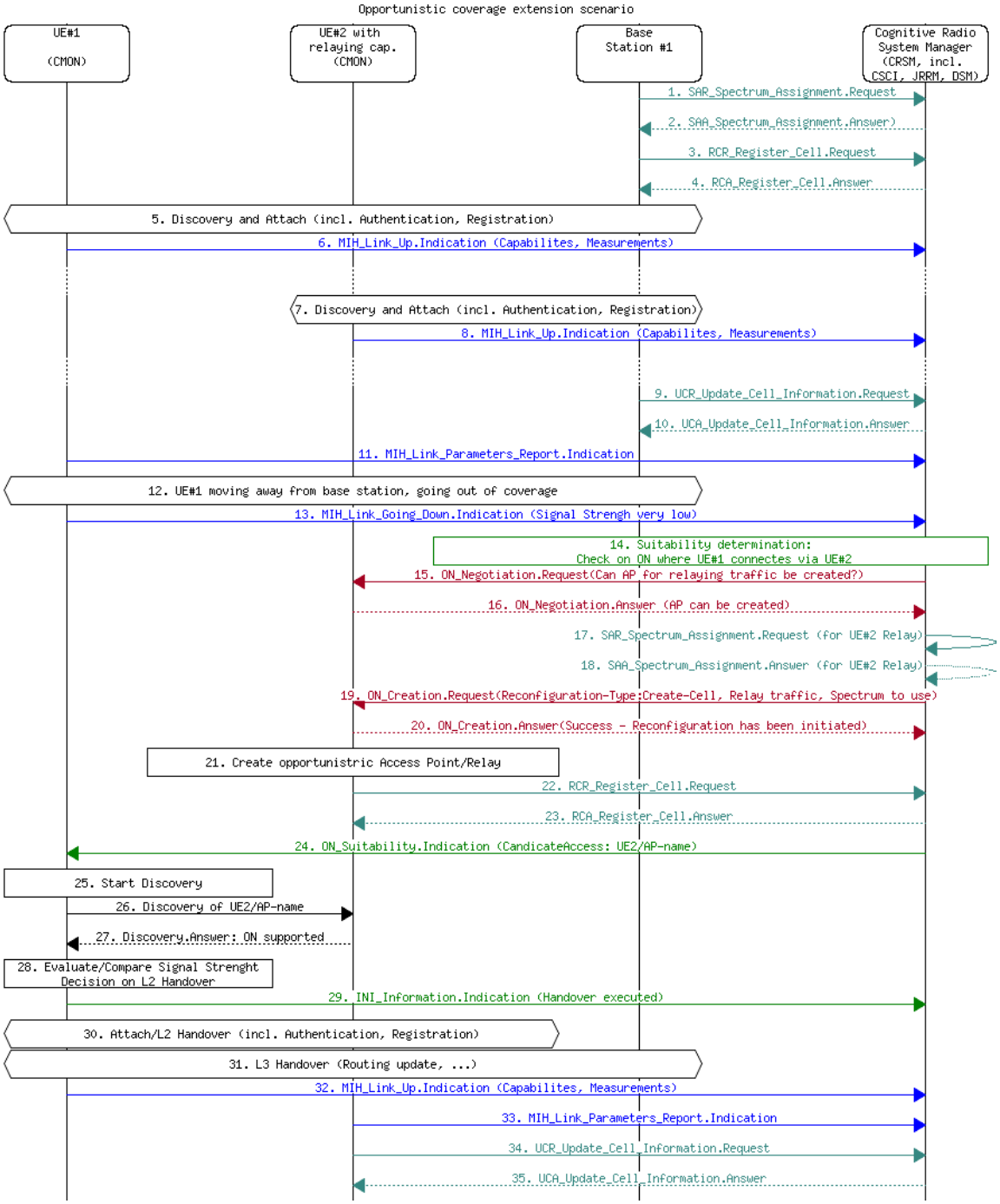

Figure 51: Verification scenario for creating an ON based on the OneFIT demonstrator.

6.1.3 Information management strategies

The exchanged information can be divided into different categories:

A. To which building block the information is related, e.g.
    a. RRM/JRRM related,
    b. CSCI/CMON-related,
    c. DSM related
B. To the procedure where the information is related to, e.g.
    a. Traditional link establishment/release
    b. ON creation/release
    c. Traditional measurement reporting
    d. ON related measurement reporting.

For this evaluation, the most interesting part is the CSCI/CMON related signalling and comparisons can be made e.g. with legacy RRM or JRRM related signalling.

For the ON establishment, the standard procedure is that first a negotiation procedure must be performed before the ON creation takes place. However, the negotiation procedure may be omitted if the negotiation related information like terminal/device capabilities or policies are exchanged with other procedures, e.g. during the classical link setup.

The signalling load strongly depends on the measurement configuration. The infrastructure can decide on which measurements are needed and send measurement configuration requests to each terminal. In the case of LTE, these measurements and measurement configurations are specified in the 3GPP RRC specification [21]. Such a Measurement Configuration Request can contain information on

- which links to be measured (Active link only or measurements of potential candidate links towards other nodes in the neighbourhood)
- type of information to be measured (e.g. signal strength, signal quality, estimated data rate, bit error rate, noise, load)
- periodicity of measurement (single measurement or periodicity in milliseconds in case of periodic measurements). 3GPP LTE RRC procedures [27] for example define for the measurement reporting a “ReportInterval” with values 120 ms, 240 ms, 480 ms, 640 ms, 1,024 sec, 2,048 sec, 5,120 sec, 10,240 sec, 1 min, 6 min, 12 min, 30 min and 60 min. IEEE 802.21 uses timer values with a range from 0 to 65536 ms.
- event based measurement reporting, e.g. information if Link-up events, Link-going-down events or Link-detected events shall be reported. Further on, the measurement configuration may include thresholds and an indication if a report shall be sent if the measurement value goes above the threshold or goes below the threshold, e.g. send report if signal strength goes below 25%.

For the opportunistic network, these measurement procedures can be reused, but the amount of measurement signalling increases, e.g. because there are additional links to be reported or because the information must be transported over two or more hops instead of one hop.

6.1.4 Signalling message size estimations

For an estimation of the message sizes, the messages sizes have been taken from the Opportunistic Networking prototype which has an IEEE 802.21 based C4MS implementation.

The message sizes vary dependent on the amount of optional parameters included in the message and also dependent on the parameter content. For example, if a hostname or an SSID is included then the parameter size depends on the length of the hostname or the SSID.

Table 26: Typical average C4MS message sizes for 802.21 based C4MS messages transported over TCP/IP

Message	Typical average C4MS message Size (bytes)	Typical average total messages size (C4MS + TCP + IP + L2 + L1)
Link Measurement reporting		
Measurement report, e.g. MIH_Link_Parameters_Rep_IND , MIH_Link_Up/Link Going Down indication	90	156
Cell load Measurement reporting		
Update Cell Information (Load report from relay)	50	116
Update Cell Information Response	20	86
ON Creation procedure		
ON_Negotiation Request	~20 byte attached to another message, e.g. the first measurement report	N.A.
Spectrum Assignment Request/Response	0 because message is not sent over an external link, only CRSM internal between CSCI and DSM	N.A.
ON Creation Request	120	186
ON Creation Response	20	86
Register Cell Request (for Relay)	100	166
Register Cell Response (for Relay)	20	86
ON Suitability Indication (Recommendation on Handover to ON possible)	120	186
Information Indication (Handover executed)	20	86
ON Release procedure		
ON Suitability Indication (Recommendation on Handover back to infrastructure	120	186
Information Indication (Handover executed)	20	86
ON Release Request	80	146
ON Release Response	30	96

6.1.5 Signalling load evaluation

Table 27 shows the signalling load evaluation for the 802.21 based C4MS.

The largest part of the signalling load comes from the measurement reporting. Please note that these measurements are normally not ON related because link measurements are also exchanged when being normally connected with an infrastructure network. However, in the case of an ON, the measurements of the device being out of direct infrastructure coverage have to be transported over an additional hop via the relaying device, therefore, the signalling load at the relaying device increases.

In the case that for example link measurements are reported all 30 seconds (e.g. periodical report all 30 seconds or a link event to be reported in average all 30 seconds), then the signalling load for the link measurements is about 0,033 messages/second. In the case that these measurements are reported all 5 seconds, then the load increases to 0,200 messages/second.

The table also shows the signalling load for ON Creation and ON Release as well as for Cell Load Measurement reporting from the relaying device.

Further on, the table shows the signalling load of the complete ON lifecycle. The two examples shown in the last two rows of Table 27 again differ in the periodicity of the link measurement reporting. In the shown example, the signalling load ranges from 0,11 messages/second to 0,28 messages per second or 48 bit/second to 168 bit/second for the C4MS signalling. When taking also the overhead of the TCP/IP stack into account, then the signalling load ranges from 107 bit/s to 315 bit/s.

Table 27: Signalling load with IEEE 802.21 based C4MS

Procedure	Signalling load in msg/s or msg/procedure	Signalling load in bit/s or bit/procedure	
		C4MS only	C4MS/TCP/IP
Signalling load per procedure			
Link measurement reporting per Terminal, periodically all 5 seconds (RRM related)	0,200 msg/s	18 byte/s = 144 bit/s	31 byte/s = 248 bit/s
Link measurement reporting per Terminal, periodically all 30 seconds (RRM related)	0,033 msg/s	3 byte/s = 24 bit/s	5,2 byte/s = 41,6 bit/s
Creation of an ON, e.g. when procedure takes 5 seconds, including relaying cell registration (ON related)	6 messages 1,2 msg/s	400 byte = 3200 bit 80 byte/s = 640 bit/s	796 byte = 6368 bit 159 byte/s = 1274 bit/s
Cell Load measurement reporting per relaying device, periodically all 30 seconds (RRM for ON)	0,066 msg/s	2,33 byte/s = 18,66 bit/s	6,73 byte/s = 53,87 bis/s
Link measurement reporting per additional hop per Terminal in an ON, periodically all 5 seconds (RRM related, extra hop due to ON)	0,2 msg/s	18 byte/s = 144 bit/s	31 byte/s = 248 bit/s
Release of an ON, e.g. when procedure takes 5 seconds (ON related)	4 messages 0,8 msg/s	250 byte = 2000 bit 50 byte/s = 400 bit/s	514 byte = 4112 bit 103 byte/s = 822 bit/s
Signalling load per complete ON Lifecycle			
Complete ON lifecycle: ON Creation, 15 minutes duration, (load meas. report all 30 sec., link meas. report all 5 sec) release	6 msgs (creation)+ 60 msgs load report + 180 msgs link meas + 4 msgs release = 250 messages 0,28 msgs/sec	400 byte + 30 * (50+20) byte + 180 * 90 byte + 250 byte = 18950 byte 21 byte/s = 168 bit/s	796 byte + 30 * (116+86) byte + 180 * 156 byte + 514 byte = 35450 byte 39,4 byte/s = 315 bit/s
Complete ON lifecycle: Same as above but link meas. reported only all 30 sec. instead of 5 sec.	6 msgs (creation)+ 60 msgs load report + 30 msgs link meas + 4 msgs release = 100 messages 0,11 msgs/sec	400 byte + 30 * (50+20) byte + 30 * 90 byte + 250 byte = 5450 byte 6 byte/s = 48 bit/s	796 byte + 30 * (116+86) byte + 30 * 156 byte + 514 byte = 12050 byte 13,4 byte/s = 107 bit/s

Figure 52 shows the number of C4MS messages exchanged during the lifetime of a "basic ON" at the example of the coverage extension scenario. Such a basic ON consists of a supported device (the

device e.g. going out of coverage), a supporting device (the device providing the relaying service) and one infrastructure network.

As shown in Figure 52 the number of of C4MS messages exchanged during the lifetime of an ON is largely dependent on the duration of an ON and is also largely dependent on the measurement reporting strategy. Two curves are shown, one where link events occur in averge all 5 seconds or a reporting periodicity of 5 seconds has been choosen and the other curve where reports are sent in average all 30 seconds (e.g. due to lower mobility of the user).

Only a relative small number of messages is needed for the creation and release of the ON.

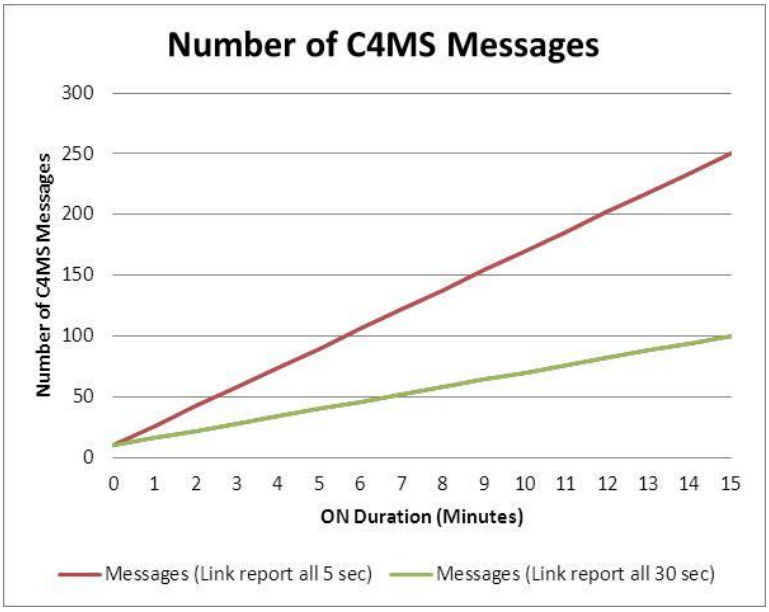

Figure 52: Total number of C4MS messages for a basic ON

Figure 53 shows the numbers of the C4MS messages per second for the same ON. For ONs with a duration of less than two minutes, the number of C4MS messages per second increases due to the fixed number of C4MS messages needed for the creation and release of an ON. For an ON with a longer duration, the amount of C4MS mainly depends on the measurement reporting strategy as explained above.

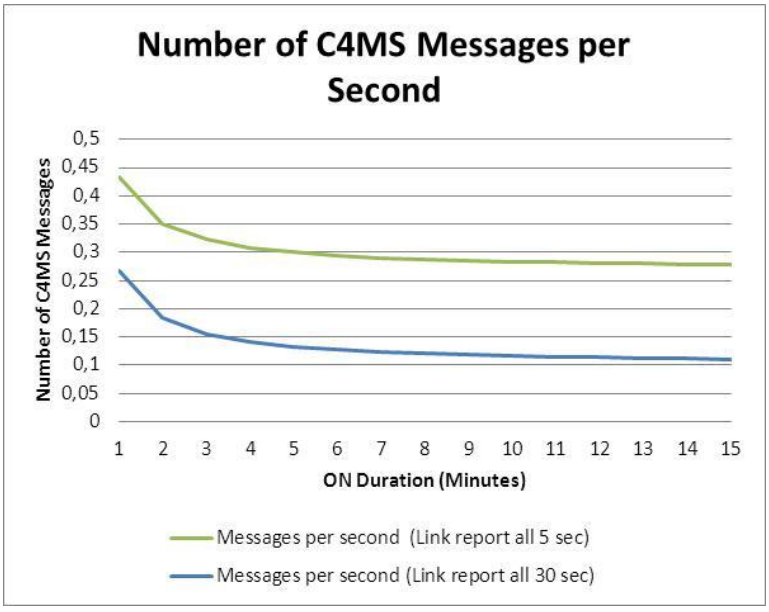

Figure 53: Number of C4MS messages per second for a basic ON

6.1.6 Conclusions

This evaluation has shown an analysis of the signalling overhead for the management of a basic opportunistic network at the example of a coverage extension scenario. It can be concluded that the signalling overhead for the opportunistic network management adds only smaller additional signalling load to the overall system and is thus affordable.

6.2 Modular decision flow approach for selecting frequency, bandwidth and radio access technique for ONs

6.2.1 Evaluation model

The evaluation is based on the scenario with out of coverage terminals. If an operator governed ad hoc network is required for the out of BS coverage terminals, short range links between UEs may be established to route traffic through UEs to the BS. The modular decision approach selects and allocates suitable spectrum (*b*), bandwidth (*w*) , and RAT (*r*) for each short range link in ON to ensure the adequate QoS provided for users with different traffic types.

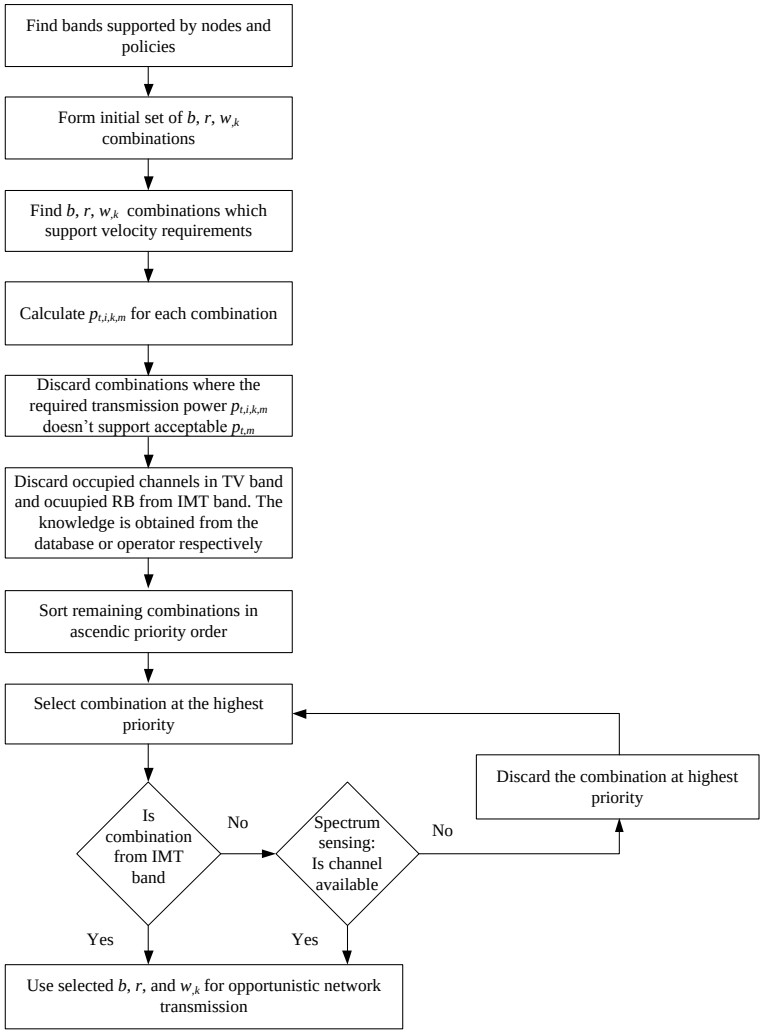

Figure 54: Modular decision flow approach.

During the ON lifecycle, the algorithm is executed on suitability determination, creation, and maintenance phases. In suitability determination phase, the algorithm detects the potential radio paths and RATs. In creation phase, the algorithm selects spectrum, bandwidth, and RAT for ON. In maintenance phase, the algorithm can be used to assign new spectrum, bandwidth, and RAT for ON. The algorithm uses as input the policy information, mobile terminal's velocity, sensing information

about the channel availability, node capabilities, as well as the application requirements. Figure 54shows the steps of the modular decision flow approach. The algorithm terminates until the suitable [*b,w,r*] combination is found.

6.2.2 Verification scenario

We consider the following simulation scenario as used in WP4 to evaluate the C4MS signalling load:

(1) Three different traffic types namely: voice, streaming and web browsing are considered. The required QoS levels are 60kbps, 13kbps, and 384kbps, respectively.

(2) We run the simulations over five TV bands which have equal bandwidth of 8MHz, one 2.4GHz band with bandwidth 20MHz, one IMT band with bandwidth 20MHz, and one 60GHz band with bandwidth 100MHz.

(3) For TV and IMT band, the entire spectrum is represented with subcarriers each having spectrum spacing of 15kHz. 20MHz band contains 100 resource blocks, and each block is formed by 12 subcarriers and the time duration is 0.5 ms.

(4) For 2.4GHz band, we consider 802.11a, where the subcarrier spacing is 312.5kHz; and for 60GHz band, we consider 802.15.3c, where the subcarrier spacing is 1.5625MHz.

To evaluate the signalling load, our evaluation mainly focuses on the ON creation phase whenever a new link needs to be established and the ON maintenance phase due to the changes in spectrum band utilization. The information exchange procedures for the coverage extension scenario are shown in Figure 55 and Figure 56. Without loss of generality, we assume here that all information exchange procedures are done perfectly such that no retransmissions are required.

As shown in Figure 55, the ON creation phase can be further divided into two sub-phases. During the first sub-phase, the ON creation algorithm determines an ON blueprint based on the confirmation information from nodes about their willingness to participate in an ON. The second sub-phase is responsible for the extension of the ON blueprint and establishment of the actual ON.

Similarly, the ON maintenance phase consists of two sub-phases, as illustrated in Figure 56. During the first sub-phase, spectrum usage relevant information is collected (e.g. link qualities) at the BS or the terminal side. The collected information is used to monitor the ON and determine a need for the ON modification. The information is collected by ON participants. The operations in the second sub-phase are responsible for the ON modification.

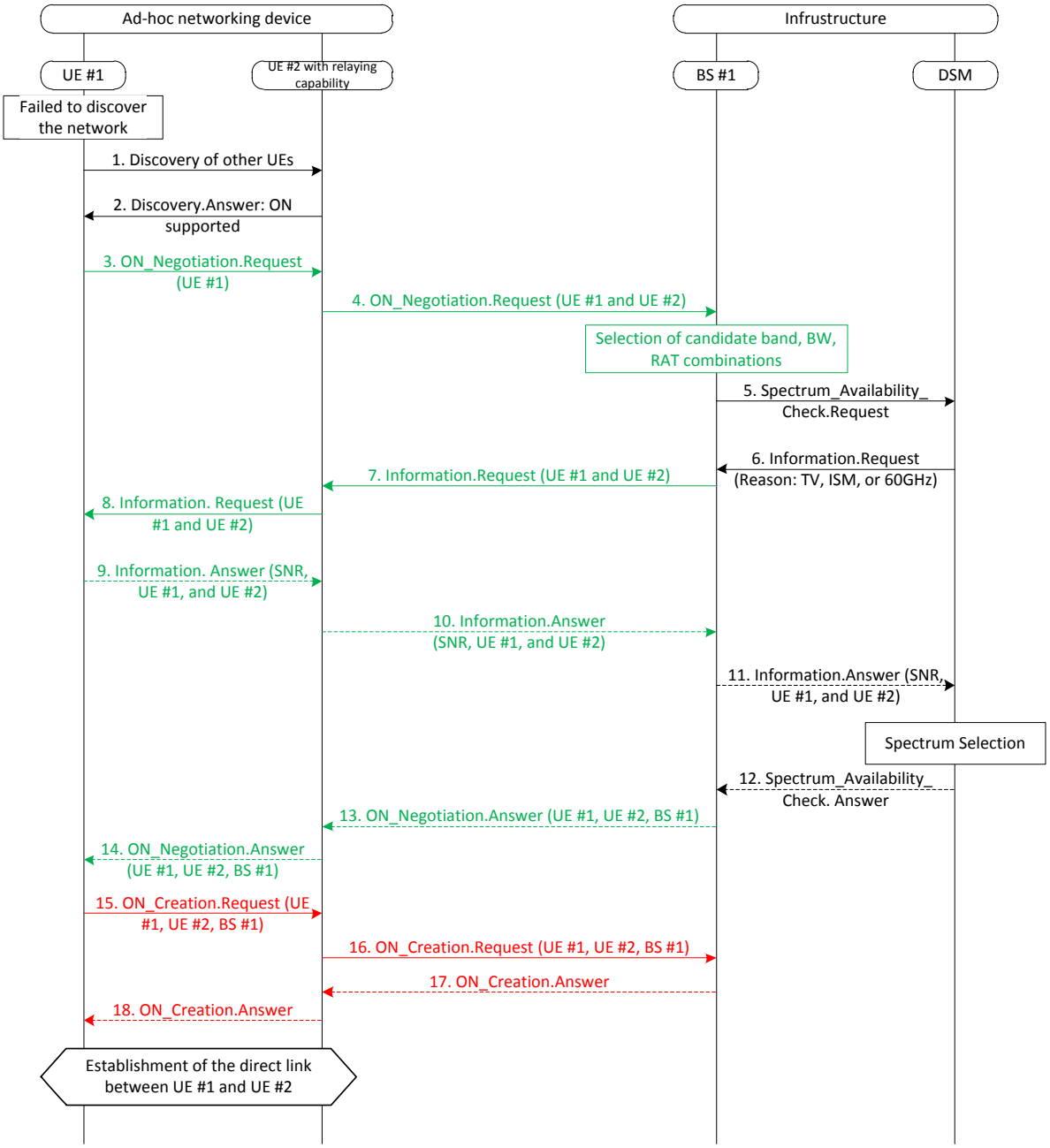

Figure 55: Message sequence chart for ON creation phase.

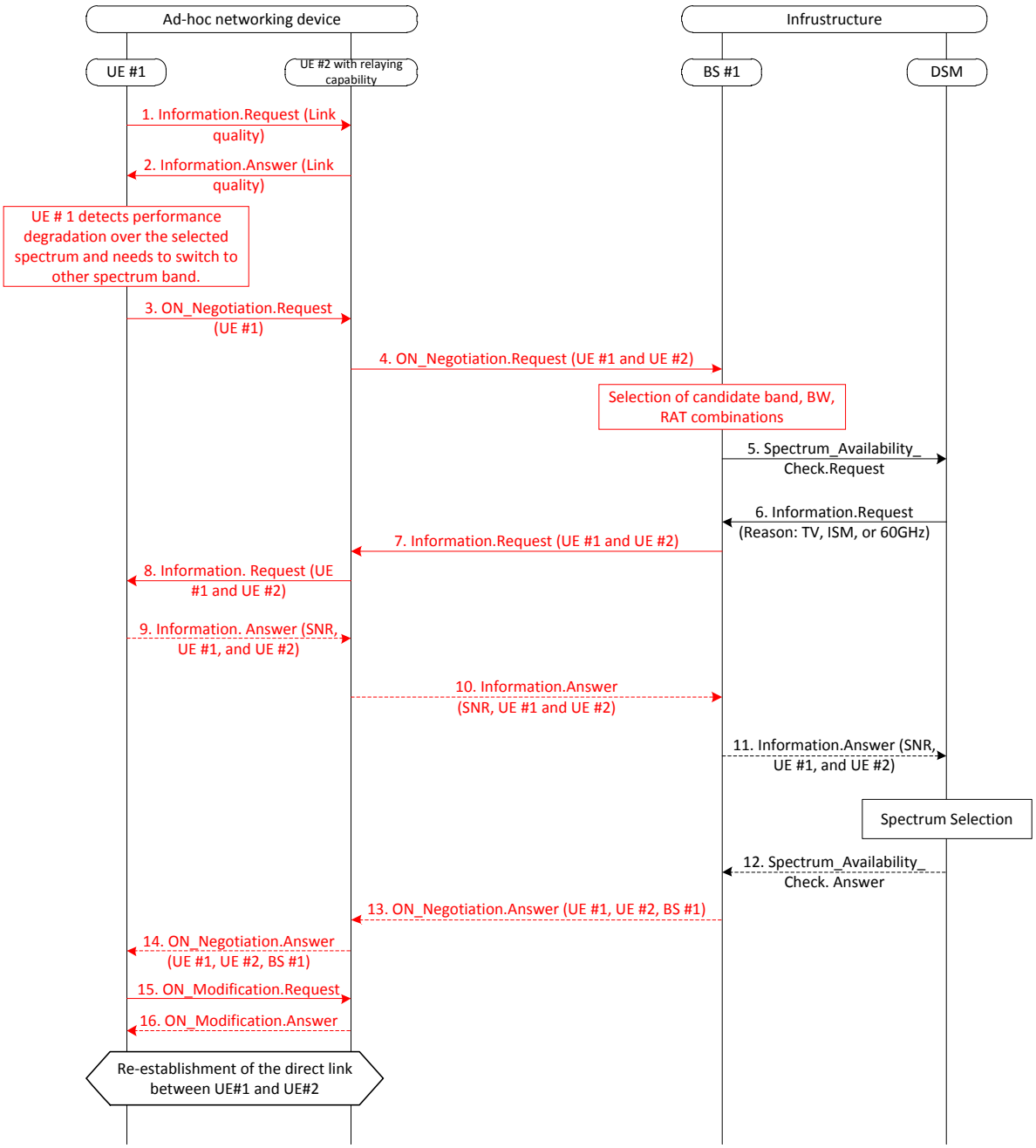

Figure 56: Message sequence chart for ON maintenance phase.

6.2.3 Information management strategies

In our evaluation, we consider energy detector based sensing. Since the UEs (secondary users) have no prior information about the primary users, they forward the received SNR measurements to the infrastructure and the spectrum availability can be checked at the BS. During the ON creation phase, the requirement of spectrum sensing is determined by the BS. That is, if the selected spectrum is TV, ISM, or 60GHz band, the BS needs to check its availability and requires the UEs to send back the SNR measurements. The spectrum band is allocated to the UEs if it's sensed to be idle.

For the ON maintenance phase, the SNR measurement is consider to be executed at the terminal side once the UEs detect performance degradation due to changes in the spectrum usage and need to re-establish a direct link. The following strategies are considered for spectrum sensing during the ON maintenance phase:

- Periodical spectrum sensing (PSS) - spectrum sensing is considered to be executed periodically so that the sensing interval is defined for every spectrum band;
- Event-triggered spectrum sensing (ESS) – as mentioned previously, once the terminals detect performance degradation and need to switch to other spectrum band, spectrum sensing is triggered to check the spectrum availability in order to re-establish the direct link between UEs.

6.2.4 Signalling message size estimations

Based on the specific fields defined in the Appendix to D3.3 [10] section 3 and the C4MS data structure in Section 3 , as well as the contents considered for evaluations, Table 28 and Table 31 show the C4MS message size and total signalling load for each of the two phases, to be used in signalling evaluations.

Table 28: The total C4MS signalling load for the ON coverage creation phase

Message	Size (bytes)
3. and 4. ON_Negotiation.Request	35
7. and 8. Information.Request	19
9. and 10. Information.Answer	23
13. and 14. ON_Negotiation.Answer	20
15. and 16. ON_Creation.Request	44
17. and 18. ON_Creation.Answer	37
TOTAL	356

Table 29: The total C4MS signalling load for the ON coverage maintenance phase

Message	Size (bytes)
1. Information.Request	11
2. Information.Answer	15
3. and 4. ON_Negotiation.Request	34
7. and 8. Information.Request	19
9. and 10. Information.Answer	23
13. and 14. ON_Negotiation.Answer	20
15. ON_Modification.Request	27
16. ON_Modification.Answer	20
TOTAL	265

6.2.5 Evaluation metrics

We consider the total signalling load as the main metric to evaluate the C4MS signalling load in scenarios discussed above. That is, the C4MS signalling load is measured through the amount of data exchanged via C4MS messages per unit of time during the whole ON creation/maintenance phase (the results are expressed in bits/s).

6.2.6 Signalling load evaluations

For the ON creation phase, there are 30 ON users and three data types are used in simulations, namely, voice, web browsing, and streaming. The simulation takes 10 seconds. Curves in Figure 57 show the total signalling total with respect to the link lengths. Ten users are stationary, twenty move with velocity 1.11 m/s. We can find that the total signalling load reduces as the link length increases. This is because spectrum sensing is required for TV, 2.4 GHz, and 60 GHz bands, which result in increasing C4MS information exchanges. Specifically, for browsing users, the 2.4 GHz band is selected mostly at short link lengths due to the browsing users less demanding bit rate requirements; and for voice and streaming users the selected band is mostly 60 GHz band, this is due to the good channel capacity that 60 GHz provides. As the link length increases the 60 GHz band becomes unsuitable due to notably large free space loss, and relatively high molecular absorption by oxygen (the 60 GHz band is best suited for short range, low mobility, and indoor communication). Transmission power constraint restricts the use of TV band in longer transmission ranges as the acceptable transmission power level for secondary users in the TV band is 50 mW [33]. Due to the earlier mentioned problems with TV and 60 GHz bands, the IMT band is selected when transmission distance is relatively large. That means spectrum sensing is no longer required, thus reducing the C4MS information exchanges. We can also find from Figure 57 that the signaling load is lower for the short range situation where there are more voice users and less streaming users. The results demonstrate that IMT bands are allocated to some of the voice and browsing users at short range due to lack of spectrum resources.

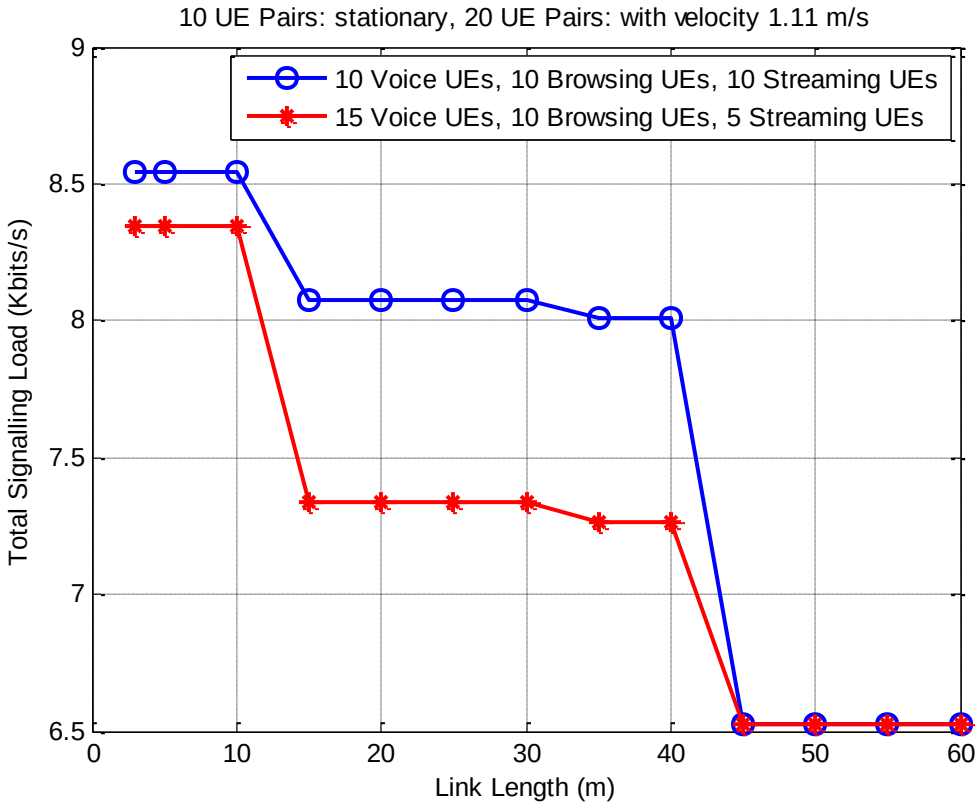

Figure 57: Total signalling load for different data type settings versus the link length

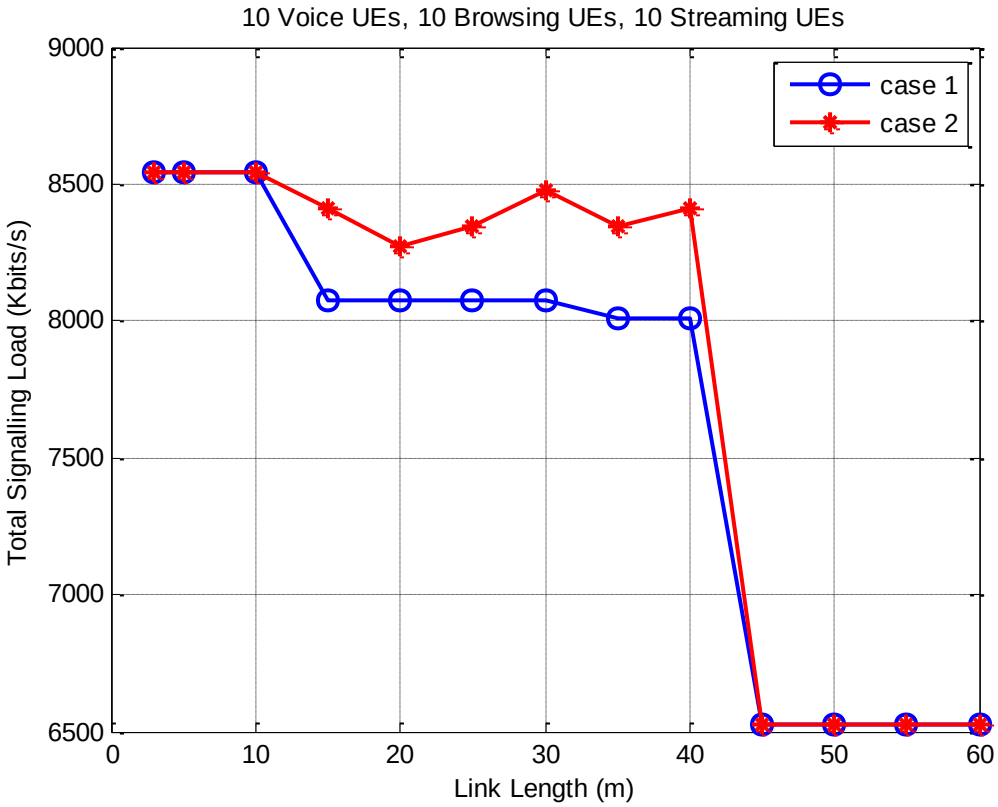

Figure 58: Total signalling load for different velocity settings versus the link length

Figure 61 depicts the signalling load for different velocity settings as the link length increases. In the evaluation, we assume 10 users per data type, and two velocity cases are considered:

- case 1: ten users are stationary and twenty users move with velocity 1.11 m/s
- case 2: six users are stationary, six users move with velocity 1.11 m/s, six users move with velocity 5.55 m/s, six users move with velocity 13.89 m/s, and six users move with velocity 27.78 m/s.

We may notice from the curves that when the link length is between 10 m and 45 m, the signalling load in case 1 is lower than that in case 2. Due to the fact that for short range communication (i.e. from 0 to 40 meters) the TV and 60 GHz bands are allocated to users which spectrum sensing is required and the signalling load is the highest. As the link length increases, in case 2 compared with case 1, less IMT bands are selected for users, thus more bands need spectrum sensing and this finally results in greater signalling load. For the largest link lengths (i.e. 45 meters and more), TV, 2.4 GHz, and 60GHz bands are not selected, therefore, the signalling load in both scenarios is the lowest.

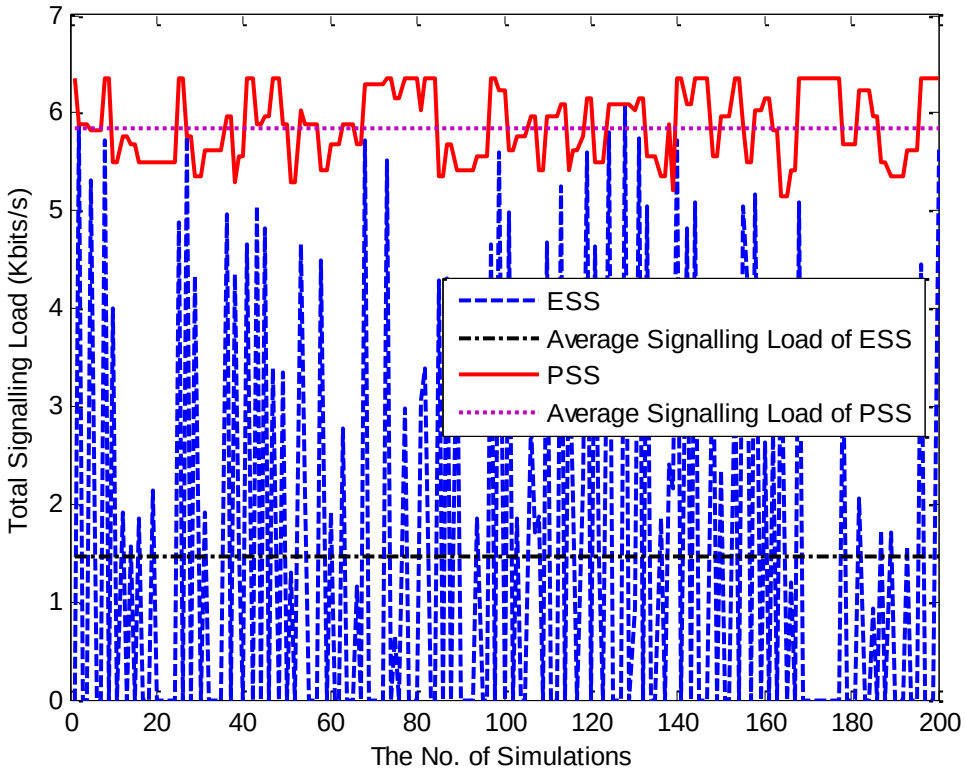

Figure 59: Total signalling load for the ON maintenance phase

Next, we consider the signalling load for the ON maintenance phase. We face a situation when users that are not part of ONs appear in the spectrum band that is used by ON participants and thus force the band allocated to the ON to be changed. So called other users are users who do not participate ON and they can be either primary users (like in TV band) or other non-licensed users like users in 2.4 GHz band or other licensed users in the operators own band (IMT). Two strategies for spectrum sensing (previously discussed in Section 6.2.3) are evaluated, namely periodical and event-triggered strategies.

When selecting new band for the ON, information needs to be exchanged between the terminals and the infrastructure. In the following, we evaluate the performance of the modular decision flow approach in terms of signalling load. In the simulations, we use exponential distributed interarrivals to model other than ON users' activity. We exploit the birth-death process [34] of ON with death rate α and birth rate β which are uniformly distributed between 0.1 and 0.5. Figure 59 shows total signalling load for 10 voice users, 10 browsing users, and 10 streaming users when link lengths varies randomly between 3 and 40 m. It's worth mentioning that under the periodical spectrum sensing strategy, we assume every terminal measures the received SNR at the beginning of each simulation time and sends the result to the infrastructure; therefore, it's straightforward that the signalling load is higher than that under the event-triggered spectrum sensing strategy.

6.2.7 Conclusions

In this subsection, we have evaluated the signalling load of the modular decision flow approach for spectrum, bandwidth and RAT selection. The total signalling load depends on the duration of creation or maintenance phase, and is affected by many factors, e.g., data type, link length, and UE velocity. Compared with the traffic load (3Mbits/s ~ 60Mbits/s), the value is much smaller for both phases. We also examine the signalling load under two different strategies for spectrum sensing

during the maintenance phase. It can be learned from the evaluation results that event-triggered strategy achieves great performance in reducing the average signalling load.

6.3 Fittingness-factor based spectrum selection

6.3.1 Evaluation model, scenario and information management strategies description

6.3.1.1 General description of the evaluation model and scenario

The problem considered by this algorithm consists in the selection of the spectrum to be used by the radio links of a set of ONs established between pairs of terminals and/or infrastructure nodes. Each ON is considered to use a radio link to support a CR application with certain bit rate requirements.

The algorithm uses as input the set of available spectrum pools resulting from the spectrum opportunity identification, together with the characteristics of each pool in terms of available bit rate based on radio considerations. The algorithm makes use of the fittingness factor concept as a metric to capture how suitable a specific spectrum pool is for a specific radio link. Different statistics regarding the observed fittingness factor based on the accumulated experience are stored in a knowledge database and used to make decisions. The spectrum selection is done either when a new application needs to be established or as a result of changes in the radio conditions or in the current active links. For details on the algorithm operation the reader is referred to [5][31].

The evaluation of the C4MS signalling load in this scenario will be based on the same simulation model that is being used for the performance evaluation carried out in WP4. It uses a system-level simulator operating in steps of 1s. The scenario is characterised by the following:

- Traffic characterisation: Two types of radio links $L=2$ radio links are considered in the scenario. The l-th link generates sessions based on a Poisson process with arrival rate λ_l and constant session duration $T_{req,l}$. Link #1 is associated to low-data-rate sessions ($R_{req,1}=64Kbps$, $T_{req,1}=2min$) while link #2 is associated to high-data-rate sessions ($R_{req,2}=1Mbps$, $T_{req,2}=20min$). The total offered load $\lambda_1 \cdot T_{req,1} \cdot R_{req,1} + \lambda_2 \cdot T_{req,2} \cdot R_{req,2}$ is varied in the different simulations. Note that $\lambda_l \cdot T_{req,l}$ is the average number of active links of the l-th type, measured in Erlangs. It has been considered that $\lambda_1 \cdot T_{req,1} = \lambda_2 \cdot T_{req,2}$.
- Spectrum characterisation: There are a total of P=4 spectrum pools. The available bandwidth at each pool is $BW_1=BW_2=0.4$MHz and $BW_3=BW_4$=1.2MHz. A heterogeneous interference situation is considered in which the total noise and interference power spectral density I_p experienced in each pool $p \in \{1..P\}$ follows a two-state discrete time Markov chain jumping between a state of low interference $I_0(p)$ and a state of high interference $I_1(p)$. In the considered case, pools #1 and #2 are always in state $I_0(p)$ while pools #3 and #4 alternate between $I_0(p)$ and $I_1(p)$ randomly with transition probabilities for pool #3 $P_{10}=55.5 \cdot 10^{-5}$ (i.e. probability of moving from state I_1 to I_0 in a simulation step of 1s) and $P_{01}=3.7 \cdot 10^{-5}$ (i.e. probability of moving from state I_0 to I_1) and for pool #4 $P_{10}=9.25 \cdot 10^{-5}$, $P_{01}= 1.32 \cdot 10^{-5}$. Based on these probabilities, the average duration of the high interference state is 0.5h for pool #3 and 3h for pool #4 while the average duration of the low interference state is 7.5h for pool #3 and 21h for pool #4. With this configuration, the achievable bit-rate by one link in pools 1 and 2 is $R(l,1)=R(l,2)$=512 Kbps, while for pools 3 and 4, it alternates between $R(l,3)=R(l,4)$=1536 Kbps for the $I_0(p)$ state, and $R(l,3)= R(l,4)$=96Kbps for the $I_1(p)$ state.

6.3.1.2 Evaluated signalling procedures

To evaluate the C4MS signalling requirements, the evaluation focuses on the ON creation stages, executed whenever a new link has to be established in the scenario, the ON maintenance stage, intended to modify the spectrum assigned to a given link (this can be due to degradations of the interference observed in a currently allocated link or to the release of another link in use), and the ON termination stage, in which a radio link of the ON is released. In all the cases, the MIH implementation of C4MS is considered. Each time that one of these procedures is executed, the message exchanges presented in Figure 60, Figure 61 and Figure 62 are considered. It is worth mentioning that it is assumed that all procedures are successfully completed from the perspective of signalling (i.e. the result_codes for all procedures are successful and thus no repetitions of messages are needed).

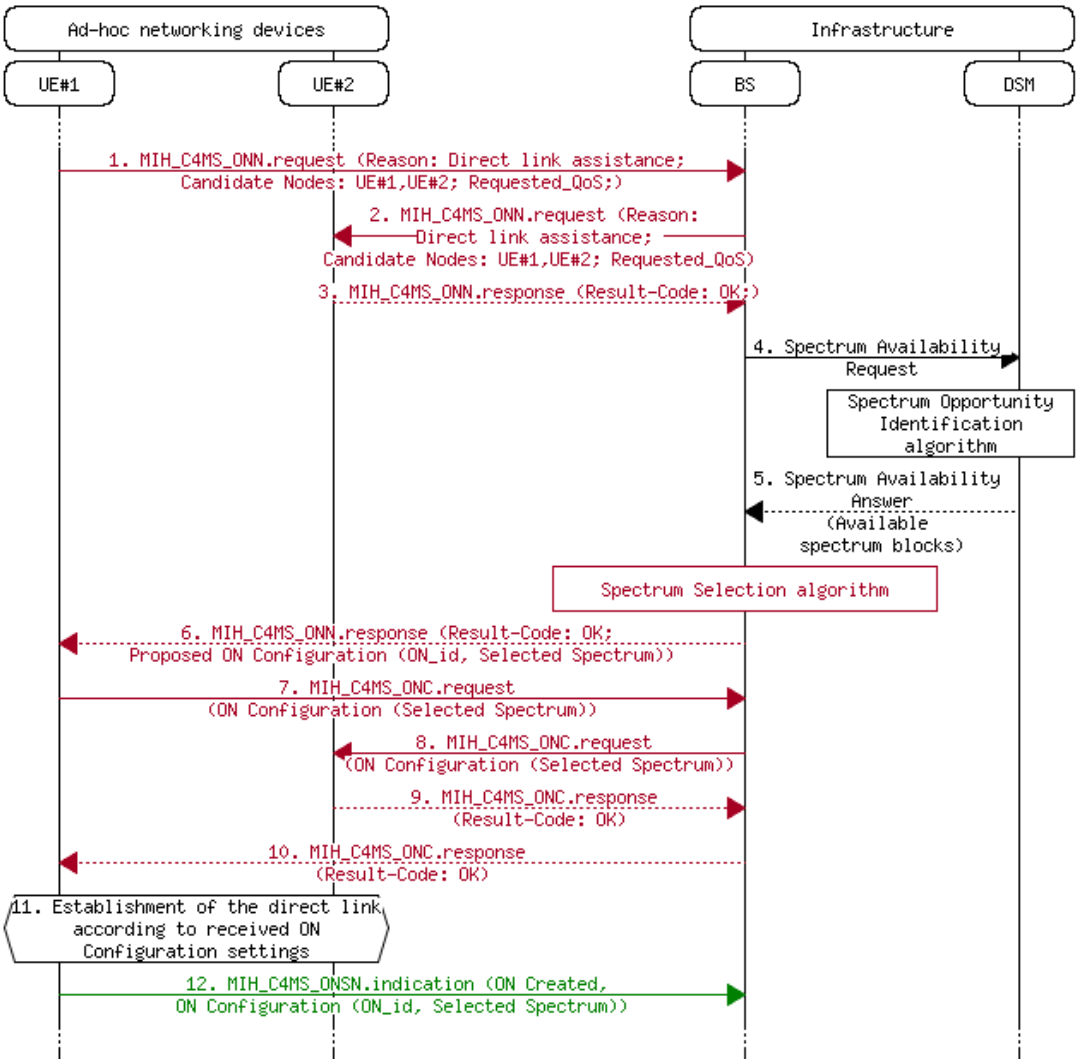

Figure 60: Signalling message flow for ON creation.

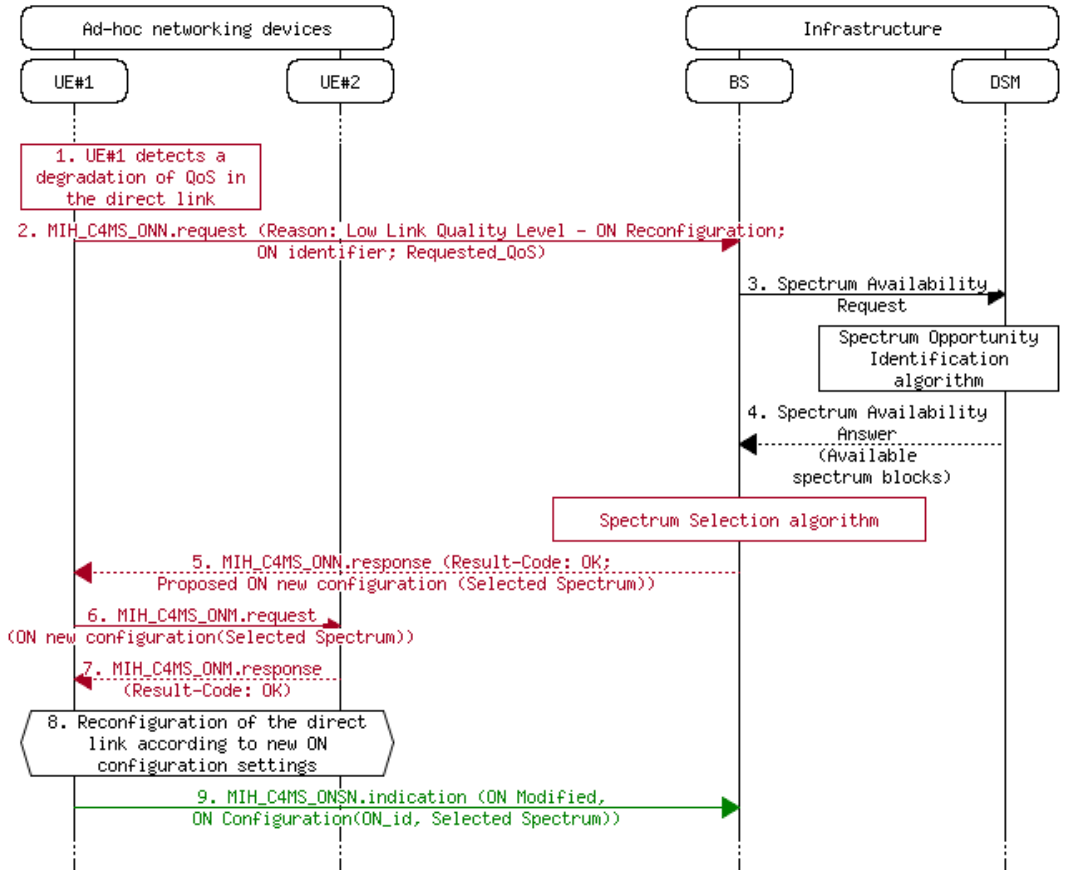

Figure 61: Signalling message flow for ON modification.

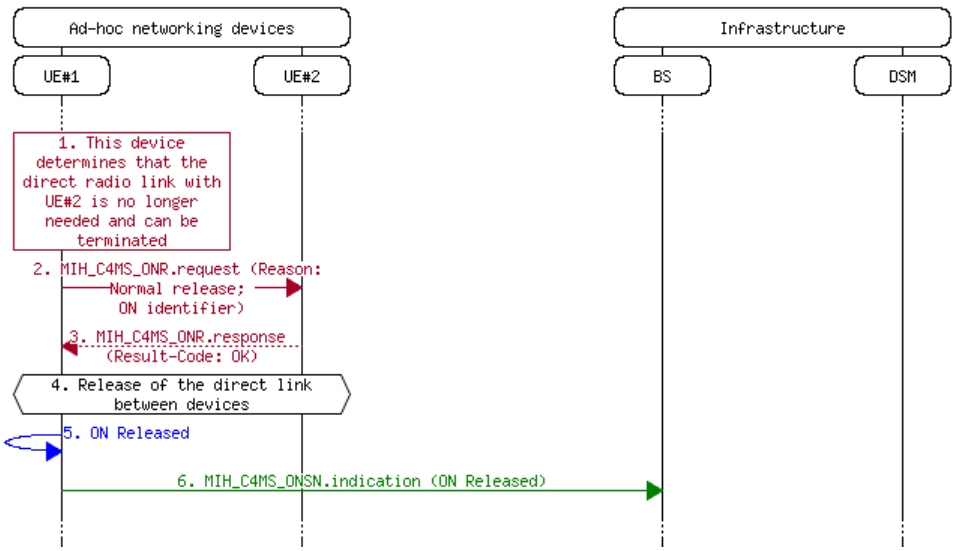

Figure 62: Signalling message flow for ON release.

6.3.1.3 Benchmarking schemes

The following two schemes will be considered in the analysis:

- Spectrum selection supported only by Knowledge Manager (SS+KM): This is the proposed fittingness factor-based spectrum selection supported only by the Knowledge Manager (KM) (see section 2.4 of [5]) but without spectrum handover support, so no ON modification

procedures are triggered. This will allow analysing the signalling associated to the ON creation and release procedures.

- Spectrum selection supported by both Knowledge Manager and Spectrum Mobility (SS+KM+SM): This is the proposed complete fittingness factor-based spectrum selection solution proposed in section 2.4 of [5] supported by both the Knowledge Manager block and the Spectrum Mobility (SM) algorithm that checks the convenience of executing spectrum handovers (SpHOs) either after variations in the interference of some spectrum pools or when a given link is released. This will allow analysing the increase of signalling associated to ON modifications.

6.3.1.4 Information management strategies

The context awareness is of major importance to ensure that the network infrastructure domain captures the actual conditions experienced by the diverse radio links supporting the applications. This enables closing the cognitive cycle and letting the decision-making processes at the infrastructure side (e.g., SM) react to any change and, therefore, achieving a highly efficient allocation of radio resources. In general, two different acquisition strategies can be considered, namely a periodic strategy in which context awareness modules at the terminals periodically report measurements to the knowledge database at the infrastructure (see section 2.4 of [5]) or an event-triggered strategy in which measurements reports are only generated when some relevant conditions are met.

In the considered algorithm, an event-triggered acquisition strategy is used based on changes in the measured value of the fittingness factor. Measurement reports in this case are generated only if the currently measured fittingness factor value is in the Low state (see section 2.4 of [5]) and the last reported value of the fittingness factor was High, or vice versa. For comparison purposes, a periodic acquisition strategy in which the measured fittingness factor value is transmitted every ΔT seconds will be also considered.

6.3.2 Signalling message size estimations

Table 30, Table 31 and Table 32 present the total C4MS signalling load for each of the three procedures, to be used in the signalling evaluation. These are based on computing the total size of each of the message in accordance to the specific fields defined in section 2 and in section 2.1 in the Appendix to the D3.3 [10], as well as the contents considered for this evaluation. It should be noted that the source and destination fields, whose length is not specified but is implementation-dependent, have been set to 1 byte. On the other hand, the measurement reports that are exchanged by context awareness modules are sent using a MIH_C4MS_INI.indication message with length 43 bytes.

Table 30: Total C4MS signalling load for the ON creation procedure

Message	Size (bytes)
1.- MIH_C4MS_ONN.request	30
2.- MIH_C4MS_ONN.request	30
3.- MIH_C4MS_ONN.response	21
6.- MIH_C4MS_ONN.response	38
7.- MIH_C4MS_ONC.request	35
8.- MIH_C4MS_ONC.request	35
9.- MIH_C4MS_ONC.response	21
10.- MIH_C4MS_ONC.response	21
12.- MIH_C4MS_ONSN.indication	35
TOTAL	**266 bytes**

Table 31: Total C4MS signalling load for the ON modification procedure

Message	Size (bytes)
2.- MIH_C4MS_ONN.request	34
5.- MIH_C4MS_ONN.response	42
6.- MIH_C4MS_ONM.request	35
7.- MIH_C4MS_ONM.response	21
9.- MIH_C4MS_ONSN.indication	35
TOTAL	**167**

Table 32: Total C4MS signalling load for the ON termination procedure

Message	Size (bytes)
2.- MIH_C4MS_ONR.request	21
5.- MIH_C4MS_ONR.response	21
6.- MIH_C4MS_ONSN.indication	22
TOTAL	**64**

6.3.3 Evaluation metrics

C4MS signalling evaluation in the considered scenario will be given in terms of the following metrics:

- Total signalling load: Amount of C4MS signalling data per unit of time transmitted in the scenario. Measured in Bits/s.
- Relative signalling load: Amount of C4MS signalling data in relation to the total amount of information data transmitted in the network. The metric is an indication of the bandwidth resources that are consumed by the signalling for the purpose of ON management.
- Signalling load per session: Average C4MS signalling data transmitted during the time that a certain ON link is active to support an application session. This includes all the signalling needed for ON creation, ON maintenance and ON release.

6.3.4 Signalling load evaluation

Figure 63 and Figure 64 present the comparison between the two benchmark schemes SS+KM and SS+KM+SM in terms of the total signalling load and the relative signalling load considering all the links that have been established in the scenario. In all cases the context acquisition follows the event-triggered scheme. The first observation that can be done is that the total signalling overhead is very low. Even for the highest considered loads the overhead is just of 50 bits/s. The main reason for this is that the different procedures involving signalling, namely the link establishment at ON creation, the ON maintenance and the link release, occur at time scales in the order of minutes, related with the duration of the different sessions and with the variations of the interference. Correspondingly, the signalling requirements are very low, while at the same time allowing a good performance (see section 3.5 in [5] for the evaluation in terms of application performance). Notice also in Figure 64 that the signalling overhead relative to the total information data transmitted reaches very low values in the order of $3 \cdot 10^{-5}$ %.

A second observation to mention in Figure 63 is the influence of the Spectrum Mobility (SM) functionality. As it can be noticed, its use leads to a slight increase in the signalling overhead with respect to the SS+KM case when no spectrum mobility is considered. This increase occurs mainly at high traffic loads beyond 1.4 Mbps approximately. The reason is that, for these high loads, it occurs very often that the preferred spectrum pool by a certain link is already occupied at link establishment. As a result of this, spectrum handover events will be triggered when the link

occupying the preferred pool is released, enabling the reallocation of the pool to another link. On the contrary, for low loads, spectrum mobility events are mainly related with variations in the interference experienced in the different allocated pools. In spite of the higher total signalling overhead with SS+KM+SM, when looking at the results in terms of the relative signalling in Figure 64, it can be noticed how SS+KM+SM has actually a slightly lower percentage of signalling than SS+KM. The reason for this behaviour is that, thanks to the adaptation capability introduced by SM, the total amount of useful information (i.e. payload) that can be successfully transmitted with SS+KM+SM is a bit higher than the one obtained with SS+KM (see section 3.5 in [5] for details about the evaluation in terms of performance), and correspondingly the ratio between signalling overhead and useful information (payload) is slightly better with SS+KM+SM.

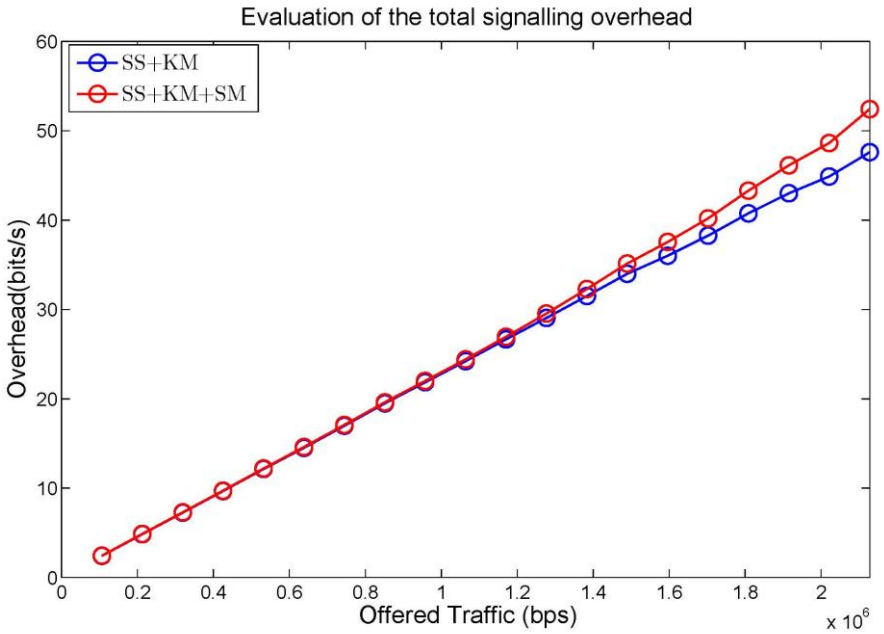

Figure 63: Total signalling load for the two spectrum selection schemes.

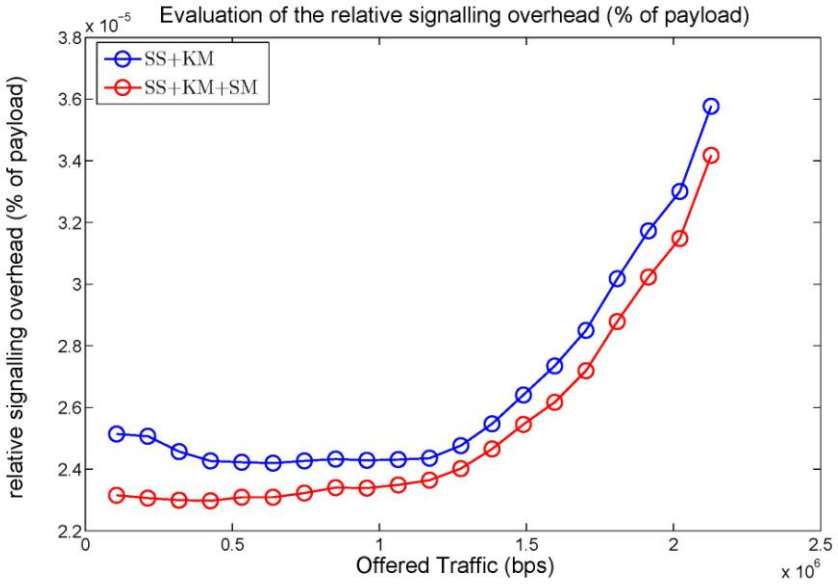

Figure 64: Signalling load relative to the total amount of information data transmitted in the network (i.e. payload) for the two spectrum selection schemes.

Figure 65 presents the comparison between SS+KM and SS+KM+SM in terms of the signalling load per session. This gives an idea of the amount of signalling bits that are required to establish, release and maintain an ON link to support a certain application. As it can be observed, the amount of required bits is also quite small, in the order of 2650 bits for low traffic loads. It can be seen in the figure that, for low loads, the amount of signalling is approximately constant. This corresponds mainly to the ON creation and ON release signalling for the SS+KM plus some additional overhead related with the ON maintenance for the SS+KM+SM scheme that executes spectrum mobility. In turn, for high loads, in the case of SS+KM there exists an increase in overhead associated to the transmission of measurement reports. Since an event-triggered scheme is used, measurement reports are only sent when changes in the interference occur for active links. Then, for high loads it is more likely that these interference changes occur during the link activity and correspondingly they have to be reported, thus increasing the average signalling overhead per session. In the case of SS+KM+SM, in addition of this effect, there is an increase due to the signalling associated to the spectrum handovers. In any case, results reflect that the additional overhead introduced by the proposed strategy (SS+KM+SM) with respect to SS+KM is below 10% even for a very high traffic load. This is due to the low number of SpHOs per session actually incurred by SS+KM+SM.

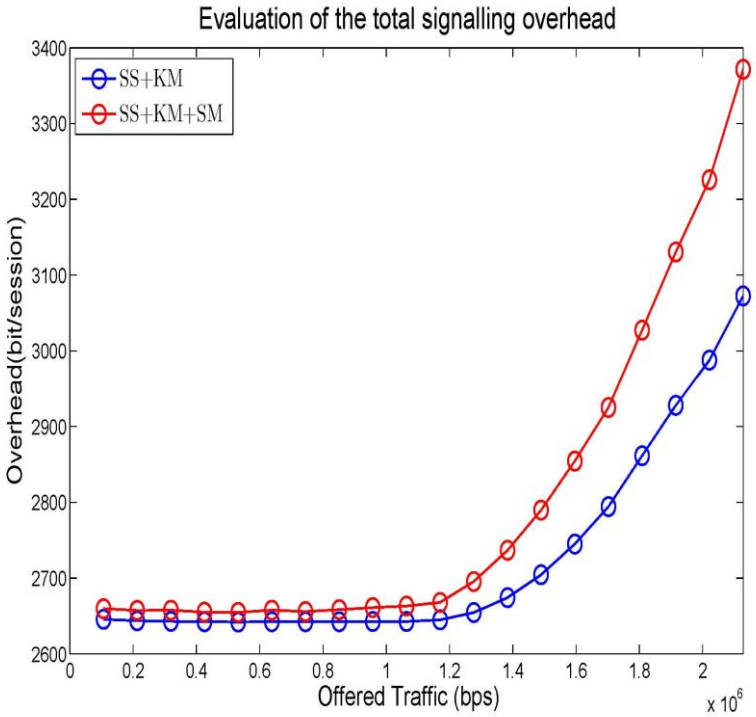

Figure 65: Signalling load per session for the two spectrum selection schemes.

In the following, the effect of the information management strategies discussed in section 6.3.1.4 is analysed. Figure 66 presents the comparison between the event-triggered and the periodic acquisition strategies for different values of the ΔT period. Only the signalling associated to measurement reports is considered. Results are presented for two different total traffic loads, namely 0.1 Erlangs and 1 Erlang, and correspond to the proposed SS+KM+SM strategy. It can be observed how the use of the proposed event-triggered scheme allows a very important reduction in signalling overhead, in different orders of magnitude, particularly for low values of ΔT. Then, as ΔT increases, the signalling overhead associated to the periodic scheme decreases. It is worth mentioning that the reduction achieved by the event-triggered scheme does not compromise the performance in terms of dissatisfaction probability for the different links (see section 3.5 in [5] for the evaluation in terms of application performance).

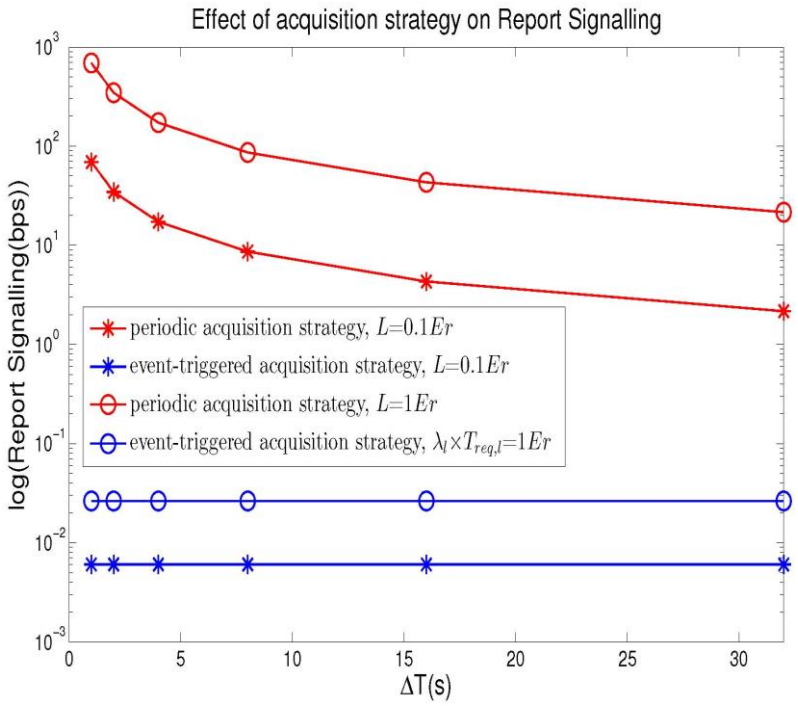

Figure 66: Impact of acquisition strategy in terms of report signalling requirements

In the following the impact of varying the interference pattern and the mean holding time of the different links is analysed. Figure 67 presents the comparison in terms of signalling overhead in bits per session dissatisfaction probability with the proposed SS+KM+SM approach for three interference conditions, namely the reference case that has been considered in the previous study, the case 2 in which all the average durations of the interference patterns have been divided by 4 with respect to the reference case, and the case 3 in which all the average durations have been divided by 8. As a result, cases 2 and 3 correspond to situations with faster variation in the interference. It can be observed how the faster variation in the interference turns into a slight increase in terms of signalling overhead. This increase is due to the higher number of situations in which the interference changes during an active session, which lead, on the one hand to an increase in the number of measurement reports, and on the other hand, to an increase in the number of ON modification procedures. In Figure 68 the same comparison in terms of the signalling associated to measurement reports is presented. The increase in this figure is more noticeable, because the number of events to be reported by an active session increases roughly proportionally with the reduction in the duration of the interference durations for cases 2 and 3. However, since the absolute values of signalling requirements associated to the reports are much lower than the ones associated to the rest of ON procedures, the increase in terms of total signalling is less significant, as it was observed in Figure 67. It is worth also mentioning that, as discussed in [5], the modification in the duration of the interference periods does not have significant impact on the performance in terms of dissatisfaction probability, which reveals the robustness of the proposed algorithm.

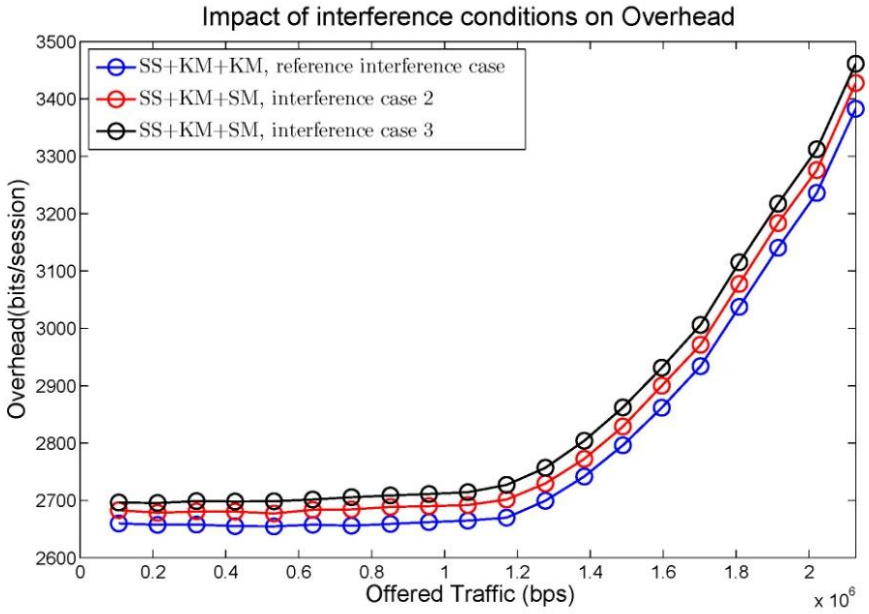

Figure 67: Impact of interference conditions on the signalling load per session

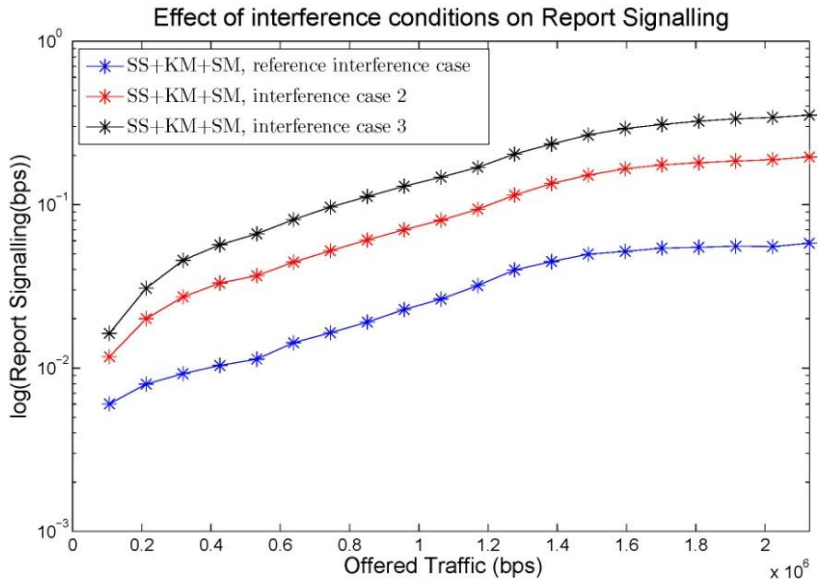

Figure 68: Impact of interference conditions on reporting signalling

Focusing on the variation of the session duration, some results are obtained comparing the performance of the reference case against the case when the session duration is multiplied by 3 or divided by 3 for both links. Interference conditions are those of the reference case in previous studies. Figure 69 plots the comparison in terms of the signalling load per session. It can be observed how the total signalling per session suffers a slight increase when multiplying by 3 the session duration. The reason is that, with longer sessions, it is more likely that an active session experiences a change in interference with the consequent increase in reporting signalling and in ON modification procedures. On the contrary, the session duration has a significant impact in terms of total signalling load in the scenario, as depicted in Figure 70. It can be observed that, for a given traffic level, a reduction in the session duration turns to an increase in the total signalling overhead. The reason is that, given the traffic level, shorter sessions mean more ON creation and ON release procedures, which significantly contribute to the total signalling overhead. In any case, the signalling requirements still reveal to be very small.

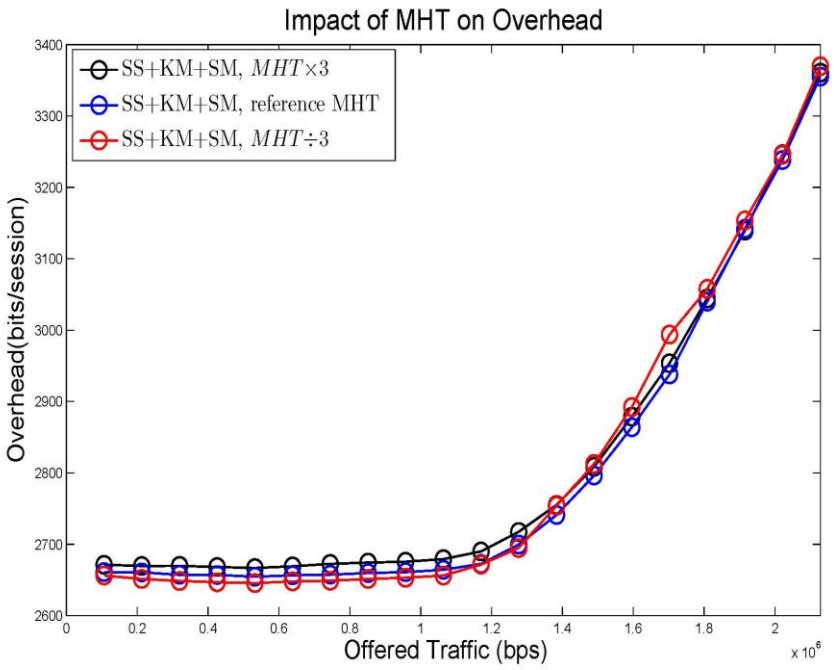

Figure 69: Impact of session duration in terms of signalling load per session

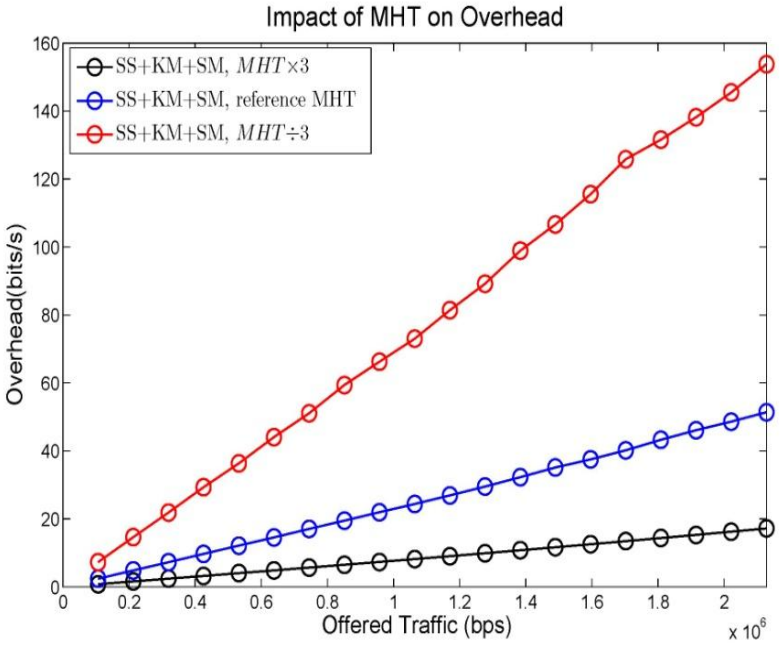

Figure 70: Impact of session duration in terms of total signalling load

6.3.5 Conclusions

As a conclusion to this section, the results of evaluating the fittingness factor-based spectrum selection algorithm in terms of signalling load have revealed that in general the total signalling requirements associated to the different procedures are very low, in the order of 50-100 b/s for the highest traffic considered and depending on the duration of the involved sessions since shorter sessions increase the total signalling for a given traffic value. In any case, these values are much lower than the total payload data transmitted (relative signalling overhead is in the order of $3 \cdot 10^{-5}$

%). Results have also analysed the impact of spectrum mobility in the overall process, and the associated signalling increase due to the resulting ON modification procedures. It has been obtained that the increase due to spectrum mobility is particularly relevant at high loads, when spectrum mobility is executed to reallocate the spectrum pools that some released links have left available. In general the increase in terms of signalling due to spectrum mobility is in the order of 10% for high traffic loads. Finally this section has also analysed the effect of acquisition strategies, by comparing a periodic acquisition against an event-triggered strategy. It has been obtained that the use of the event-triggered scheme turns into a very important reduction in the signalling overhead with respect to the periodic case and that this improvement is achieved without compromising the performance in terms of dissatisfaction probability.

6.4 Techniques for Aggregation of Available Spectrum Bands/Fragments

6.4.1 Evaluation model, scenario and information management strategies description

6.4.1.1 General description of the evaluation model and scenario

The problem considered here is the spectrum selection with spectrum aggregation (SA) capabilities for the link established between nodes in ONs. While aggregated spectrum is allocated to users to satisfy the requested throughput requirement, multiple factors are considered simultaneously; 1) maximization of the total throughput, 2) minimization of channel switching, and 3) the minimization of complexity by spectrum aggregation. Since system is assumed to have set/pre-defined thresholds for each performance metric based on system level Key Performance Indicators (KPIs) to be met, the proposed algorithm operates adaptively with the machine learning module depending on the environment changes (e.g. PU appearance). Thus, the performance of each objective remains close as possible to the pre-defined thresholds.

The pre-defined thresholds for each performance metric based on KPIs are given for the algorithm. As the input, the algorithm uses the available spectrum information resulting from the spectrum opportunity identification, together with the characteristics of each available spectrum in terms of available bit rate. The algorithm makes use of the weighted-sum utility function to consider the multi-objective to capture how suitable a set of aggregate spectrum pool is for a link of a certain QoS requirement. The detail of the algorithm is described in D4.2 [5].

The evaluation of the C4MS signalling load in this scenario will be based on the same simulation model that is being used for the performance evaluation carried out in WP4. It is evaluated by means of the Matlab simulations. The scenario is characterised by the following:

- Traffic characterisation: In order to simulate the opportunistic spectrum access, PU traffic modelled through the On/Off process with the unit of a channel of 200 kHz width is generated. Since the number of secondary users is variable for the performance evaluation, service time follows a uniform distribution with the mean 5secs. Once finishing the service time of a certain link, the link is terminated and new link appears to request the resource. Each link in the ON is assumed to require 5 Mb/s during the service time.
- Spectrum characterisation: It is assumed that 30 MHz is available for 4 different bands. The average spectrum occupancy by primary users is set to 50%.

6.4.1.2 Evaluated signalling procedures

The evaluation of the C4MS signalling load focuses on the ON creation stages [executed whenever a new link has to be established requiring spectrum allocation] and the ON reconfiguration/maintenance stage [to modify the spectrum assigned to a given link (this can be due to degradations of QoS in a currently allocated link or to the release of another link in use, appearance of primary users)]. In both cases, the MIH implementation of C4MS is considered. Each time that one of these procedures is executed, the message exchanges presented in section 6.3 Figure 59 for ON Creation and Figure 61 for ON modification are also considered with regard to this section.

6.4.1.3 Benchmarking schemes

The proposed utility-based spectrum aggregation algorithm can adaptively adjust the weights of each performance metrics with the learning module depending on the environment changes (e.g. PU appearance). In order to evaluate the signalling overhead of the proposed algorithm, the utility-based aggregation algorithm without the machine learning is considered as the reference approach for the performance comparisons/benchmarking. The reference scheme without the learning module will use the equal-weights all the time regardless of the environment changes. The following two schemes are considered in the signalling overhead analysis:

- The utility-based spectrum aggregation algorithm without machine learning (No-Learning)
- The utility-based spectrum aggregation algorithm with machine learning (Proposed)

6.4.1.4 Information management strategies

In the proposed aggregation algorithm, an event-triggered strategy is used to react to changes in interference levels of active links, PU appearance or drop in QoS. So at high loads it is more likely that such triggers occur more frequently during the link lifetime and since they are reported, average signalling overhead per session increases.

6.4.2 Signalling message size estimations

Table 30 and Table 32 present the total C4MS signalling load for each of the two procedures, used in the signalling evaluation. These are based on computing the total size of each of the message in accordance to the specific fields as well as the contents considered for this evaluation. It should be noted that the source and destination fields, whose length is not specified but is implementation-dependent, have been set to 1 byte.

Table 33: Total C4MS signalling load for the ON creation procedure

Message	Size (bytes)
1.- MIH_C4MS_ONN.request	32
2.- MIH_C4MS_ONN.request	32
3.- MIH_C4MS_ONN.response	21
6.- MIH_C4MS_ONN.response	38
7.- MIH_C4MS_ONC.request	26
8.- MIH_C4MS_ONC.request	26
9.- MIH_C4MS_ONC.response	20
10.- MIH_C4MS_ONC.response	20
12.- MIH_C4MS_ONSN.indication	35
TOTAL	**250 bytes**

Table 34: Total C4MS signalling load for the ON modification procedure

Message	Size (bytes)
2.- MIH_C4MS_ONN.request	34
5.- MIH_C4MS_ONN.response	42
6.- MIH_C4MS_ONM.request	26
7.- MIH_C4MS_ONM.response	20
9.- MIH_C4MS_ONSN.indication	35
TOTAL	**157**

6.4.3 Evaluation metrics

C4MS signalling evaluation results are given in terms of the following metrics:

- Total signalling load: Amount of C4MS signalling data per unit of time transmitted in the scenario. Measured in Bits/s.
- Relative signalling load: Amount of C4MS signalling data in relation to the total amount of information data transmitted in the network. The metric is an indication of the bandwidth resources that are consumed by the signalling for the purpose of ON management.

6.4.4 Signalling load evaluation

Figure 71 and Figure 72 present the comparison between the benchmark scheme (No-Learning) and the proposed algorithm (Proposed) in terms of the total signalling load and the relative signalling load considering all the links that have been established in the scenario.

In Figure 71, it is observed that the signalling overhead increases as the offered traffic increases. At low traffic load, the signalling overheads of two algorithms are the same. From the traffic offer of 15Mbps, the proposed algorithm (Proposed) outperforms by generating less signalling than the algorithm without learning (No-Learning). In the scenario considered, the network can accommodate the traffic up to 15Mbps. For the case of the less traffic than 15 Mbps, when the operation condition changes, the pre-defined threshold of each performance metric can be satisfied. For example, when PU appears more frequently and the number of channel switching of SUs increases, the increased number of channel switching can be still lower than the pre-defined threshold of channel switching number. Then, for the case of lower traffic (e.g. up to 15 Mbps), the learning module will not be triggered in the proposed algorithm. For the case of the increased traffic load (i.e. higher than 15 Mbps), when PU appears and it leads to increasing the channel switching, it is highly probable that the increased number of channel switching becomes larger than the pre-defined threshold. Then, the machine learning module will be triggered to optimize the multi-objective spectrum allocation & aggregation algorithms. While other performance metrics are optimized, the proposed algorithm tries to reduce the number of channel switching. Thus, it is observed that the signalling overhead of the proposed algorithms with the learning module is lower than the proposed algorithm without learning for the higher traffic (i.e. from 15 Mbps).

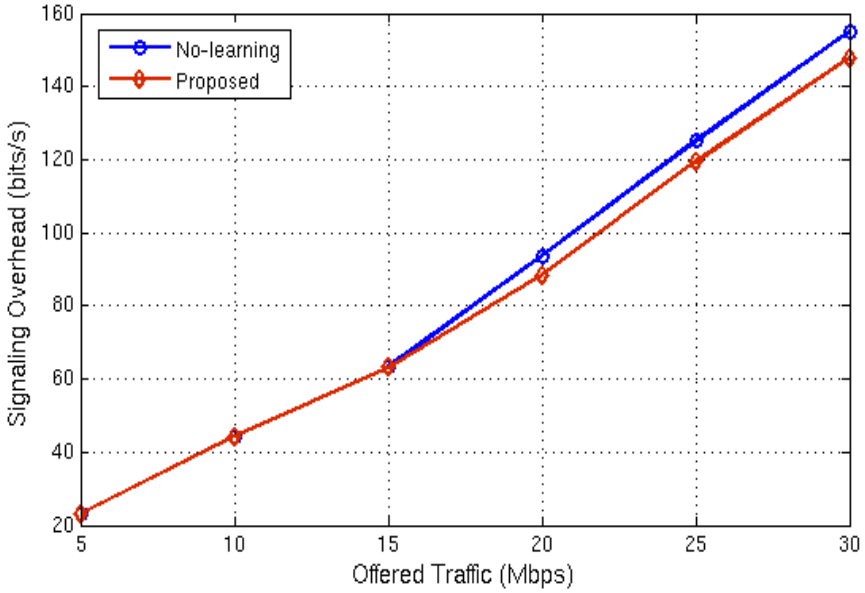

Figure 71: Total signalling load for the two spectrum selection schemes

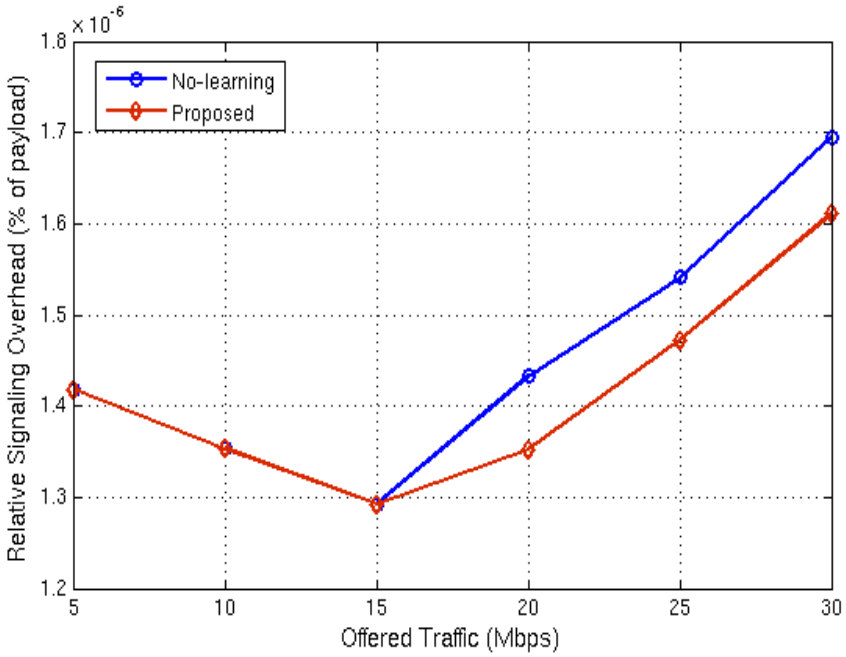

Figure 72: Signalling load relative to the total amount of information data transmitted in the network (i.e. payload) for the two spectrum selection schemes

In Figure 72, the relative signalling overheads (defined the ratio of the amount of signalling overhead to the size of payload) of two algorithms are compared. At the low traffic load, it is observed that the relative signalling overhead decreases. Actually, when the traffic load increase, the signalling overhead increases as shown in Figure 71. At the case of traffic load up to 15 Mbps, the achievable data rate increases as the offered traffic load increases. Thus, it leads to decrease the relative signalling overhead. However, for the high traffic (larger than 15 Mbps), when the signalling overhead increases, the achievable data rate does not increase. It makes to increase the relative signalling overhead for the increase of the traffic load. In this case, the proposed algorithm also outperforms in terms of the relative signalling overheads since the proposed algorithm reaction is to maximize the total throughput and to reduce the number of channel switching.

6.4.5 Conclusions

Based on results provided it can be concluded that:

- the machine learning which is adopted by the proposed algorithm helps reduce the signalling overhead;

- the signalling overhead will be affordable although it increases with an increase of the offered traffic.

6.5 Algorithm on knowledge-based suitability determination and selection of nodes and route

6.5.1 Evaluation model, scenario and information management strategies description

Table 35 illustrates scenario specific aspects which have been considered for the capacity extension through neighboring terminals scenario. These aspects include generic scenario aspects such as world size, mobility patterns, propagation models etc. Also, terminal and BS/AP related aspects are taken into account such as total number of terminals and BSs considered, network interfaces supported, location of terminals and BSs etc. Finally, some ON-specific aspects are described such as the size of ONs.

Table 35: General scenario aspects for coverage extension through neighboring terminals

General scenario aspects	
ON phase considered	
Scenario size	4000m x 4000 m (but it can be configurable)
Mobility of terminals	speed within range and with various models, e.g. random walk (average velocity: 0, 1 or 2 m/s)
Signal propagation model	WINNER 5bf, Okumura-Hata, Friis model
Traffic model	variable packet sizes, and intervals (terminals are grouped and each group creates a message with a mean of 5 secs. The created message every time has different size which ranges from 64kB to 1MB (uniform distribution). Of this can also be configured to be constant or to have a different range)
Terminal related aspects	
(Total) number of terminals in scenario	Configurable (usually around 130)
Number of ON capable terminals (Fraction of ON capable terminals in the scenario)	Configurable (usually around 40)
Location of terminals (distribution of terminal)	Configurable but usually a proportion is configured to be near the edge and the others are uniformly distributed
Network interfaces supported by terminals	1 long-range (range of 800m) 1 short-range (range of 100m)
BS / femto / AP related aspects	
(Total) Number of Base Stations /	7 BSs

femtocells / access points in scenario	
Number of ON capable Base Stations/ femtocells / access points (Fraction of ON capable Base Stations/ femtocells / access points)	configurable
Location of BS/femtos/APs (distribution of BSs/femtos/APs)	configurable
Network interfaces supported by BSs/femtocells/access points	1 long-range interface (range for BSes – 800m, for femtocells up to 150m)
Opportunistic Network related aspects	
Maximal size of ON	3 hops
Fraction of nodes which are in ON at simulation start (number of terminals, number of BSs/Femtos/APs)	0 – the simulation starts without pre-created ONs. All terminals are directly connected to BSs.

6.5.2 Verification scenario for the capacity extension

Specific MSCs have been defined in D3.2 for capacity extension through neighboring terminals. In this scenario it is assumed that a BS experiences congestion issues. This is BS#1. Moreover, it is assumed that the terminal UE#1 is registered to the problematic BS#1. There is also a non-congested BS in the area (BS#2). Finally, it is assumed that UE#2 is close to UE#1. UE#2 is located into the non-congested area (BS#2) and can act as an intermediate node in order to redirect traffic from terminals in the congested area to terminals in the non-congested area.
Illustrations from Figure 73 to Figure 76 provide the sequence of the exchange messages during the phases of suitability determination, creation, maintenance and termination respectively.

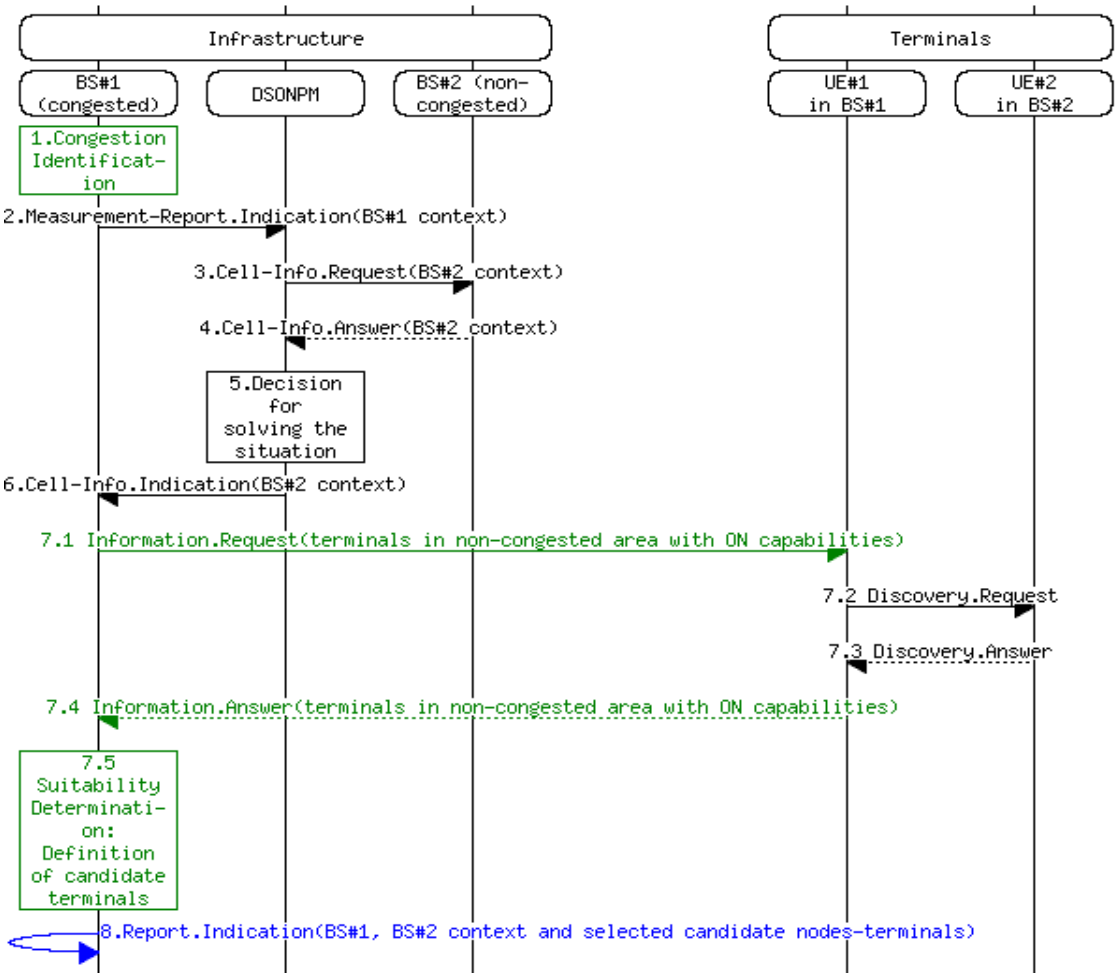

Figure 73: Capacity extension through neighboring terminals; Suitability determination phase.

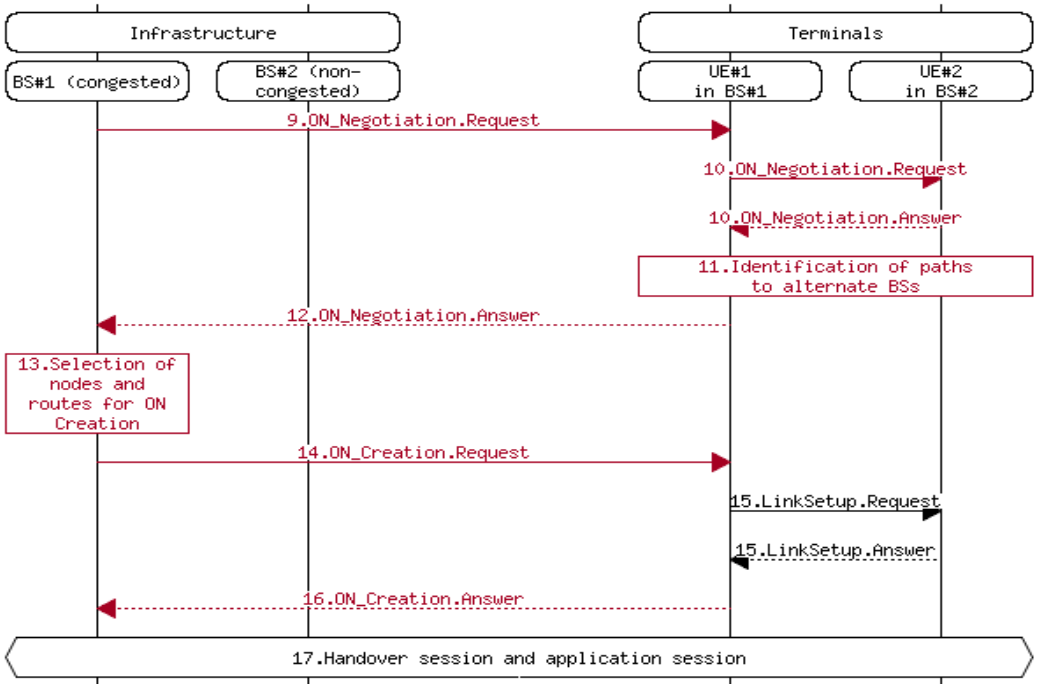

Figure 74: Capacity extension through neighboring terminals; Creation phase.

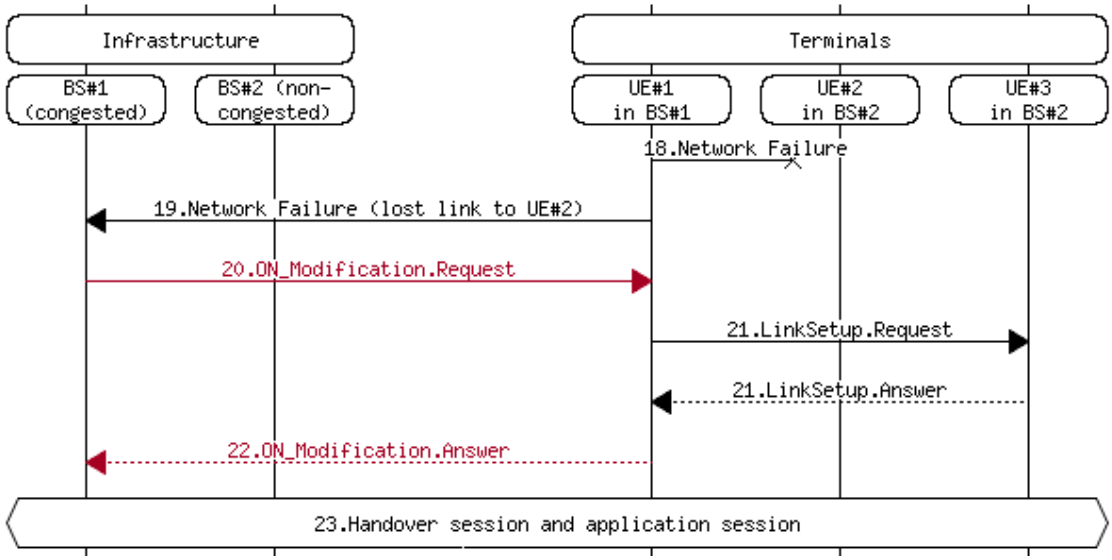

Figure 75: Capacity extension through neighboring terminals; Maintenance phase.

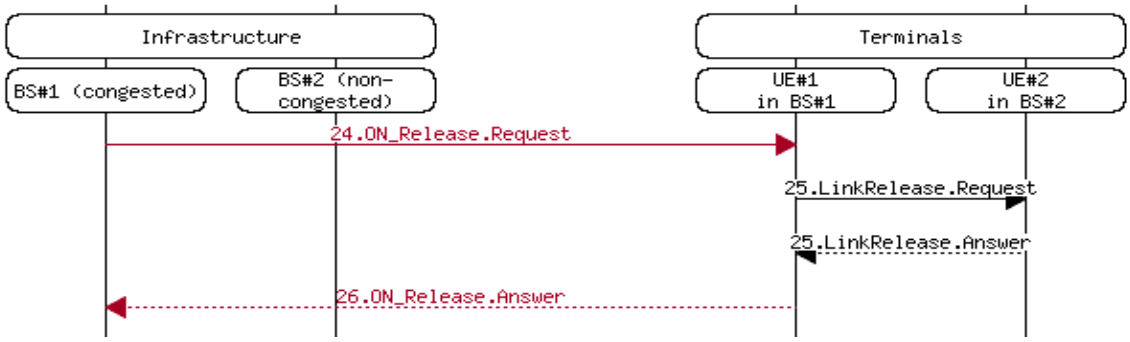

Figure 76: Capacity extension through neighboring terminals; Termination phase.

6.5.3 Information management strategies

The information management strategies considered in this approach depend on the phase. For example, during the suitability determination and creation phase necessary profile and context information are being exchanged in a trigger-based manner upon request. This means, that as soon as a problem occurs (e.g. congestion identification) the respective functional entities will be informed in order to initiate the procedure for the establishment of an ON. On the other hand, during the maintenance phase, information could be exchanged in a trigger-based (upon request) or periodical manner in order to monitor the status of the formed ON and potentially proceed to reconfiguration, if needed. Finally, in the case of the ON termination, necessary release messages are exchanged in a trigger-based manner. For example, if the operator dictates that the ON is no longer needed, or neighboring users can no longer support a formed ON, then the procedure of the termination will be executed.

6.5.4 Signalling load evaluation

Signalling load in this section has been estimated according to analytical models. The models take into account the contents of each data structure as defined in Sections 3 and the appendix to D3.3, section 3 [10]. According to the assumed scenario the following input parameters are considered: 7 Base Stations (1 congested, 6 neighboring, non-congested) and 130 terminals (40 in the congested BS, 15 to each non-congested). Also, each BS has 1 interface and 1 RAT per interface, each terminal has 2 interfaces and 1 RAT per interface. Moreover, each terminal has 1 active application and 2

links with neighboring nodes (BS or terminal). To that respect, the associated signaling load for each phase of the ON is as follows:

Table 36: Associated signalling load of the scenario

ON Phase	Signaling load	
Suitability determination and creation	48 KB	
Maintenance	(Terminal_Context)245B*12 terminals≈3KB	
	5-sec period 3KB/5sec=0.6KB/s	30-sec period 3KB/30sec=0.1KB/s
Termination (for a single termination procedure)	24 B	

It is noted that during the maintenance phase a periodical exchange of messages is considered compared to the other phases which are triggered based. For the periodical exchange a 5-sec period of transmission and a 30-sec period of transmission are considered. In the first case the associated signaling load should raise up to 0.6 KB/s while in the latter case the load drops to around 0.1 KB/s. In both cases it is assumed that only the terminals which participate in the ON are transmitting their context every 5 or every 30 seconds. This is needed in order to verify the current status of each terminal and whether it is still suitable for the ON or not. Finally, a single termination procedure (i.e., load needed to terminate one ON out of *x* created ONs) is evaluated. The procedure is estimated to be 24 bytes and it is triggered upon request from the operator.

6.5.5 Conclusions

According to the previously mentioned evaluations, it is shown that for a network of 7 BSs and 130 mobile terminals the signaling load for the phases of the ON remains rather low (some tens of KBs) compared to the actual traffic of data (which could be hundreds of KBs or several MBs). To this respect, C^4MS is seen as a viable solution which does not impose large overhead to the network due to flooding of signaling messages. Moreover, it should be considered that suitability determination and creation phases could be triggered-based (i.e., initiated by the operator as soon as there is a specific problem to the network –e.g. capacity; coverage problems etc.). In the maintenance phase, messages could be exchanged in a periodical manner, but the exchanged information is limited to some context data (e.g. profiles, policies have been acquired from the previous phases, so it is not necessary to resend it). Finally, the termination phase could be also triggered-based according to the decision made by the operator (unless the network experiences a sudden failure).

6.6 Application cognitive multi-path routing in wireless mesh networks

6.6.1 Evaluation model

Application cognitive multi-path routing in wireless mesh networks algorithm copes with the route selection and establishment of appropriate set of multiple paths in the wireless backhaul side of the wireless mesh networks (WMNs). The main goal is to opportunistically aggregate the backhaul bandwidth and provide it on the access side of a heavily loaded access points (APs) in order to provide higher backhaul bandwidth utilization and balance the load. The algorithm takes into account: 1) topology of the underlying WMN, 2) backhaul traffic patterns, 3) status of the WMN backhaul links and 4) bandwidth requests at access side of the WMN APs.

Proposed solution makes use of Optimized Link State Routeing (OLSR) as underlying single-path routing protocol in the WMN. Necessary contextual data is gathered from WMN nodes with Simple Network Management Protocol (SNMP is defined in a set of documents: from RFC 3411 [16] to RFC 3418 [17]). Decision making algorithm resides on the centralized management server, which also

monitors network status/state with SNMP protocol and stores gathered contextual data into database. This database contains current and historical contextual data as well as history of previous decision instances. The SNMP is used for gathering not only contextual data, but also OLSR routing tables from which a complete network graph can be constructed.

An exemplary message sequence chart for the algorithm operation is depicted in the Figure 77 below. Noticeably, the majority of the ON related signalling is performed within the centralized management system where the presented algorithm for backhaul bandwidth aggregation resides. Only instructions for routing table modifications and creation of additional backhaul links are sent towards the WMN nodes. These instructions are used for modifying the OLSR routing tables in order to enable creation of multiple paths from WMN APs towards WMN GWs.

Contextual parameters are gathered over the SNMP by the network monitoring process of the network management system. Reconfiguration instructions and parameters are also sent over the SNMP messages from the centralized management towards the WMN nodes. Route discovery and establishment are done with the OLSR routing protocol. More information about the role of the SNMP and OLSR protocols, as variants of the C4MS protocol, can be found in the M5.3 document [9] and for a detailed description of the algorithm please refer to section 2.12 in D4.2 Deliverable [5].

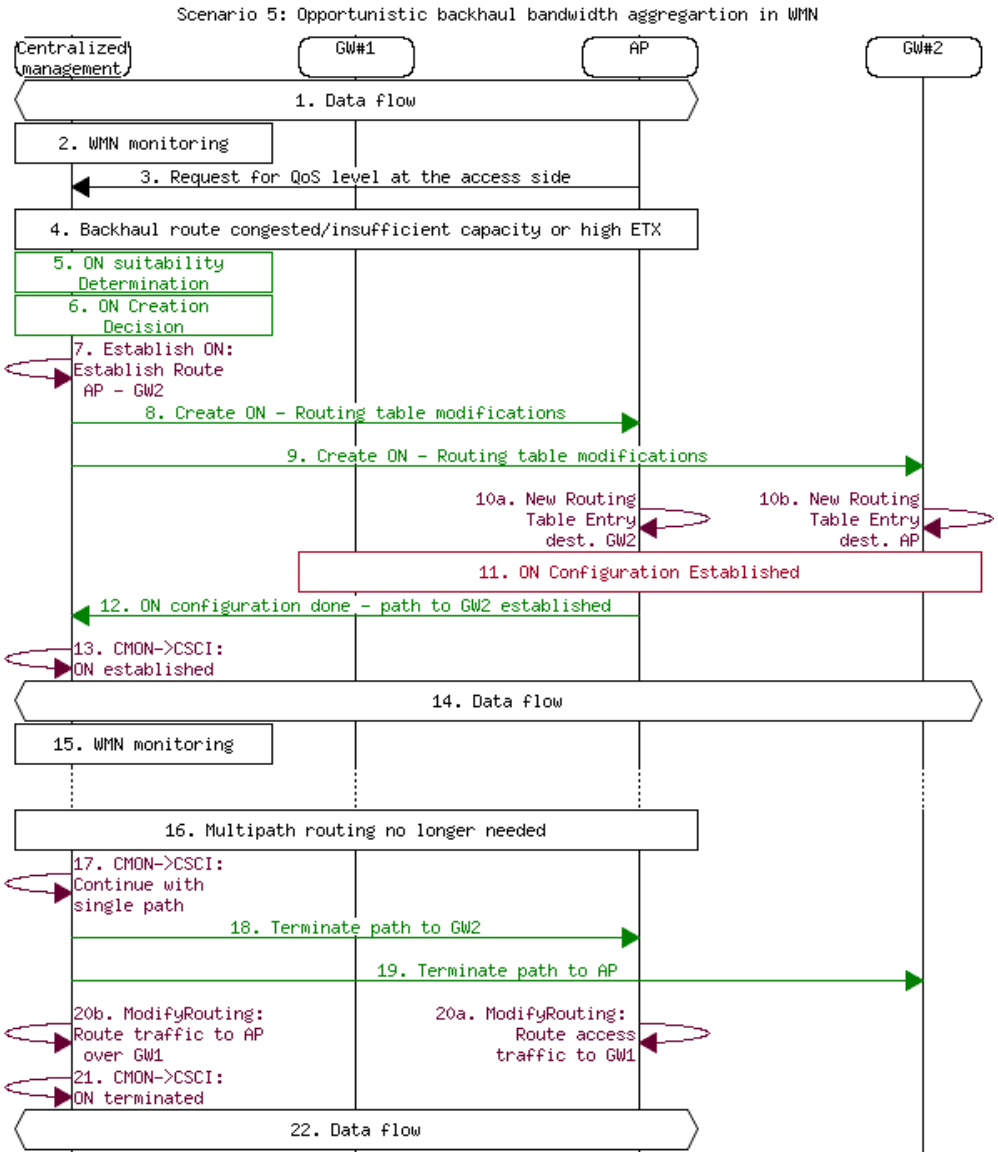

Figure 77: MSC of the backhaul bandwidth aggregation

6.6.2 Verification scenario

For the purpose of signalling evaluation the following general assumptions are made:

- Every mesh router has *i* wireless interfaces. One wireless interface is always used for access side of the network, the remaining (*i-1*), which we will call mesh interfaces, are used for backhaul communication among WMN APs. Thus we can say that the number of active mesh interfaces can vary from 1 to (*i-1*).
- In the multi hop multi channel mesh networks, all active mesh interfaces, belonging to a single node, work on different channels. In order to form a link, two wireless interfaces must work on the same channel. Thus, we can say that the number of neighboring nodes with which mesh node is connected is determined by the number of active mesh interfaces of that mesh node.
  Example: If mesh node has 4 wireless interfaces (1 for access and 3 mesh interfaces), and if only 2 of 3 mesh interfaces are active, it is assumed that mesh node is connected with 2 neighbouring nodes. If the third mesh interface is activated, mesh node will be connected with one more neighbour.

- In order to determine the maximal and the minimal number of wireless links in the network, the graph theory is used. A mesh network is considered as an undirected graph, where number of nodes in the graph corresponds to the number of mesh nodes in the network, and graph node's degree corresponds to the number of active mesh interfaces of corresponding mesh node. Since the graph is undirected, an edge of the graph corresponds to two links in the network.
- The minimal number of links in the network, needed for every mesh node to be able to communicate with the remaining nodes in the network, is determined as the minimal covering tree of the graph and it is given by *2*(n-1)*, where *n* is the number of nodes in the graph. The minimal covering tree of the graph contains *n-1* edges, but since one edge corresponds to two links the expression written above is multiplied by 2.
- The maximal number of links is determined when all mesh interfaces of every mesh node in the network are active. If we assume that every mesh node has the same number of mesh interfaces (*i*), graph that corresponds to the mesh network can be considered as regular graph. In that case the number of edges in the graph is calculated as *(n*i)/2*. In order to determine number of links in the network, previous expression is multiplied by 2, for the same reason which is given in the previous paragraph.

In order to determine the dependency of the signalling overhead generated by the algorithm to different parameters (i.e. size of the WMN and the number of active interfaces), two test cases were investigated in detail:

- Test no. 1
  - 50 nodes are considered in the scenario
  - Each has 4 network interfaces, however only 1, 2 or 3 network interfaces are being turned ON
- Test no. 2:
  - 40, 50, 60, 70 and 80 WMN nodes are considered in the scenario
  - Each node has 4 interfaces

6.6.3 Information management strategies

The parameters exchanged between WMN nodes may be categorized into two groups:

- The fastest changing parameters that include: link cost (ETX value), SINR, Tx and Rx packets, Tx and Rx packet drops, number of clients;
- Parameters that are not changing very often: remote IP (changes as links are established and terminated), interface and its state, mode and used channel (MAC protocols for 802.11a channel selection don't change channel assignments very often for the existing links);

Parameters belonging to the first group should be collected as often as possible for diagnostic purposes.

Parameters such as IP and MAC addresses and interface names can be static and defined by the operator. However these parameters need to be gathered together with fast changing parameters in order to enable their identification (identification to which node/interface the collected parameters belong).

Monitoring system gathers contextual parameters every one minute. Standard monitoring systems that are in commercial use (i.e. PRTG) gather contextual parameters every 5 to 10 minutes. They also have agents located on suitable networking nodes (routers, switches, wireless controllers…) which can report changes in certain contextual parameters when a defined threshold are reached.

6.6.4 Signalling message size estimations

The data collected from one mesh node are:

- Routing table (*RT*)
- Interface table (*IT*)
- Topology table (*TT*)
- Neighbor table (*NT*)
- Link table (*LT*)

Total amount of data collected from one mesh node is the sum of all these tables:

$$PL_x = IT_x + LT_x + NT_x + TT_x + RT_x \qquad (1)$$

We will consider the size of one entry in the corresponding table as constant, and the number of entries in tables as variable.

For mesh network with fixed number of nodes *n*, where every node has the same number of interfaces *i,* equation (1) can be presented as:

$$PL_x = i_x e_{IT} + u_x e_{LT} + u_x e_{NT} + e_{TT} \sum_n u_n + e_{RT} \sum_{n \neq x} u_n \qquad (2)$$

This equation defines how the amount of collected data from a mesh node *x* changes with respect to topology changes and changes in the number of active mesh interfaces of the node *x.*

- PL_x – data payload for node *x* (gathered contextual data),
- i_x – total number of wireless interfaces for node *x*,
- u_x – the number of active mesh interfaces for node *x*,
- $e_{IT}, e_{LT}, e_{NT}, e_{TT}, e_{RT}$ – size of single entry in *interface*, *link*, *neighbor*, *topology* and *routing* table, respectively. As we said earlier, these parameters are considered to be of corresponding constant size.

The first term in the equation (2) represents the size of interface table (*IT*) of the observed node *x*. This term depends only on the total number of wireless interfaces of the observed mesh node, because data regarding interfaces are collected regardless if the interface is active or not.

The second term of the equation (2) represents the size of link table (*LT*) of the observed node *x.* It depends on the number of neighbors of observed node, and the number of neighbours depends on the number of active mesh interfaces of the observed node *x*.

The third term, $u_x e_{NT}$, represents the size of neighbour table (*NT*). The same dependences apply as for the second term.

The forth term in the equation (2) represents the size of topology table (*TT*) of the observed node. The size of this table depends on the number of links in the mesh network. Earlier, it was shown how the number of links can be determined if the number of nodes and the degree of each node is known. Due to the use of OLSR proactive routing protocol, every node in the network has routes to all the remaining nodes in the network, which implies that this table is the same size for every node in the network.

Finally, the fifth term represents the size of routing table (*RT*) of the observed node. The size of this table can be determined based on the number of active mesh interfaces of all nodes in the network except the observed node.

Next we will show parameters in entries of all tables mentioned earlier.

Table 37: Links Table format and fields

Local IP	Remote IP	Hist	LQ	NLQ	Cost

Description:

- Local IP – IP address of the interface via which the node communicates with its neighbor;
- Remote IP – IP address of the neighbor's interface via which it communicates with the node;
- Hist – the current hysteresis value for this link;
- LQ (*Link Quality*) – the link quality (ETX) toward the neighbor determined by the node;
- NLQ (*Neighbor Link Quality*) – neighbor's view of the link quality (ETX value);
- Cost – the ETX value for this link (used by the OLSR protocol), calculated as $1/(LQ * NLQ)$.

Entry size (all of the listed parameters are included) goes between 50 and 60 bytes.

Table 38: Neighbours Table format and fields

IP address	SYM	MPR	MPRS	Will.	2 Hop Neighbors

Description:

- IP address – the main IP address of one neighbor;
- SYM – depicts whether the link to the particular neighbor is considered as symmetric by olsrd's link detection mechanism;
- MPR (multi-point relay) – indicates whether the node has selected this neighbor node to be its MPR;
- MPRS (multi-point relay selector) – indicates whether this neighbor node has selected the node to act as its MPR;
- Will – the neighbor's willingness to act as a potential MPR for a node;
- 2 Hop Neighbors – the number of node's two hops neighbors via the listed neighbor.

Entry size (all of the listed parameters are included) goes between 50 and 60 bytes.

Table 39: Topology Table format and fields

Destination IP	Source IP	LQ	NLQ	Cost

Description:

- Destination IP – the node to which the source node reports the link.
- Source IP – the node that reports a link.
- LQ - the quality of the link as determined by the source node. For the source node this is the Link Quality. For the destination node this is the Neighbor Link Quality.
- NLQ – the quality of the link as determined by the destination node. For the source node this is the Neighbor Link Quality. For the destination node this is the Link Quality.
- Cost – the ETX value for this link, calculated as $1/(LQ * NLQ)$.

Entry size (all of the listed parameters are included) goes between 50 and 60 bytes.

Table 40: Routes Table format and fields

Destination IP	Gateway IP	Metric	ETX	Interface

Description:

- Destination IP – the IP address of the destination node;
- Gateway IP – the IP address of the next hop on the route;
- Metric – number of hops to the destination node;
- ETX – expected transmission count for the route;
- Interface – outgoing interfaces toward the destination node;

Entry size (all of the listed parameters are included) goes between 50 and 60 bytes.

Table 41: Interfaces Table format and fields

Ifname	IP add.	MAC	State	Mode	Channel	SSID	Encryption
Rate	Power	Signal	Noise	Link Q.	TX pkts	TX bytes	
RX pkts	RX bytes	TX pkts drop	RX pkts drop	Clients			

Description:

- Ifname – name of the wireless interface;
- IP address – IP address of the interface;
- MAC – hardware/MAC address of the interface;
- State – current status of the interface (on, off, idle);
- Mode – current mode of the interface (access point, station, ad-hoc);
- Channel – frequency channel (802.11a/b/g) used by the interface;
- SSID – Service Set IDentifier of the interface;
- Encryption – type of encryption used by the interface;
- Rate – transmission bit rate of the interface;
- Power – transmission power of the interface;
- Signal – received signal strength of the interface (RSSI);
- Noise – background noise level;
- Link Q - overall quality of the link;
- TX pkts – number of packets transmitted by the interface;
- TX bytes – outgoing traffic of the interface in bytes;
- RX pkts – number of packets received by the interface;
- RX bytes – incoming traffic of the interface in bytes;
- TX pkts drop – number of dropped packets during transmission;
- RX pkts drop – number of dropped packets during receiving;
- Clients – number of clients connected to the interface (only for those interfaces in AP mode);

Entry size (assuming that all of the listed parameters are included) resides between **80 and 130** bytes.

For a description of C4MS messages suitable for delivering parameters mentioned above please refer to section 3.7 of M5.2 [9]

6.6.5 Evaluation metrics

Considerations in the subsequent section focus mainly on the total load of control information that needs to be exchanged between the nodes enabling proper algorithm operation.

6.6.6 Signalling load evaluation

Figure 1 shows how the amount of data gathered from the mesh node changes with respect to topology (the number of established links) and the number of active interfaces of observed node for mesh network with 50 nodes, where every node has 4 wireless interfaces (1 for access and 3 for backhaul). The number of active interfaces of the observed node increases by 1. The results on the graph are expected since the equation (2) represents linear dependence in which, at each iteration, the first three terms are constant, and the remaining two sums have linear growth.

Let us assume that in the first iteration the observed node has only one mesh interface which is active. This means that it is connected only to one neighbor node. During this iteration the number of neighboring nodes of the observed node will not be changed, which implies that the size of link and neighbor table will remain unchanged. Interface table (*IT*) does not depend on the number active interfaces of a node and it has nearly constant value. As a result, the first three terms in the equations (1) and (2) will be constant. By increasing the number of links in the network by 1, the number of entries in topology and routing table will also be increased by 1. Thus, it is clear that topology and routing table will have linear growth by increasing the number of links.

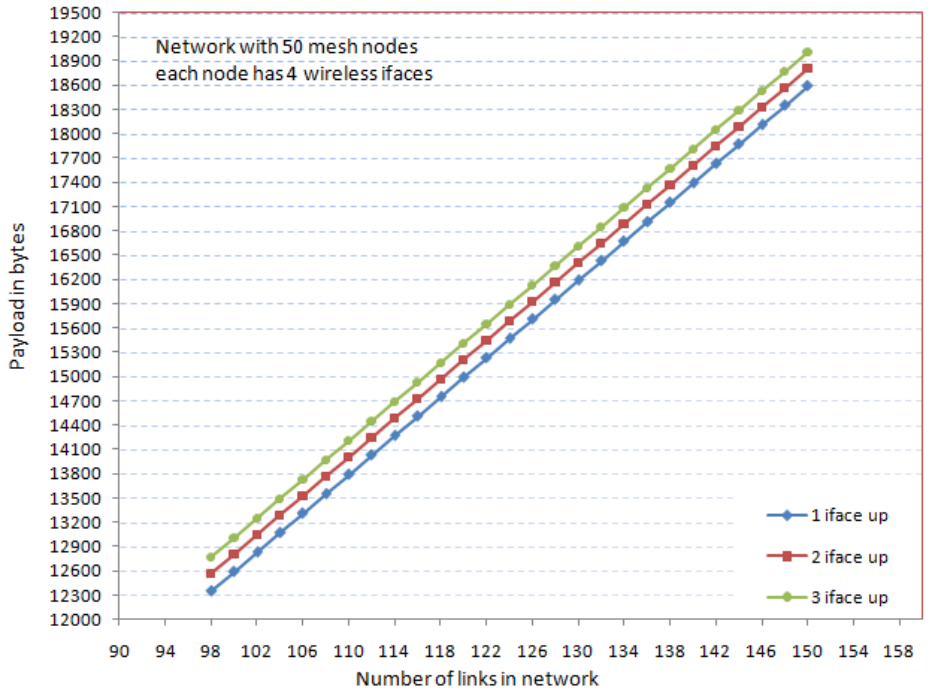

Figure 78: Amount of data obtained from mesh node as a function of topology (number of active links in the WMN) and number of active interfaces of the observed node

If we increase the number of active mesh interfaces of the observed node in second iteration to 2, interfaces table will remain unchanged, while neighbor and link table will be increased for one entry,

because the observed node is now connected with two neighboring nodes. During iteration the size of these tables will not be changed anymore, so the first three terms in equation (2) will be constant again. Hence a jump in the graph comes for different values of the parameter *i*.

So far the analysis referred to the network with fixed number of nodes. When the number of nodes in the network increases, linear dependency also applies with the same coefficient of direction.

Now, we will take a look how is the size of collected data changed on level of entire network when topology changes. The total amount of data can be represented as sum of data obtained from every single node in the network:

$$PL_{net} = \sum_{n} PL_x = \sum_{n} (IT_x + LT_x + NT_x + TT_x + RT_x) = IT + LT + NT + TT + RT \quad (3)$$

Considering that data from every single node can be divided on tables, the final result is also presented as sum of corresponding tables. This means that *IT* represents sum of interface tables from all nodes in the network, *LT* represents sum of link tables from all nodes in the network, and so on.

If we mark the number of links in the mesh network with *l,* where every node has the same number of wireless interfaces *i,* the equation (3) can be transformed in following:

$$PL_{net} = nie_{IT} + le_{LT} + le_{NT} + nle_{TT} + (n-1)le_{RT} \quad (4)$$

In equation (4), we can see that for fixed value of *n,* PL_{net} represent linear dependency on *l* of following form:

$$PL_{net} = Kl + C$$

where

$$K = e_{LT} + e_{NT} + ne_{TT} + (n-1)e_{RT},$$
$$C = nie_{IT}.$$

As the number of nodes in the network is increased, parameters *K* and *C* grow, leading that PL_{net} also grows but with changed coefficient of direction.

Figure 2 shows how is the amount of collected data changed for the whole mesh network with topology changes.

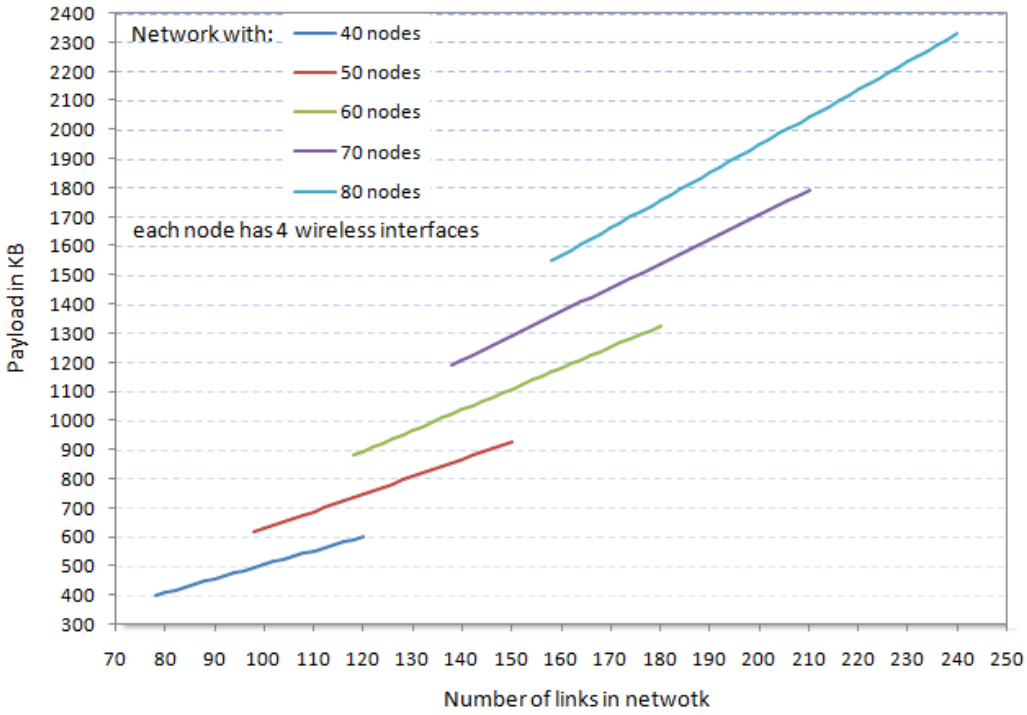

Figure 79: Amount of collected data on mesh network level in function of topology and number of mesh nodes

6.6.7 Conclusions

The algorithm, which signalling evaluation is conducted in this section, is successfully implemented into the open platform WMN test-bed (please see D5.2 for more details about implementation and the test-bed). Since the algorithm relays on contextual parameters which can be gathered with the SNMP protocol (supported by all networking devices) it is easily deployable in real world situations. The amount of gathered contextual parameters can be fine tuned in order to reduce signalling overhead. Also, some parameters are identified as fast changing so their values need to be gathered more often. For these parameters it is a common practice to be locally monitored by the networking nodes (i.e. WMN station). This monitoring is performed in order to check values of these parameters against the set of configured triggering levels. When trigger is met (i.e. congested link or fast growing link load), then the latest values of these fast changing parameters can be sent to the centralized management system as well as the alarm that the local trigger is detected. The centralized management system will react accordingly. Locally monitored parameters are logged and these logs are periodically sent to the centralized contextual database for the purpose of knowledge derivation.

If the decision is made based on false values of the monitored parameters, the created ON will be terminated in the maintenance phase as soon as this situation is detected. Underlying single-path routing protocol works all the time on load forwarding, so existing users are continuously served whether the ON is created or not. Only newly arrived users (or users requesting new service/application) are affected by ON creation and termination. These users will not get requested QoS whether or not the improper ON is created.

6.7 UE-to-UE Trusted Direct Path

6.7.1 Evaluation model

We have defined a system architecture based on the 3GPP network architecture that can setup an ON between two UEs, by establishing a UE to UE direct path using 802.11 WLAN technologies. The architecture is depicted in the following diagram

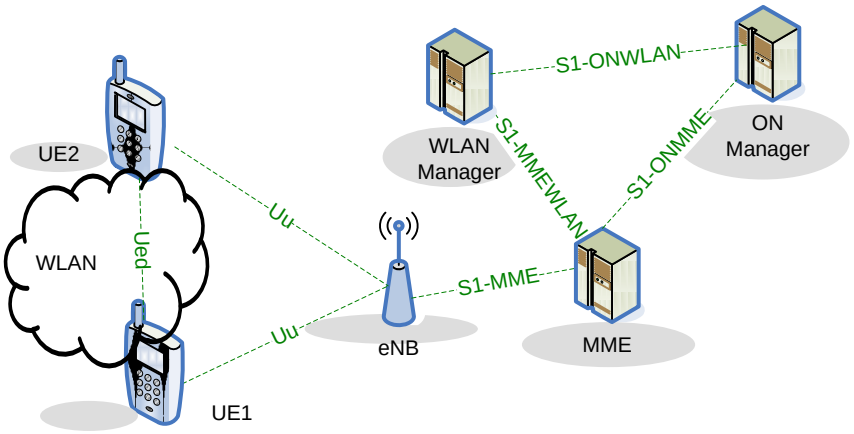

Figure 80: System architecture of the 3GPP based implementation

The following interfaces are defined in the core network infrastructure:

- S1-ONWLAN
- S1-MMEWLAN
- S1-ONMME
- S1-MME

The following interfaces are defined in the radio access network:

- Uu
- Ued

Our designed solution has been defined with a centralised ON manager, and with a WLAN manager taking care of the WLAN ONs. Those two entities are located in the core network (EPC). All the signalling messages exchanged between the WLAN manager and a UE have to be transit in the EPC before going in the UTRAN and reaching the UE through the Uu interface.

Our working assumption is that the infrastructure interfaces in the core network and the radio access network are always far less critical than the wireless interfaces. With this respect, we have studied in this chapter, the impact of the signalling on the wireless interfaces, for the identified scenario.

6.7.2 Verification scenario

The main scenario that was targeted by our research is the scenario 3 “Infrastructure supported opportunistic ad-hoc networking”. This scenario was expected to be appealing to mobile network operators for two main reasons: First it can perform traffic offloading from the core network, and secondly it can create opportunities for operator to create new innovative proximity based services.

We have detailed the messages exchanged for this scenario, and estimated the size of the message.

We focussed our evaluation on the configuration of an UE for participating to an ON. As previously mentioned, the considered messages are the ones transported on the Uu interfaces, as those messages will be transported in the wireless spectrum of the operator. The signalling message transported on the Ued interface is transported in the WLAN wireless spectrum.

We have not detailed the mechanism and procedure conducting to the decision that a UE can enter in an ON. As pointed in the appendix 2.3.5, different methods are possible for this. Some could

involved specific user actions and would generate a reduced level of signalling from the UE to the ON manager, while other could be purely based on already available services of the network, like the location based services.

We have perform our evaluation for estimating the signalling size for one single ON creation and termination between two UEs (ie : UE to UE direct path). The following table present the scenario aspect that was used during the evaluation of signalling. No dynamic aspect for this evaluation was considered. An estimation of the worst case scenario is presented in the paragraph 0.

General scenario aspects	
ON phase considered	Creation, Release
Scenario size	A Direct path established between 2 UEs. (an ON between two UEs)
Mobility of terminals	No
Signal propagation model	NR
Traffic model	NR
Terminal related aspects	
(Total) number of terminals in scenario	2
Number of ON capable terminals (Fraction of ON capable terminals in the scenario)	2
Location of terminals (distribution of terminal)	Static
Network interfaces supported by terminals	1 interface with the RAN (Uu) 1 WLAN interface (IEEE 802.11)
BS / femto / AP related aspects	
(Total) Number of Base Stations / femtocells / access points in scenario	1
Number of ON capable Base Stations/ femtocells / access points (Fraction of ON capable Base Stations/ femtocells / access points)	0
Location of BS/femtos/APs (distribution of BSs/femtos/APs)	N/A
Network interfaces supported by BSes/femtos/APs	Uu
Spectrum related aspects	
Spectrum occupancy model	N/A
Spectrum bands	N/A
Opportunistic Network related aspects	
Maximal size of ON	N/A
Fraction of nodes which are in ON at simulation start (number of terminals, number of BSs/Femtos/APs)	N/A

6.7.3 Information management strategies

Information management strategies are not considered in the algorithm evaluation.

6.7.4 Signalling message size estimations

The message containing the most significant parameters is the message configuring the UE to act as a WLAN 802.11 access point or as a WLAN 802.11 station. In this message, the largest parameters are: the SSID of the network that can be as large as 32 bytes, and the security key which can be also be 32 bytes. Another significant parameter is the IP address than can be 16 bytes in the IPv6 case. An additional overhead for the other parameters can be maximised to 48 bytes, leading to an estimated total maximum message size of 128 bytes.

The other messages are far smaller, as they mostly contain status information, or bytes size parameters. They are maximized to a size of 48 bytes.

As seen in the appendix to D3.3 [10] section 2.3.5 on the message sequence charts, each UE of an ON exchanges 4 messages over the Uu interfaces : One configuration message (<128 bytes), and 3 of status (each consisting less than 48 bytes). The upper bound of the cumulative size of the exchanged data is thus 272 bytes.

For the termination of the ON, 4 messages are exchanged per UE over the Uu interface (each consisting less than 48 bytes) thus resulting in the upper bound of 192 bytes.

It is interesting to note that during our design, we have considered that no periodical maintenance message is exchanged between the WLAN manager and a UE during the ON maintenance phase. We have assumed that during the ON maintenance, such periodical message is not required. The only maintenance message that can occurs is limited to the loss of the WLAN connection by an UE that will be sent to the WLAN manager. This is a one shot message that would end up in terminating the ON.

The total signalling messages for the creation and the termination of an ON between two UEs (a UE to UE direct path) is estimated to 16 messages and 928 bytes in size (464 bytes per UE).

Further to this estimation, real business information estimation from network operators would be useful to estimate the overall signalling generated on a single cell Uu interface due to the ON constitution.

In absence of proper business information, a worse case example can be taken to check the maximum signalling size and estimate the time required to transmit it over an LTE Uu interface. The scenario will be to create/terminate an ON with the maximum possible number of active users : 200 users (cf. 3GPP TR 25.913). This will require a total signalling size of 93 kB. Considering a low bandwidth hypothesis of 10 Mbits/s per UE on the LTE cell, all this signalling could be exchanged in under 75 ms.

In a real use case, this signalling will be spread over a longer time of several seconds for setting up the ON, and several seconds for terminating the ON. What can be concluded is that the amount of signalling needed for creating an ON in the worst case scenario, based on the defined architecture, is largely affordable by the system.

6.8 Content conditioning and distributed storage virtualization/aggregation for context driven media delivery

As it is explained hereinafter, no specific signalling results are outlined in this section as the signalling evaluations and possible scenarios presented in section 6.6 do pertain to this algorithm as well. The

algorithm runs on a centralized server and has the insight into the users requests (their spatial and temporal distribution) and status of all Wireless Mesh Network (WMN) nodes and their storage space. Topology, Routing and Links tables presented in section 6.6 (algorithm named: Application cognitive multi-path routing in wireless mesh networks) are the base input for making the statistical graph (frequency of the link establishing is incorporated into the cost of the corresponding graph's edge) of the underlying WMN. It needs to be noted however, that from the aforementioned tables the following parameters are not required for WMN graph derivation: Hist, LQ and NLQ (please refer to section 6.6.4 for more details).

Parameters in the Interfaces table are used for capacity estimation of the WMN backhaul links. Since these parameters are already gathered for the routing algorithm they are reused and do not impose any additional control traffic. These parameters are used for estimation of traffic patterns in backhaul links for the purpose of proactive content caching therefore a fast response to changes of these parameters is not needed. Estimated backhaul links capacity is important for choosing a path for the content delivery from WMN nodes to the requesting users.

All decisions are made at the centralized management system: 1) where the content is going to be proactively placed, 2) how it will be re distributed when needed, 3) which WMN node should serve as a streaming server for requesting user and 4) when the new content is going to replace the existing content in the node's caching storage.

All of the users' requests are sent to the centralized management. Traditionally, these requests would be sent to service provider, therefore they as well do not impose any additional signalling traffic. Centralized management derives users' request distribution and file popularity from these single requests. Also, centralized management system knows exactly what is the current status of the caching storages of WMN nodes (which chunks are currently stored, the size of the storage space and the size of the available space) since decisions of content placement/replacement are made by this system. Therefore, these parameters don't need to be reported by the WMN nodes. If the monitoring system detects the failure of the node, centralized management system makes a conclusion that the corresponding cache storage is out of reach.

The unique traffic generated by the system, to which this algorithm belongs, is related to the centralized management's replies to the users' requests with the message containing the URL and if needed the IP address of the node with which the user needs to establish the streaming session. Straightforwardly, the number of requests, generated by users, stimulates the number of replies from the centralized manager.

For the energy consumption aware version of the content placement algorithm, the centralized management system needs the contextual information on the current power consumption of the WMN nodes. If this parameter is available on the WMN node, the monitoring system can send new SNMP requests for acquiring this information. Data should be presented as a real number thus the contextual data derivation procedures described in 6.6 would need to be updated accordingly.

6.9 Capacity Extension through Femto-cells

6.9.1 Evaluation model, scenario and information management strategies description

General scenario aspects	
ON phase considered	
Scenario size	1000m x 1000m (but it can be configurable)
Mobility of terminals	speed within range and with various models, e.g. random walk (average velocity: 0, 1 or 2 m/s)

Signal propagation model	femtocell propagation model, WINNER 5bf, Okumura-Hata
Traffic generation model	variable packet sizes, intervals; bitrate requirements depending on user profile
Terminal related aspects	
(Total) number of terminals in scenario	Configurable(usually 40, min 30, max 50)
Number of ON capable terminals (Fraction of ON capable terminals in the scenario)	Configurable (probably 100%)
Location of terminals (distribution of terminal)	Configurable but usually uniformly distributed
Network interfaces supported by terminals	2 long-range interface (800m range);
BS / femto / AP related aspects	
(Total) Number of Base Stations / femtocells / access points in scenario	1 BS and 9 femtos
Number of ON capable Base Stations/ femtocells / access points (Fraction of ON capable Base Stations/ femtocells / access points)	configurable
Location of BS/femtos/APs (distribution of BSs/femtos/APs)	Configurable
Network interfaces supported by BSes/femtos/APs	2 long-range interfaces (range for BSes – 800m, for femtocells up to 150m)

6.9.2 Verification scenario for the capacity extension

Specific MSCs have been defined in D3.2 for capacity extension through femtocells. In this scenario it is assumed that a BS experiences congestion issues. This is BS#1. Moreover, it is assumed that an available femtocell (i.e., BS#2) is located in the service area of the problematic BS. Available femtocells can be seen as an opportunity to provide capacity extension to overloaded infrastructure elements due to the fact that they can seize the opportunity of the radio environment (extra resources) in a specific region for a specific timeframe. In order to allow the creation of an ON, the femtocell would temporarily change to OSG mode (Open Subscriber Group) from CSG (Closed Subscriber Group) or it may temporarily add extra UEs in its subscriber group. Then, if the femtocell is available, the negotiation procedure will be triggered in order to become temporarily OSG from CSG or to add temporarily extra UEs.
Illustrations from Figure 81 to Figure 84 provide the sequence of the exchange messages during the phases of suitability determination, creation, maintenance and termination respectively.

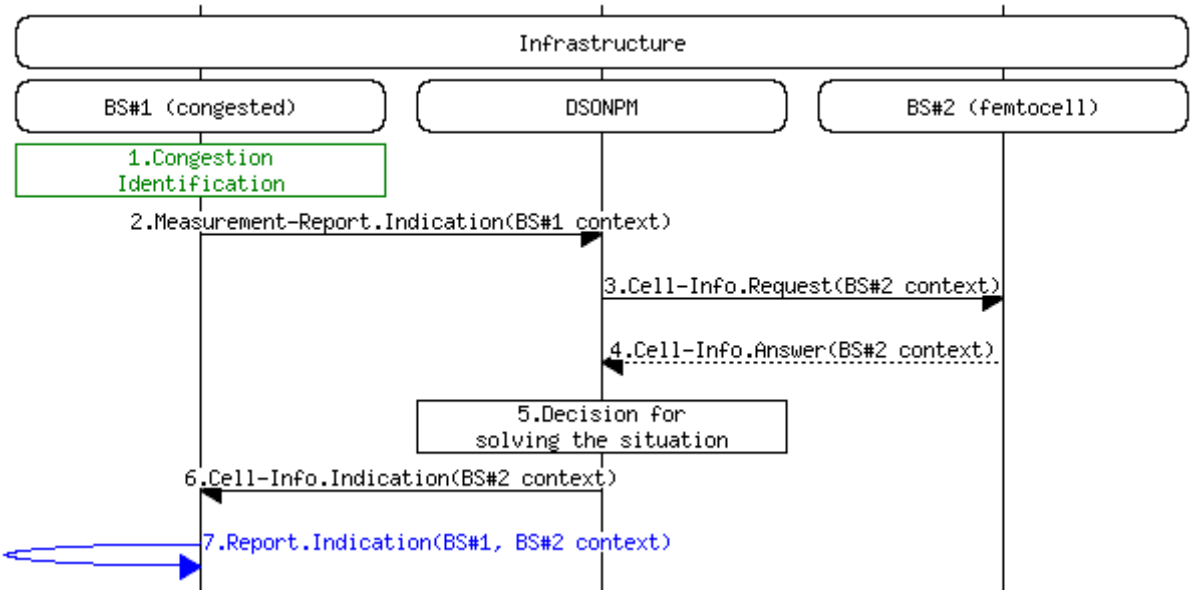

Figure 81: Capacity extension through femtocells; Suitability determination phase.

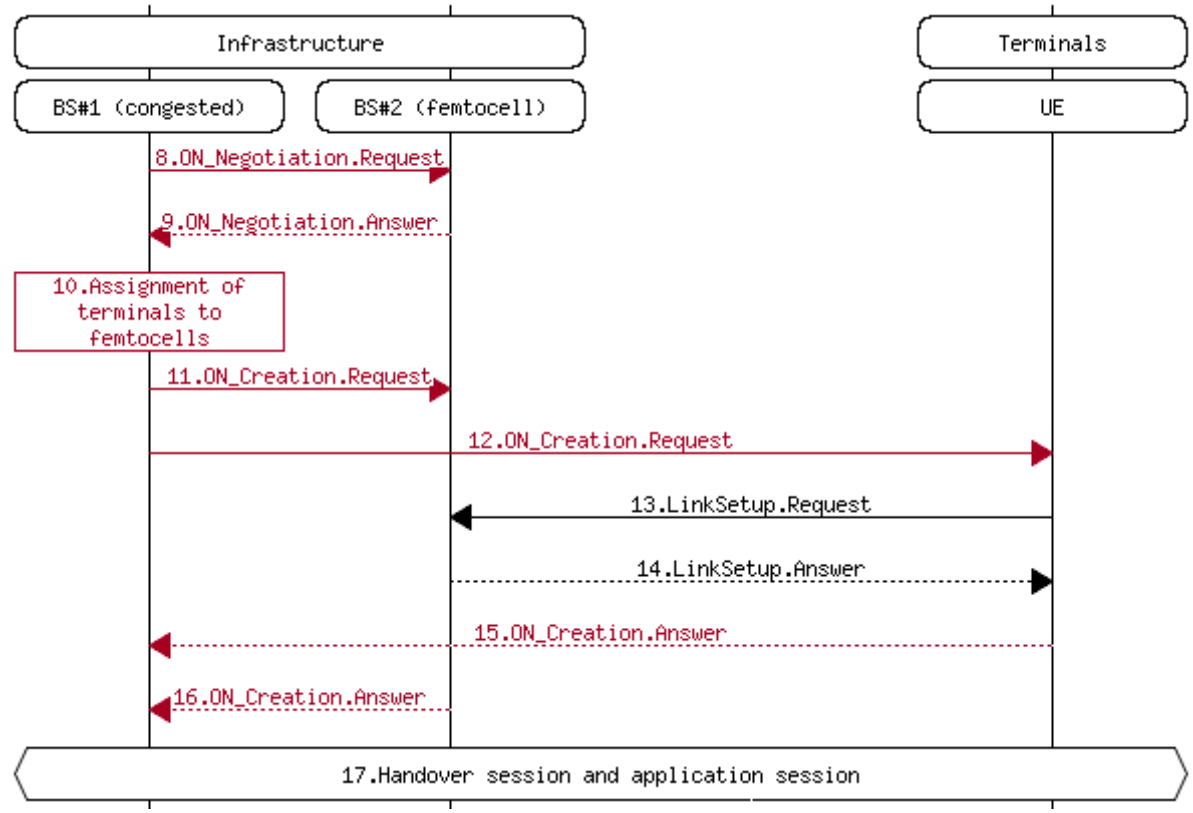

Figure 82: Capacity extension through neighboring terminals; Creation phase.

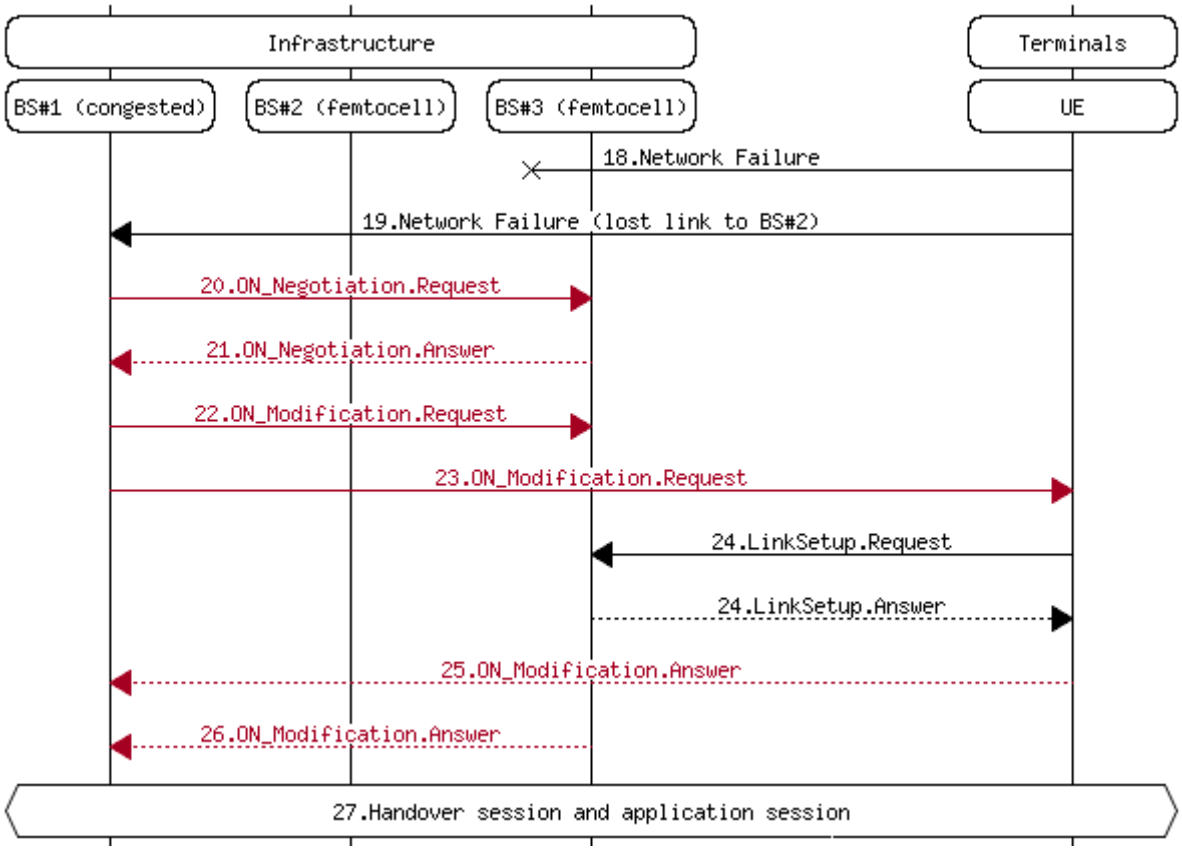

Figure 83: Capacity extension through femtocells; Maintenance phase.

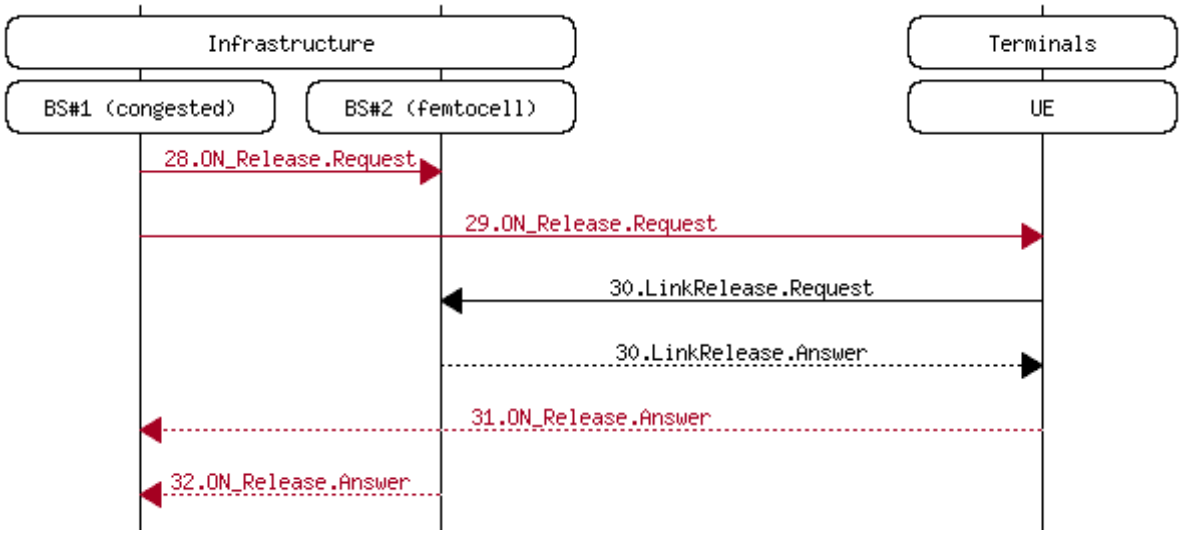

Figure 84: Capacity extension through femtocells; Termination phase.

6.9.3 Signalling load evaluation

Signalling load in this section has been estimated according to analytical models. The models take into account the contents of each data structure as defined in Sections 3 and the appendix to D3.3, section 3 [10]. According to the assumed scenario the following input parameters are considered: 1 congested Base Station and 40 terminals. Also, each BS has 1 interface and 1 RAT per interface, each terminal has 2 interfaces and 1 RAT per interface. Moreover, each terminal has 1 active application

and 1 active link (either with a BS or a femtocell). Furthermore, 9 femtocells are deployed in the area which initially (i.e., before the assignment of users to femtocells), are assumed to serve no users. After the solution enforcement, it is assumed that 18 out of 40 users are assigned to nearby, available femtocells (that number corresponds to 2 users per femtocell). To that respect, the associated signaling load for each phase of the ON is as follows:

Table 42: Associated signalling load of the scenario

ON Phase	Signaling load	
Suitability determination and creation	27 KB	
Maintenance	(Terminal_Context)245B*18 terminals≈5KB	
	5-sec period 5KB/5sec=1KB/s	30-sec period 5KB/30sec=0.2KB/s
Termination (for a single termination procedure)	24 B	

As mentioned also in Section 6.5.4 during the maintenance phase a periodical exchange of messages is considered compared to the other phases which are triggered based. Also, for the periodical exchange a 5-sec period of transmission and a 30-sec period of transmission are considered. In the first situation the associated signaling load should raise up to 1 KB/s while in the latter case the load drops to around 0.2 KB/s. In both cases it is assumed that only the terminals which switch to femtocells are transmitting their context every 5 or every 30 seconds. In this scenario, it is assumed that 18 terminals switch to femtocell. Finally, a single termination procedure (i.e., load needed to detach one terminal from a femtocell) is evaluated. The procedure is estimated to be 24 bytes and it is triggered upon request from the operator.

6.9.4 Conclusions

The conducted evaluations, show that for a network of 9 femtocells and 40 users the signaling load for the phases of the ON remains rather low (around 30 KBs) compared to the actual traffic of data (which could be hundreds of KBs or several MBs). As Section 6.5.4 designates, it should be considered that suitability determination and creation phases could be triggered-based. In the maintenance phase, messages could be exchanged in a periodical manner between the a femtocell and an attached terminal, but the exchanged information is limited to some context data (as also Section 6.5.4 describes). Finally, the termination phase could be also triggered-based according to the decision made by the operator (unless the network experiences a sudden failure).

The exploitation of the opportunity of available femtocells in the network shall provide e.g. capacity extension in congested macrocells without at the same time flooding the network with control messages. To this respect the solution seems feasible and viable in terms of signaling load overhead.

7. Conclusion

This document provides the refined and detailed specification of the C4MS protocol introduced in D3.1 [2] and further elaborated in D3.2 [3]. The specification includes, among others, revised and extended message format definitions (originally proposed in D3.1) and precise information regarding the content and structure of conveyed information. This enables the potentially interested parties (e.g. network operators) to conduct their own evaluation for determining the feasibility of the C4MS implementation and the ON usage in different network configurations and for different scenarios. The document elaborates also on the possible C4MS implementation options, originally presented in D3.1 deliverable and also - based on OneFIT contributions - further described in ETSI TR 102 684 "Feasibility Study on Control Channels for Cognitive Radio Systems" [28]. The document considers three different approaches: i.e. IEEE 802.21, DIAMETER, and 3GPP based approaches. By focusing on the IEEE 802.21 based approach it was shown that the C4MS can be implemented to existing standards with only minor changes (implementation considerations were necessary in order to provide the essential input towards WP5). It is worth to underline here, that although the validation platforms that are presented in WP5 do not follow exactly the solutions presented in this deliverable, the general idea behind the approach towards C4MS remains unchanged.

The analysis of the C4MS protocol presented in this deliverable indicates that the application of the protocol does not introduce an excessive signalling overhead for the considered scenarios (and considered scenario settings) and thus is well suited for the purpose of the ON management (see Section 5 and Section 6 for more detail). The results indicate also that there exists a certain level of flexibility in optimizing the signalling overhead by selecting different Information Management Strategies to trade signalling load for the signalling delay. It is worth to underline here that in order to fully confirm the feasibility of the C4MS for ON management further and more thorough analysis is necessary. The additional analysis should include an estimation of the signalling overhead introduced by the joint operation of multiple ON related algorithms (the existing analysis either determine the upper bound of the signalling overhead or focus on the evaluation of the signalling generated by a single algorithm) as well as an thorough estimation of the amount of measurement related information exchanged during the maintenance phase. Some additional analysis to determine signalling overhead for large scale scenarios could be also necessary.

In general, although more validation activities and performance analysis need to be performed and some key issues need to be still addressed, the solution presented hereinbefore, based on the current results and standardization efforts, is considered as a promising idea for providing opportunistic networks services into the real world and shall finally provide a far-reaching product.

8. References

[1] ICT-2009-257385 OneFIT Project, http://www.ict-onefit.eu/

[2] OneFIT Deliverable D3.1 “Proposal of C4MS and inherent technical challenges”, March 2011

[3] OneFIT Deliverable D3.2 “Information definition and signalling flows”, September 2011

[4] OneFIT Deliverable D4.1 “Formulation, implementation considerations and first performance evaluation of algorithmic solutions”, May 2011

[5] OneFIT Deliverable D4.2 “Performance assessment & synergic operation of algorithmic solutions enabling opportunistic networks”, June 2012

[6] OneFIT Milestone M3.3 “Protocols for the integrated C4MS”, January 2011

[7] OneFIT Milestone M4.2 “Interactions and synergies among diverse algorithmic solutions for enabling opportunistic networks”, December 2012

[8] OneFIT Deliverable D5.2 “Validation platform implementation description”, June 2012

[9] OneFIT Milestone M5.3 “Integration of algorithms enabling opportunistic networks in the validation platform”, April 2012

[10] Appendix to D3.3: Detailed C4MS Protocol Specification, June, 2012

[11] IETF RFC 0793 “Transmission control protocol”, September 1981

[12] IETF RFC 3588 “Diameter Base Protocol”, September 2003

[13] IETF RFC 5106 “The Extensible Authentication Protocol-Internet Key Exchange Protocol version2 (EAP-IKEv2) Method”, February 2008

[14] IETF RFC 5201”Host Identity Protocol”

[15] IETF RFC 5216 “The EAP-TLS Authentication Protocol”, March 2008

[16] IETF RFC 3411 “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002

[17] IETF RFC 3418 ” Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)”, December 2002

[18] IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks Part 21: Media Independent Handover Services, IEEE, January 2009.

[19] Java Remote Method Invocation Specification, Sun Microsystems, http://java.sun.com/javase/technologies/core/basic/rmi/index.jsp

[20] IEEE 802.1X-2010 Port-Based Network Access Control, February 2010

[21] 3GPP TS 24.109 V10.1.0, Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details

[22] 3GPP TS 33.221 V10.0.0, Generic Authentication Architecture (GAA); Support for subscriber certificates

[23] 3GPP TS 33.402 v11.3.0, System Architecture Evolution (SAE); Security aspects of non-3GPP accesses

[24] 3GPP TS 36.300 V11.0.0 Overall description of Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

[25] 3GPP TS 23.402 v11.2.0, “Architecture enhancements for non-3GPP accesses”

[26] 3GPP TS 36.331 v11.0.0, “Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification”

[27] ETSI TR 102 683 v1.1.1, “Reconfigurable Radio Systems (RRS); Cognitive Pilot Channel (CPC), 2009

[28] ETSI TR 102 684 v1.1.1, “Reconfigurable Radio Systems (RRS); Feasibility Study on Control Channels for Cognitive Radio Systems”, April 2012

[29] E3 Deliverable D4.4 “Final solution description for autonomous CR Functionalities”, September 2009

[30] A. Keranen, J. Ott, T. Karkkainen, “The ONE Simulator for DTN Protocol Evaluation”, Proc. SIMUTools'09: 2nd International Conference on Simulation Tools and Techniques, Rome, March, 2009

[31] J. Gebert, R. Fuchs, “Probabilities for opportunistic networking in different scenarios” Future Network Mobile Summit (FuNeMS), Berlin, Germany, July 2012

[32] Andrei Gurtov, Host Identity Protocol (HIP); Towards Secure Mobile Internet, Willey and Sons, June 2008

[33] Y. Zeng, C. L. Koh, and Y.-C. Liang, “Maximum eigenvalue detection: theory and application,” in Proc. of IEEE ICC, Beijing, China, May 2008.

[34] M. A. Nowak. Evolutionary Dynamics: Exploring the Equations of Life. Harvard University Press, 2006.

[35] H. Eltaief, H. Youssef, “MLCC: A new hash-chained mechanism for multicast source authentication”, International Journal of Communication Systems - Secure communications and data management in ubiquitous services, September 2009

[36] Liang Tang, QiaoLiang Li , “S-SPIN: A Provably Secure Routing Protocol for Wireless Sensor Networks”, International Conference on Communication Software and Networks, 2009

[37] Muhammad Agni Catur Bhakti, Azween Abdullah, Low Tan Jung, “EAP-Based Authentication for Ad Hoc Network”, Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2007

[38] Harri Holma, Harri, Antti Toskala, “LTE for UMTS: Evolution to LTE-Advanced”, Second Edition, March 2011

[39] Martin L. Puterman. Markov Decision Processes: Discrete Stochastic Dynamic Programming. Wiley-Interscience, April 1994