NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-140)TP/874

www.sto.nato.int

**STO TECHNICAL REPORT** **TR-IST-140**

# Cognitive Radio Networks: Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management

(Réseaux de radio cognitifs : solutions efficaces pour le routage, le contrôle de la topologie, le transport de données et la gestion des réseaux)

Final Report of IST-140.

Published October 2019

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(IST-140)TP/874

www.sto.nato.int

**STO TECHNICAL REPORT** **TR-IST-140**

# Cognitive Radio Networks: Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management

(Réseaux de radio cognitifs : solutions efficaces pour le routage, le contrôle de la topologie, le transport de données et la gestion des réseaux)

Final Report of IST-140.

# The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.



Published October 2019



ISBN 978-92-837-2198-7

# Table of Contents

# List of Figures

# List of Tables

# List of Acronyms

| | |
|---|---|
| 3WH | TCP Three Way Handshake |
| ACK | Acknowledgment |
| ACROPOLIS | Advanced Coexistence technologies for Radio Optimisation in Licensed and unlicensed Spectrum |
| AODV | *Ad hoc* On-Demand Distance Vector |
| API | Application Programming Interface |
| APPL | Application |
| ARE | Application Request Enforcement |
| ARN | Application Request Notification |
| ARP | Address Resolution Protocol |
| ARQ | Automatic Repeat Request |
| AWGN | Additive White Gaussian Noise |
| BPSK | Binary Phase Shift Keying |
| CA | Collision Avoidance |
| CAODV | Cognitive *Ad hoc* On-demand Distance Vector |
| CCC | Common Control Channel |
| CDMA | Code Division Multiple Access |
| CEMCA | Connectivity, Energy and Mobility driven weighted Clustering Algorithm |
| CH | Cluster Head |
| CHN | Channel Handoff Notification |
| CIMIC | Civil Military Cooperation |
| CLI | Cross-Layer Interface |
| CNE | Cognitive Network Engine |
| CNMP | Cognitive Network Management Protocol |
| CNMS | Cognitive Network Management System |
| CoBA | Collaborative Bottleneck Analysis |
| COMSEC | Communications Security |
| COP | Common Operational Picture |
| CORE | Common Open Research Emulator |
| CPFSK | Continuous Phase Frequency Shift Keying |
| CR | Cognitive Radio |
| CRAHN | Cognitive Radio *Ad Hoc* Network |
| CRE | Cognitive Radio Engine |
| CREATE | Cognitive Radio networking Architecture |
| CRM | Cognitive Resource Manager |
| CRN | Cognitive Radio Network |
| CRNo | Connection Restart Notification |
| CRQ | Cognitive Radio Q-Routing |
| CRS | Cognitive Radio System |
| CSL | Cognitive Specification Language |
| CSMA | Carrier Sense Multiple Access |
| C/TDMA | Code/Time Division Multiple Access |
| CTR | Critical Transmission Range |
| CWND | TCP Congestion Window |

| | |
|---|---|
| DAA-OFDM | Detect and Avoid – Orthogonal Frequency Division Multiplexing |
| DADS | Delay and Avoid Direct Sequence |
| DB | Database |
| DE | Deconfliction Entity |
| DESAR | Delay and Energy-Based Spectrum Aware Reactive Routing |
| DFS | Dynamic Frequency Selection |
| DFT | Discrete Fourier Transform |
| DHCP | Dynamic Host Configuration Protocol |
| DLBC | Degree-Load-Balancing Clustering |
| DLEP | Dynamic Link Exchange Protocol |
| DS | Dominating Set |
| DSA | Dynamic Spectrum Access |
| DSDV | Destination-Sequenced Distance Vector |
| DSM | Dynamic Spectrum Management |
| DSmT | Dezert and Smarandache Inference and Classification Theory |
| DSR | Dynamic Source Routing |
| DSSS | Direct Sequence Spread Spectrum |
| DYMO | Dynamic MANET On-Demand |
| | |
| ECN | Explicit Congestion Notification |
| E-D2CARP | Enhanced Dual Diversity Cognitive Ad-hoc Routing Protocol |
| EMANE | Extendable Mobile Ad-hoc Network Emulator |
| EPD | Expected Path Delay |
| EPN | Explicate Pause Notification |
| ERFN | Explicit Route Failure Notifications |
| ETX | Expected Transmission Count |
| EW | Electronic Warfare |
| | |
| FAB | Fulfilment, Assurance, Billing |
| FC | Fusion Centre |
| FCAPS | Fault, Configuration, Administration, Performance, and Security |
| FDD | Frequency Division Duplexing |
| FER | Frame Error Rate |
| FFT | Fast Fourier Transform |
| FH | Frequency Hopping |
| FIFO | First In, First Out |
| FIR | Finite Impulse Response |
| FPGA | Field Programmable Gate Array |
| | |
| GMSK | Gaussian Minimum Shift Keying |
| GUI | Graphical User Interface |
| | |
| HC | Hop Counts |
| HCC | Highest Connectivity Clustering |
| HDR | High Data Rate |
| HEED | Hybrid Energy-Efficient Distributed Clustering |
| HF | High Frequency |
| HIL | Hardware in the Loop |
| HQ | Headquarters |
| HTTP | Hypertext Transfer Protocol |
| | |
| ID | Identification Number |
| IED | Improvised Explosive Device |
| IEEE | Institute of Electrical and Electronics Engineers |

| | |
|---|---|
| IIR | Infinite Impulse Response |
| IPv4 | Internet Protocol, Version 4 |
| IPv6 | Internet Protocol, Version 6 |
| IQ | In-Phase Quadrature |
| ISO | International Standardization Organisation |
| ITIL | Information Technology Infrastructure Library |
| ITU-R | International Telecommunication Union, Radiocommunication Sector |
| | |
| LBC | Load Balancing Clustering |
| LCC | Least Cluster Change |
| LDR | Low Data Rate |
| LIC | Lowest ID Cluster |
| LPD | Low Probability of Detection |
| LPI | Low Probability of Interception |
| LTE | Long Term Evolution |
| | |
| MAC | Medium Access Layer |
| MANET | Mobile *Ad Hoc* Network |
| MIB | Management Information Base |
| MOBIC | Mobility Based Metric for Clustering |
| MPR | MultiPoint Relays |
| MSS | Maximum Segment Size |
| M-TCP | Military TCP |
| M-TCP-CE | M-TCP Cognitive Engine |
| | |
| NATO | North Atlantic Treaty Organisation |
| NCIA | NATO Communications and Information Agency |
| ND | Neighbour Discovery |
| NEC | Network Enabled Capability |
| NET | Network Layer |
| NGO | Non-Governmental Organisation |
| NKRL | Network Knowledge Representation Language |
| | |
| OAMP | Operation, Administration, Maintenance, and Provisioning |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OFDMA | Orthogonal Frequency Division Multiple Access |
| OLSR | Optimized Link State Routing |
| OLSRv2 | Optimized Link State Routing, Version 2 |
| OSI | Open Systems Interconnection |
| OSPF | Open Shortest Path First |
| | |
| P2P | Peer to Peer |
| PCN | Policy Change Notification |
| PDL | Packet Delay |
| PHY | Physical Layer |
| PLR | Packet Loss Ratio |
| PPP | Point-to-Point Protocol |
| PSK | Phase Shift Keying |
| PU | Primary User |
| | |
| QAM | Quadrature Amplitude Modulation |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| QPSK | Quadrature Phase Shift Keying |

| | |
|---|---|
| RA | Range Assignments |
| RF | Radio Frequency |
| RLAN | Radio Local Area Network |
| ROC | Receiver Operating Characteristics |
| RREQ | Route Request |
| RRPL | Route Reply |
| RTP | Real-Time Transport Protocol |
| RTT | Round Trip Time |
| | |
| SCA | Stable Cluster Algorithm |
| SC-FDM | Single Carrier – Frequency Division Multiplexing |
| SCTP | Stream Control Transmission Protocol |
| SDN | Software Defined Networking |
| SDR | Software Defined Radio |
| SEARCH | Spectrum Aware Routing Protocol for Cognitive *Ad Hoc* Networks |
| SLA | Service Level Agreement |
| SNMP | Simple Network Management Protocol |
| SPoF | Single Point of Failure |
| SSDF | Spectrum Sensing Data Falsification |
| SU | Secondary User |
| SWIG | Simplified Wrapper and Interface Generator |
| | |
| TC | Topology Control |
| TCN | Transmission Control Notification |
| TCP | Transport Control Protocol |
| TCP-CRAHN | Transport Control Protocol for Cognitive Radio *Ad Hoc* Networks. Abstract: Cognitive Radio |
| TDD | Time Division Duplexing |
| TDMA | Time Division Multiple Access |
| TFRC-CR | TCP Friendly Rate Control for Cognitive Radio |
| TN | Technical Note |
| TRANSEC | Transmission Security |
| TUBE | Trust-Based Situation Awareness System |
| TV | Television |
| | |
| UDP | User Datagram Protocol |
| UHD | Universal Hardware Driver |
| UHF | Ultra-High Frequency |
| USRP | Universal Software Radio Peripheral |
| UWB | Ultra-Wideband |
| | |
| VHF | Very-High Frequency |
| | |
| WBACA | Weight Based Adaptive Clustering Algorithm |
| WBCA | Weight Based Clustering Algorithm |
| WCA | Weighted Clustering Algorithm |
| WCETT | Weighted Cumulative Estimation of Transmission Time |
| WSN | Wireless Sensor Network |

# IST-140 Membership List

## CHAIR

Mr. Stefan COUTURIER
Fraunhofer-FKIE (Communications Systems)
GERMANY
Email: stefan.couturier@fkie.fraunhofer.de

## MEMBERS

Dr. Andreas BOYD BUCHIN
Rohde & Schwarz GmbH & Co. KG
GERMANY
Email: boyd.buchin@rohde-schwarz.com

Mr. Ozgur BIYIK
Atos A.S.
TURKEY
Email: ozgur.biyik@atos.net

Dr. Timo BRÄYSY
University of Oulu
FINLAND
Email: timo.braysy@ee.oulu.fi

Dr. Lorenza GIUPPONI
Centre Tecnològic de Telecommunicacions de Catalunya (CTTC)
ITALY
Email: lorenza.giupponi@cttc.es

Ms. Eylem KOKSAL
Atos A.S.
TURKEY
Email: eylem.koksal@atos.net

Dr. Jaroslaw KRYGIER
Military University of Technology
POLAND
Email: jkrygier@wat.edu.pl

Dr. Ir. Vincent LE NIR
Royal Military Academy
BELGIUM
Email: vincent.lenir@rma.ac.be

Mr. Risto MAATTA
Finnish Defence Research Agency
FINLAND
Email: risto.maatta@mil.fi

Mr. José NUNEZ
Centre Tecnologic de Telecomunicacions de Catalunya (CTTC)
SPAIN
Email: jose.nunez@cttc.cat

Mr. Niels SMIT
Dutch MoD
NETHERLANDS
Email: NS.Smit@mindef.nl

Cdr. Topi TUUKKANEN
Finnish Defence Research Agency
FINLAND
Email: topi.tuukkanen@mil.fi

Mr. Erik VERHEUL
Royal Netherlands Navy
NETHERLANDS
Email: e.verheul@mindef.nl

# Cognitive Radio Networks: Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management

## (STO-TR-IST-140)

# Executive Summary

One of the most important aspects in today's military missions and operations is information superiority. Gathered information shall be available at the right place at the right time in all situations. For its distribution, communication networks are used. Consequently, there is a requirement for adaptability of such networks to all possible situations, which may lead to a certain complexity. Despite this complexity, they shall be robust, reliable, efficient, and easy to handle.

This report proposes solutions for radio networks to achieve these goals. These solutions are based on the idea that upcoming radio networks will be able to monitor their internal states as well as external influences, like changes in the spectral environment, and to react on them autonomously. The process to observe, to take decisions based on these observations, and to learn from the decisions is termed cognition. Therefore, networks that will have this capability are "Cognitive Radio Networks".

Cognitive Radios, which will have the ability to observe the spectral environment and to accordingly adapt their transmission frequency usage on link basis, have already been addressed in the groups "Cognitive Radio in NATO" (IST-077/RTG-035) and "Cognitive Radio in NATO II" (IST-104/RTG-050). This report instead focuses on network-related technologies in order to pursue end-to-end optimization in the network, taking into account the results achieved in those groups. Network-related aspects have also already been investigated in the group "Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency" (IST-124/RTG-061) with focus on interoperability, while this report targets their enhancement for supporting the aims of Cognitive Radio Networks.

The investigations of this group have come to the result that existing network paradigms for fixed and civilian networks do not necessarily fit military tactical radio networks. These paradigms may actually be counter-productive, as they often do not support e.g., typical military traffic patterns and security aspects. Moreover, they do not provide the flexibility and adaptability required for Cognitive Radio Networks. Consequently, the following proposals for network-related technologies have resulted:

- Routing should use artificial intelligence or machine-learning techniques to optimize route selection.
- For Topology Control, the choice between multiple frequencies on a single link should be considered, as well as specific military aspects, like classification of position information or lack of updates due to radio silence.
- In addition to that, an enhancement regarding the existing protocols for a more efficient data transport is proposed.
- Furthermore, the investigations have pointed out that clustering is important for the design of the network and should therefore support the other technologies used in tactical Cognitive Radio Networks.

- The control channel needs to deal with heavily varying data volumes; therefore, it should be adaptable to the current traffic.

Solutions based on these proposals will lead to improved availability and better end-to-end communication, as the network will be able to better adapt to its environment. Moreover, the spectrum will be used more efficiently.

Network management should be automated, which will lead to reduced management efforts before, during, and after a mission. This allows focusing even more on the mission. In addition to that, the research on trust management has shown its importance for the authenticity of control information. It should be based not only on the observation of the neighbouring nodes, but also on a strong reputation system.

Based on those findings, a new architecture framework for Cognitive Radio Networks is proposed, which can be seen as a starting point for the standardization and development of cognitive tactical radio systems.

# Réseaux de radio cognitifs : solutions efficaces pour le routage, le contrôle de la topologie, le transport de données et la gestion des réseaux

## (STO-TR-IST-140)

# Synthèse


La supériorité de l'information est l'un des aspects les plus importants des missions et opérations militaires d'aujourd'hui. Les informations collectées doivent être disponibles au bon endroit, au bon moment et dans toutes les situations. Pour leur diffusion, des réseaux de communication sont utilisés. Par conséquent, il est nécessaire que de tels réseaux soient adaptables à toutes les situations possibles, ce qui peut entraîner une certaine complexité. Malgré cette complexité, ils doivent être robustes, fiables, efficaces et faciles à mettre en œuvre.

Ce rapport propose des solutions afin que les réseaux radio atteignent ces objectifs. Ces solutions reposent sur l'idée que les réseaux de radio à venir pourront surveiller leurs états internes ainsi que les influences externes, telles que les modifications de l'environnement spectral, et y réagir de manière autonome. Le processus consistant à observer, à prendre des décisions en fonction de ces observations et à en tirer des leçons s'appelle la cognition. Par conséquent, les réseaux qui auront cette capacité sont appelés « réseaux radio cognitifs ».

Les radios cognitives, qui auront la capacité d'observer l'environnement spectral et d'adapter en conséquence leur utilisation de la fréquence de transmission sur la base de liens, ont déjà été traitées dans les groupes « Radio cognitive dans l'OTAN » (IST-077 / RTG-035) et « Radio cognitive dans l'OTAN II » (IST-104 / RTG-050). Ce rapport met plutôt l'accent sur les technologies liées au réseau afin de poursuivre l'optimisation de bout en bout du réseau, en tenant compte des résultats obtenus dans ces groupes. Des aspects liés au réseau ont également déjà été étudiés dans le groupe « Réseaux tactiques hétérogènes - Amélioration de la connectivité et l'efficacité des réseaux » (IST-124 / RTG-061), avec un effort sur l'interopérabilité, tandis que le présent rapport vise à renforcer leur capacité à soutenir les objectifs des réseaux radio cognitifs.

Les recherches de ce groupe ont abouti à la conclusion que les paradigmes de réseau existants pour les réseaux civils et fixes ne conviennent pas nécessairement aux réseaux radio tactiques militaires. En réalité, ces paradigmes peuvent être contre-productifs, car souvent ils ne supportent pas, par exemple, les caractéristiques typiques du trafic radio militaire et les aspects liés à la sécurité. De plus, ils n'offrent pas la souplesse et l'adaptabilité requises pour les réseaux radio cognitifs. Compte tenu de ces éléments, les propositions suivantes concernant les technologies liées aux réseaux ont été élaborées :

- Le routage doit utiliser des techniques d'intelligence artificielle ou d'apprentissage automatique pour optimiser la sélection des cheminements.
- Pour le contrôle de la topologie, le choix entre plusieurs fréquences sur une seule liaison doit être pris en compte, ainsi que des aspects militaires spécifiques, tels que la classification des informations de position ou le manque de mises à jour dues au silence radio.
- Par ailleurs, une amélioration concernant les protocoles existants pour un transport de données plus efficace est proposée.

- Enfin, les recherches ont montré que la mise en grappes est importante pour la conception du réseau et devrait donc prendre en charge les autres technologies utilisées dans les réseaux radio cognitifs tactiques.
- Le canal de contrôle doit gérer des volumes de données extrêmement variables ; par conséquent, il devra être adaptable au trafic actuel.

Les solutions fondées sur ces propositions amélioreront la disponibilité et la communication de bout en bout, car le réseau sera capable de mieux s'adapter à son environnement. De plus, le spectre sera utilisé plus efficacement.

La gestion du réseau doit être automatisée, ce qui amènera une réduction des efforts de gestion avant, pendant et après une mission. Cela permet de se concentrer davantage sur la mission. En outre, les recherches sur la gestion de la fiabilité ont montré son importance pour l'authenticité des informations de contrôle. Elle devra reposer non seulement sur l'observation des nœuds voisins, mais également sur un système de contrôle de la réputation solide.

Reposant sur ces résultats, un nouveau cadre d'architecture pour les réseaux de radio cognitifs est proposé, qui peut être considéré comme un point de départ pour la normalisation et le développement de systèmes de radiocommunication tactique cognitive.

# Chapter 1 – INTRODUCTION

The "survival of the fittest" is an important law in evolution. It does not mean that the one will survive that is physically fit, it means that the one will survive that best fits into his environment. We know this from the work of Charles Darwin's observations of nature. Also, in radio network technology, there is a continuous evolution ongoing. Much research is done, and new designs are published almost continuously. Here, too, the best performance is given by the radio network that best suits to the environment. Mobile Ad hoc Networks (MANET) already offer a significant challenge in this respect, because the network itself is mobile and therefore the environment can change continuously. So, how to adapt to a changing environment?

This report is a study on how to bring cognition into the radio network, so that it can adjust to a changing environment. This is different from existing MANET protocols. These network protocols can only adapt their network topology but not their network behaviour when the circumstances change.

It is also different from Software Defined Networking (SDN), because even though SDN can quickly adjust the network behaviour, SDN lacks the cognition and awareness of the environment and thus the knowledge what to adapt to.

It is furthermore different from Cognitive Radio (CR), too, because CR is intended to optimize point-to-point radio links because of its awareness of the local spectral environment, but it cannot optimize the total network performance.

The Cognitive Radio Network (CRN) is a network that can sense its environment, adjust its network behaviour accordingly and learn from previous experiences. This is not a simple task, and networks like this do not exist yet today. The expected advantages are significant: a radio network that can optimize its network behaviour under changing circumstances will give the best possible performance without manual reconfiguration of the equipment. This means that military personnel in the field can focus on their mission without having to perform difficult network configuration tasks during the mission. Therefore, the technical training effort before missions is reduced. In addition, advanced features of the CRN support improvements in the Network Enabled Capability (NEC) value chain.

This study attempts to identify the requirements and challenges, explore solutions and technologies, and propose an architecture framework and further research on CRNs. Further beneficial research topics are addressed at the end of the report.

# Chapter 2 – WHAT ARE COGNITIVE RADIO NETWORKS AND WHY DO WE WANT THEM?

## 2.1 WHAT ARE COGNITIVE RADIO NETWORKS?

In this chapter, we list and analyse definitions from literature with the goal of outlining the concept of CRNs used in this document.

### 2.1.1 What is Cognition?

Cognition can be understood as a process of acquiring knowledge and understanding through thought, experience, and the senses. It includes tasks like attention, memorizing, learning, judgment and evaluation, reasoning, problem solving, and decision making among others. These use existing knowledge and may generate new knowledge.

The term "cognition" is used differently in various scientific disciplines. Different academic approaches to the analysis of cognition are synthesised in the developing field of cognitive science that may also include disciplines of machine learning and artificial intelligence.

### 2.1.2 Cognitive Radio (CR)

CR has been mentioned as a next generation evolution from the Software Defined Radio (SDR), of which the first commercially available examples are just about to enter the market. Various stakeholders place expectations to CRs from different viewpoints. Regulators and mobile operators are hard pressed for the available bandwidth in scarce radio frequency spectrum, thus proposing features like dynamic spectrum access or cognitive spectrum management. Military users would need zero-configurable radios that are easy to use and are capable of adapting to different operating modes, including avoiding detection, circumventing jamming, or adjusting functional behaviour based on the phase of operations or depending on the geographic region, including underdeveloped, degraded, and denied operational environments [1].

As the challenges faced by many military research and development as well as acquisition programs demonstrate, the "requirements creep" can dramatically influence the outcome of any potential CR development project [1].

Regarding CR, there are partially competing definitions. As CR is not the focus of our work, we will refrain from selecting one of the definitions, but instead list the definitions and discuss their implications.

CR has been introduced in Ref. [2]. Following the definition found in Ref. [3]:

> *"Cognitive radio is an intelligent wireless communication system that is **aware** of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to **learn** from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind:*
>
> - *Highly reliable communications whenever and wherever needed; and*
> - *Efficient utilization of the radio spectrum."*

Ref. [4] describes CR as:

> *"An evolution from an SDR and that a CR further develops SDR technologies to support three major application areas, namely:*

- *Spectrum management and optimization;*
- *Interface with a wide variety of networks; and*
- *Interface with a human and providing electromagnetic resources to aid the human in his activities."*

The Wireless Innovation Forum recognizes that there may be an intermediate development stage from a contemporary SDR on the way to fully developed CR that they call an Adaptive Radio. By definition, this would be:

> *A radio / communication system that has means to monitor its own performance and to vary its own parameters in order to improve that performance.*

However, this notion is inherently limited in its capabilities, as it implies a somewhat narrowly focused control loop, which, in itself, is predefined in its scope and response.

The CR has been defined in Ref. [4] as:

> *"[A radio that] uses SDR, Adaptive Radio and other technologies to automatically adjust its behavior or operations to achieve desired objectives."*

In conjunction with this, the Wireless Innovation Forum [5] used, in 2007, the working definition for the CR as:

> *"Radio in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information and predefined objectives."*

However, by 2008, the Wireless Innovation Forum was able to agree and formally approve the definition for CR although with caveats that will be explored below in some detail. The terms and definitions for CR from scientific literature, standardization bodies, and other relevant entities were analysed, and the Wireless Innovation Forum [6] came up with a multifaceted definition for the CR:

> *"**Cognitive radio (as a design paradigm)***
>
> *An approach to wireless engineering wherein the radio, radio network, or wireless system is endowed with the capacities to:*
>
> - *Acquire, classify, and organize information (aware);*
> - *Retain information (aware);*
> - *Apply logic and analysis to information (reason);*
> - *Make and implement choices (agency) about operational aspects of the radio, network, or wireless system in a manner consistent with a purposeful goal (intelligent)."*

There are a number of ways that the CR paradigm can be implemented, thus examples of implementation are presented:

> ***"Cognitive radio (as examples of implementation)***
>
> *A radio designed according to the cognitive radio engineering paradigm:*
>
> - *Cognitive radio as defined above that utilizes Software Defined Radio, Adaptive Radio, and other technologies.*
> - *A radio endowed with the capacities: to acquire, classify, retain, and organize information, to apply logic and analysis to information, and to make and implement choices about operational aspects of the radio in a manner consistent with a purposeful goal.*

- *A radio, radio network, or wireless system designed according to the cognitive radio engineering paradigm."*

In an SDR, the transmission characteristics are defined mostly within the software that as an entity is called a waveform, and this includes the characteristics that are needed for a successful communication to take place in most of the ISO/OSI layers. From a radio engineering viewpoint, the ISO/OSI layers most often addressed include layers from PHY/MAC up to and including link and network layers. Therefore, it is not surprising to note that cognitive features are expected from these layers, or the waveform, too [7]. At this point, the reader is cautioned. It seems that terminology is diverging and that issues that are addressed as communication systems in civilian context are easily labelled in military domain as waveform issues.

According to Ref. [8], CR is a type of radio in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behaviour based on that information and predefined objectives.

The cognition capability of a CR is defined as the ability of the CR transceiver to sense the surrounding radio environment, analyse the captured information and accordingly decide the best course of action(s) in terms of which spectrum band(s) to be used and the best transmission strategy to be adopted. Such a cognition capability allows a CR to continually observe the dynamically changing surrounding radio environment in order to interactively come up with the appropriate transmission plans to be used [9].

### 2.1.3 Cognitive Radio System (CRS)

In 2009, the ITU-R has provided a definition of a CRS [10]:

> *"A radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained".*

Following the ITU-R definition, the cognition in CRS means the ability to build knowledge about the environment in general (not only about spectrum usage) and use this knowledge to adapt the parameters of the whole protocol stack in the system to achieve some objectives. The objectives can be for example optimal spectrum utilization, jamming avoidance, but also efficient traffic distribution or even high security assurance. Admittedly, the last ITU-R report on CRS in the land mobile service [11] is concentrated mainly on potential spectrum sharing in land mobile communications, but it also points out the need of employing many system elements (databases, protocols) to utilize and build the CRS knowledge.

Actually, there are already existing applications (i.e., Radio Local Area Networks (RLANs) using Dynamic Frequency Selection (DFS)) or planned applications (i.e., radio systems using TV white space) that employ some of the CRS capabilities in order to obtain knowledge of their radio environment. Based on the obtained knowledge, they are able to select parameters, such as their frequencies and/or adjust their transmit power to enhance co-existence and sharing with the aim of avoiding harmful interference being caused. Besides, significant research activity can be found on many aspects of cognitive technology. CRS are mainly connected with intelligent spectrum sharing and access, intelligent radio network organization and management, as well as with intelligent data transmission control and routing. The proposed solutions are often based on adaptation capabilities, relying on separate protocol rather than on building knowledge about a system environment.

### 2.1.4 Cognitive Radio Network (CRN)

The term CRN has multiple meanings in the literature. In Ref. [4], Fette defines a **cognitive network** as:

> *"A **network of nodes**, that intelligently select and optimize parameters, based on the end-to-end requirements of the network".*

In Ref. [4], the authors assume that CRs shall form CRNs to complete the packet deliveries. Thus, the **network of cognitive radios** is a set of:

> *"**Cognitive radios** that operate as a network but pursue their own local, link-level objectives rather than their end-to-end objectives."*

A more complex meaning of CRN is discussed in Ref. [12]. There, it is assumed that a CRN is generally a multi-hop wireless heterogeneous network, meaning it allows peer-to-peer communications and may include different types of radios. When CRs are connected and form a CRN, they may share knowledge, which means the information gathered at each node, and decisions may be made in a distributed manner. In an abstract sense, the cognition then becomes a function of the network, rather than of the individual radio.

**For the purpose of this Task Group, the CRN will be defined as a network composed of CRs able to build local knowledge about their environment (spectral and network). In addition, the network – as a whole – is able to perform cognitive tasks to reach an overall network goal (efficient end-to-end communication, efficient spectrum utilization, etc.).**

Example functionalities of the **Network Cognitive Cycle** can be as follows, in Figure 2-1:

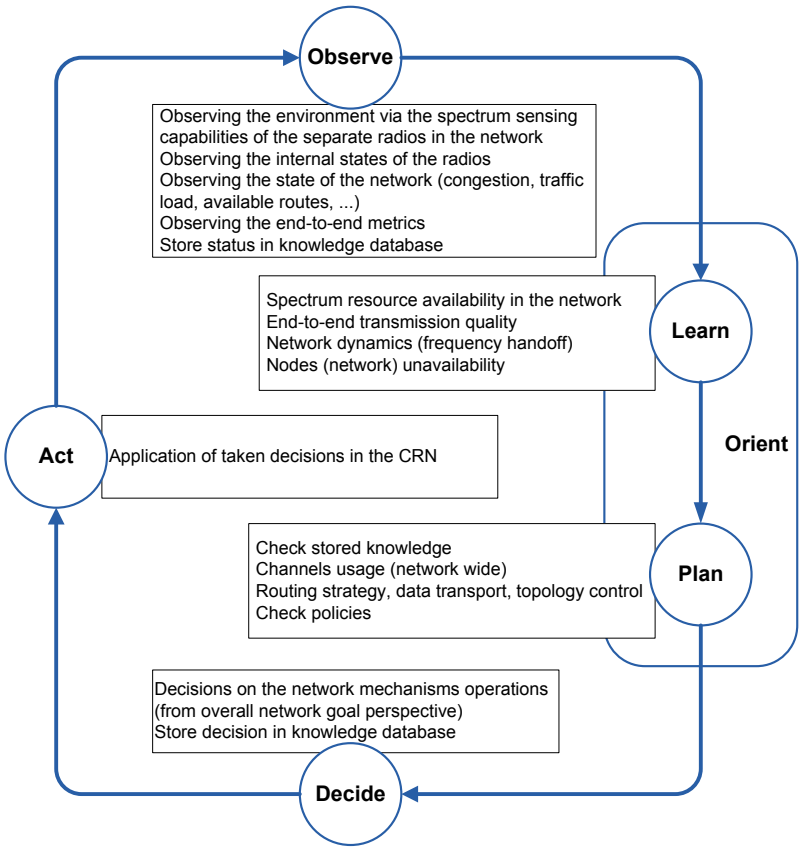



**Figure 2-1: Example Functionalities of the Network Cognitive Cycle.**

In order to avoid optimization conflicts between the individual node's and network's objectives, a deconfliction process has to be elaborated.

From the ITU-R definition of CRS, we infer that the notion of CRN is included in the definition, and we further point to the fact that Ref. [11] further defines the "node" as a singular element within the system instead of a "radio unit" or "radio device".

Ref. [13] furthermore introduces the term Cognitive Radio Ad Hoc Network (CRAHN), which describes a CRN specifically designed for ad hoc networking tasks. CRAHNS can be distinguished from infrastructure networks by their distributed multi-hop architecture, their dynamic network topology, and the time and location, varying spectrum availability.

As this report mainly focuses on ad hoc networks, without completely omitting infrastructure networks though, the terms CRN and CRAHN are not strictly distinguished. Nevertheless, the usage of the term CRAHN in this report indicates that the related section is mainly applicable to ad hoc networks and less relevant for infrastructure networks.

### 2.1.5 Related Terminology

- A **Cognitive Specification Language (CSL)** describes the interfaces between policies, objectives, and the cognitive engine.
- A **Network Knowledge Representation Language (NKRL)** is used to store and communicate information regarding network state (e.g., router metrics) to cognitive engines.
- **Policies** are regulations / sets of rules that allow, disallow or prioritize network parameters.
- **Goals/Objectives** in a networking context are desired results of end-to-end optimizations.
- A **Strategy** is an algorithm used to find a set of network parameters to achieve one or multiple goals, taking into account policies.
- The **Cognitive Engine** is the decision taking entity in the CRS that uses one or more strategies for decision making.
- A **Primary User (PU)** is a spectrum user, who has higher priority or legacy rights on the usage of a specific part of the spectrum [14].
- A **Secondary User (SU)** is a spectrum user who has lower priority and therefore exploits the spectrum in such a way that it does not cause interference to primary users [14].

In civilian/commercial domains, PU refers to the incumbent user whose systems are to be protected from interference of the SU accessing spectrum opportunistically. The concept of PU and SU could be adopted into a military CRS as defined in civilian/commercial domain. That can relate to the prioritization of one network to another one, but also to services/functions inside one network. An example of the latter, approach could be that preference or priority to spectrum is being assigned to important time-sensitive uses, such as fire control and intelligence, whereas the secondary spectrum access status is to be assigned to less time-sensitive uses like regular reporting and administrative users.

## 2.2 WHAT ARE THE BENEFITS OF COGNITIVE RADIO NETWORKS?

CRN go beyond current networks, as they do not only take into account topology information, but also perform reasoning based on relevant measurement data and continuously adjust their parameters based on the results. They further go beyond CR, as they do not only try to find the optimal frequency for one link but focus on achieving end-to-end optimization. This leads to several benefits.

Most important is an improved availability of critical communications for the soldier in the field. Moreover, efficiency and robustness of communications are improved, which results in improved end-to-end Quality of Service (QoS) and Quality of Experience (QoE). In addition to that, the autonomous adaptation capability of CRN allows for an adjustment of communications to changing user needs. Furthermore, autonomous reactions on changes in the environment do not require any user intervention, e.g., CRN are able to cope with simple electronic attacks.

By using CRN, not only are user interventions during a mission reduced, also less administrative activities before and after a mission are required. Due to automatic device configuration, there is a reduced burden on mission planning and data retention. Furthermore, networks are (re)configured very fast. In addition to that, less focus on radio operation and configuration results in more focus on the mission.

Benefits like efficiency and robustness can only be achieved when the CRN is able to quickly adapt to arbitrary environments and user needs. That requires considering a multitude of information on possible routes, disturbances on these routes (congestion, interference), message priorities, node mobility, etc. The adaptation can concern transmission parameters like frequency, power, or modulation, but also lead to changes in the network setup. Also, knowledge of the currently available battery power of individual nodes can improve CRN lifetime and the robustness of end-to-end connectivity.

As giving an optimal set of parameters for all possible environment information is hardly achievable, there must be capability inside the network that constantly observes its status and learns from previous actions in order to better adapt to unknown environments. There may be no single optimal solution for the adaptation, as different local optimization functions may conflict with the global optimum but targeting a global optimum will increase the network and services utility.

This report shall consider CRN technologies in a domain agnostic manner. However, the Research Task Group assesses that most benefits are applicable to user environments where:

a) Radio channels are variable (mountains, etc.);

b) Hostile Electronic Warfare (EW) measures can be expected;

c) There are a number of radio nodes to be networked;

d) Nodes may belong to different formations, units or even nations; and

e) Capabilities of nodes vary (e.g., vehicular *vs*. handheld).

These characteristics lead to the assessment that CRN technologies would be most beneficial in the Land Tactical domain while recognizing that aspects of such technologies may also have added value in other domains.

In the course of preparing this report, the Research Task Group was well-aware of existing challenges contemporary MANETs face, e.g., in terms of scalability and network setup times. This report assesses the feasibility of CRAHNs, assuming that cognition in networks may either solve or alleviate these challenges, but that this assumption is yet to be properly verified by demonstrations and prototyping.

## 2.3 WHAT ARE THE CHALLENGES?

One of the most important capabilities of modern military communication systems is networking, which allows for automatic message forwarding even in heterogeneous communication equipment. Networking not only lays the foundation for message forwarding, but it also furthermore organizes the routing of messages based on network topology information. But, for achieving optimal end-to-end connectivity in unknown or hostile environments (e.g., on a mission), also information about the electromagnetic spectrum is necessary.

This information needs to be collected and be regarded in the processes of routing, topology control, data transport, and network management.

For using CRN towards a network's end-to-end objectives, it is furthermore necessary to limit the overhead on the control channel and the complexity of the algorithms. Indeed, CRN will need to track different metrics for routing, topology control, data transport, and network management for multiple channels at the same time. This knowledge requires new algorithms able to track multiple channels with increased overhead on the control channel. It can be expected that the network performance will increase for networks operating in an environment that changes only slowly over time. However, for networks operating in a fast-changing environment, the development of optimization algorithms able to cope with this environment in a timely fashion is a challenge.

Considering the architecture of a network, there are basically two types, infrastructure and ad hoc networks. While infrastructure networks are associated with centralized network organization, ad hoc networks are rather associated with distributed network organization. Therefore, CRN need to support both centralized and distributed networks. In addition to that, the military specific considerations, like the avoidance of a single point of failure or the support for Transmission Security (TRANSEC) and Communications Security (COMSEC), need to be regarded.

Routing must take into account the frequency availability information for determining the path and thus the next hop. Future frequency availabilities can only be predicted based on statistics of previous occupations, which therefore must be recorded.

The main challenge for topology control is to keep topology information about the whole network up to date. This can be impeded by temporal resource unavailability or heavy changes in the topology due to mobility. In heterogeneous networks, common topology information is a challenge, especially if this information is classified.

Data transport mechanisms need to be adapted to support the dynamics of CRN. Existing protocols have limited knowledge of the network and the spectrum conditions, which is required for adequate reactions on congestion or bandwidth changes. Moreover, message loss due to changes in the CRN must be avoided.

When a CRN is in operation, network configuration should be automated as far as possible. For this, an optimal balance between automation and human control must be found. The interaction between network configuration and the battle management systems containing information on the environment like the Common Operational Picture (COP) may be seen more like an administrative than as a technical challenge. In order to guide the autonomous decision-making process, policies need to be defined and be applied.

## 2.4 REFERENCES

[1] Tuukkanen, T. and Anteroinen, J., "Initial Assessment of Proposed Cognitive Radio Features from a Military Perspective." 18th International Command and Control Research and Technology Symposium (ICCRTS), Alexandria, VA, USA, June 2013.

[2] Mitola, J., "Cognitive Radio: Making Software Radio More Personal." IEEE Personal Communications, pp. 13-18, August 1999.

[3] Haykin, S., "Cognitive Radio: Brain-Empowered Wireless Communications." IEEE Journal on Selected Areas in Communications, 23, pp. 201-220, February 2005.

[4] Fette, B.A., Cognitive Radio Technology. Second Edition, Academic Press, 2009.

[5] Software Defined Radio Forum. “Cognitive Radio Definitions.” SDRF-06-R-0111-V1.0.0, 8th Nov 2007.

[6] Software Defined Radio Forum. “Cognitive Radio Definitions and Nomenclature.” SDRF-06-P-0009-V1.0.0, 10th Sept 2008.

[7] Needs, H.H., “Research and Development on Software Defined Cognitive Radio Technology.” ITU-R WP 5A Seminar on SDR and CR Systems, 4th Feb 2008.

[8] Mitola, J., “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio.” Royal Institute of Technology (KTH), Stockholm, Sweden, 2000.

[9] Mukesh, G., and Kumar, S., “Cognitive Radio Technology: Architecture, Sensing and Applications – A Survey”, International Conference on Emerging Trends in Engineering, Science and Management, Hyderabad, India, March 2017.

[10] International Telecommunications Union, “Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS).” ITU-R SM.2152, 2009.

[11] International Telecommunications Union – Working Party 5A, “ITU-R M. [LMS.CRS2] Cognitive Radio Systems in the Land Mobile Service.” Tech. Rep. 5/178-E, 6 Nov 2014.

[12] Tang, H. and Watson S., “Cognitive Radio Networks for Tactical Wireless Communications.” DRDC – Ottawa Research Centre, Scientific Report DRDC-RDDC-2014-R185. December 2014.

[13] Akyildiz, I.F., Lee, W-Y., and Chowdhury, “CRAHNs: Cognitive Radio Ad Hoc Networks.” Ad Hoc Networks, Elsevier, Vol. 7, Issue 5, pp. 810-836, July 2009.

[14] Arslan, H. (Ed.), Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems, Springer, p.263, 2007.

# Chapter 3 – SCENARIOS AND USE CASES

## 3.1 SCENARIOS FOR COGNITIVE RADIO NETWORKS

In this chapter, military scenarios are introduced to point out the possible value of CRN in military operations. The scenarios used in this chapter are derived from NATO NCIAs TN-1331 document [1]. In this document six scenarios are described for MANETs. Two of these scenarios were selected to demonstrate the use of CR. The chosen scenarios are:

1) Convoy protection and situational awareness; and
2) Disaster recovery and reconnaissance.

The second scenario was simplified, and the original Non-Governmental Organization (NGO) was replaced by a military organization of another nationality to create a situation, in which the merging networks could be demonstrated in a better way. In addition to the chosen scenarios, vignettes are applied to the chosen scenarios to refine the application for CRN.

## 3.2 CONVOY PROTECTION AND SITUATIONAL AWARENESS

In this scenario, two NATO convoys are on the way and they meet each other halfway (see Figure 3-1). Both convoys make use of four networks in total. The first network is the local convoy network. This network is a UHF network and is used to communicate and exchange data between the vehicles of the convoy. The second network is the backbone to the Headquarters (HQ). This is done through a satellite link. One of the convoy vehicles is therefore equipped with a satellite communication system. The third network is used to establish a coalition network when another convoy or compound comes in range. The fourth network is used to retrieve sensor data from sensors placed along the route.

The sensors along the route gather magnetic, seismic, and acoustic data to detect (the placement of) Improvised Explosive Devices (IEDs). The sensors will store the data gathered and wait until a passing vehicle will connect to the sensor. The connection is made with a UHF ad hoc network. Usually only the first vehicle in a convoy is equipped with a radio system that can connect to the sensors. The sensor data is then relayed via the convoy network to all the other vehicles, if necessary, through several hops. The Common Operational Picture (COP), which consists of both sensor data and convoy data, is transmitted to the HQ using the satellite link.

Two convoys are on the way, one travelling from north to south, the other in the opposite direction. When the two coalition convoys meet, their coalition networks will connect with each other, and situation awareness and relevant mission data are exchanged. This data is valuable for both convoys, because it gives them information about the route ahead.

The threat in this scenario is a hostile UHF jammer placed near a sensor, blocking its communication with passing convoys. An IED is placed nearby and is operated with a VHF remote control.

### 3.2.1 Vignette 1: Two Non-Cognitive Convoys

#### 3.2.1.1 Description

In this vignette of the scenario, it is assumed that both coalition convoys are using Non-Cognitive Radio Networks (Non-CRN). Both convoys have a local convoy network on UHF, both on the same frequency. In addition, there is a common coalition UHF frequency used by both convoys; however, both convoys use a different waveform and are, therefore, unable to exchange information. The sensor radio network is also a UHF and Non-CRN network.

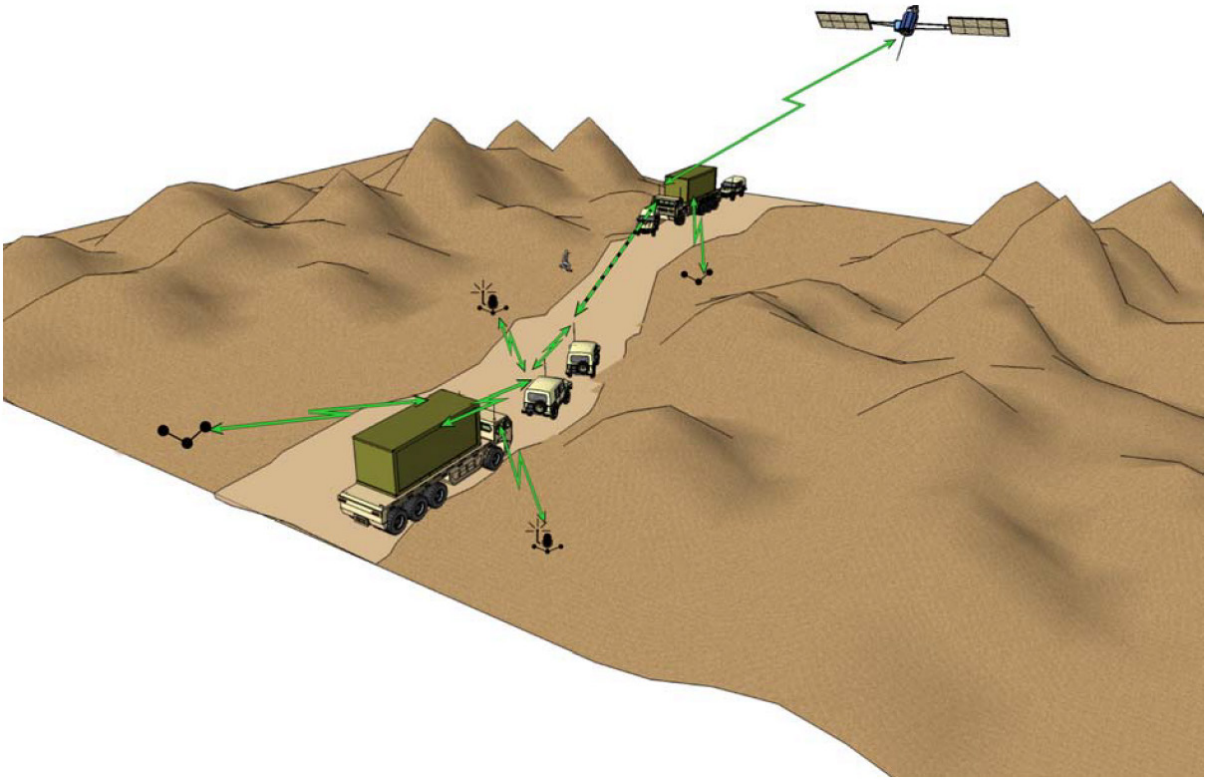


**Figure 3-1: Convoy Protection and Situation Awareness Scenario.**

#### 3.2.1.2 Storyboard

The situation in the African country of Sambala is deteriorating since armed guerrillas have violated the cease-fire. The French forces have secured the northern area around the city of Lumpía. A French convoy is now transporting wounded civilians from the city of Lumpía to the German compound near the airport south of the city from where they will be evacuated. The same day, a German convoy with ammunition and supplies is leaving the German compound and is heading north to Lumpía.

Helmut is a sergeant on the German convoy. Today, Helmut is assigned a new task. A series of seismic sensors is placed along the route to detect possible insurgents placing an IED. Helmut's job is to interpret the data from the sensors that are placed along the route. The sensor data is picked up by the first vehicle in the convoy and then sent over the local convoy network to the SATCOM vehicle. This vehicle has the backbone connection to the German HQ and is placed last but one in the line of the convoy since this is the safest position for IEDs. Helmut was glad to get this task because he could now use the better chairs of the satellite equipped vehicle, and he was curious about the information he could get from the sensor data.

The convoy departs from the German compound exactly at 10:00 as planned. The estimated time of arrival in Lumpía is 16:00, and Helmut is looking forward to visiting the city of Lumpía, since he has never been there before and had heard good stories about this beautiful city.

They are half an hour on the way and Helmut is studying the data that is coming in from the sensors. The sensors data goes back a whole week, and he can see that another convoy had passed three days earlier. This information is also sent over the satellite link to the German HQ.

The French convoy has a similar system, but in addition, they have a jammer that jams frequencies in the VHF band. This should protect them against some of the most frequently used radio-controlled IEDs and

would leave the UHF frequencies free for the convoy networks and the sensor receiver. SATCOM is not affected by the VHF jammer, either.

Jean-Pierre is studying the sensor data in the French convoy, and he too can see the data from the convoy that passed here three days ago. At 11:30, Jean-Pierre notices that sensor data is not being received anymore. From five known sensor locations in a row no data is received, and the last sensor that came within visual range contained bullet holes. This is clearly an indication that insurgents have been active, and he makes a notification that is sent to all other vehicles. The same message is sent to the HQ over the satellite link, and it is also stored on the bulletin board of the coalition network.

Later that day, they meet the German convoy. The very first thing they notice is that the squelch of the local voice channel of the convoy network opens, and they hear disturbing sounds in their headphones. The German local convoy network operates on the same frequency! When they pass by, no communication is possible at all within Jean-Pierre's convoy. That is very inconvenient, because just when there is a need to communicate about the other convoy, all local communications are disrupted, voice and data, alike!

The communication with the German convoy is attempted over the coalition channel, but that is not successful, either. The coalition frequency is used by both convoys, but since different waveforms are used, the communication cannot be established.

The convoys stop for a minute, so the drivers of the first vehicles can talk to each other through the open window and exchange information about the condition of the road ahead. The missing sensor data, however, is not discussed because the drivers consider this a technical issue for the communication vehicle and not a driver's issue.

At 15:30, Helmut is looking at the real-time sensor data. He notices that from the last two known sensor positions, no data has been received at all. He thinks it is probably no problem because the French convoy has passed that point safely earlier today. However, he did not realize that the French have used their VHF jammer against IEDs, and they do not have one.

#### 3.2.1.3 Conclusion

In this scenario, there was no communication possible between the convoys on the coalition frequency, when the French and the German convoys met halfway because of the different waveforms used.

The French convoy was not warned about an IED threat because the communication with the road sensor was jammed. They were lucky because their own VHF jammer avoided the activation of the IED.

The German convoy was not so lucky. The information that sensor data was missing on part of the trajectory was available within the French convoy but could not be transferred to the German convoy because of interoperability issues. The IED could not be detected nor could activation be prevented resulting in a loss of life and materiel.

### 3.2.2 Vignette 2: One Cognitive and One Legacy Convoy

#### 3.2.2.1 Description

In this vignette of the scenario, it is assumed that the German convoy is using CRNs, and the French convoy is not. The sensor radio network is also cognitive.

#### 3.2.2.2 Storyboard

The French convoy leaves the city of Lumpía on its way to the German compound near the airport at 10:00 as planned. At the same time, the German convoy leaves the airport and heads for Lumpía.

Jean-Pierre is studying the data that the French convoy retrieves from the sensors. At 11:30, he notices that sensor data is not received anymore, but the convoy proceeds without problems.

Later that day, the French and the German convoy meet each other. Both local convoy networks operate at the same frequency. Therefore, there is some interference, but before this leads to real communication problems, the German cognitive local convoy network detects this and is automatically switched to a new frequency, and both convoys maintain local convoy communication.

Both convoys are interested in the information that the other convoy has retrieved from the sensors because it is useful information about the route ahead. Since both convoys use different waveforms, it takes an extra minute for the German cognitive system to automatically recognize the French waveform and to adapt to it. Then, the collected sensor information is exchanged.

At 15:30, Helmut is signalling the driver of the first vehicle in his convoy that, according to the French information, there is extra attention required because of the missing sensor data. Therefore, the speed of the convoy is reduced. Ten minutes later, the missing sensor information is successfully retrieved by the German convoy from the jammed sensors because the cognitive sensor network was able to negotiate a new and undisturbed frequency with the German convoy. The sensor information gave clear indications on where a possible IED was located, and the convoy was able to eliminate the threat. Both convoys arrived safely at their destination, and while Helmut enjoyed a nice dinner at Lumpía's city centre, Jean-Pierre enjoyed a well-prepared schnitzel at the German compound.

#### 3.2.2.3 Conclusion

Like in the first scenario, the French convoy was not warned about an IED threat because the communication with the road sensor was jammed. The road sensor had the possibility to avoid the jammed part of the band, but the French radio had no means to make use of this feature. The French convoy was aware of the jamming of the sensor but remained unaware of the presence of the IED. They were lucky because their own VHF jammer avoided the activation of the IED.

When the two convoys met halfway, the German local convoy network noticed the interference caused by the French local convoy network on the same frequency and switched to a free channel. Thus, both local convoy networks remained operational.

The information about the jammed sensor was passed to the German convoy over the coalition network, even though the French and the German coalition networks used different waveforms. Due to the cognitive capabilities of the German network, its waveform was adapted automatically to the waveform used by the French convoy.

The lack of sensor information received from the French convoy caused a minor warning in the German SA system. Fortunately, the German cognitive sensor network was capable of communicating with the jammed sensor; a usable frequency was found and agreed upon with the sensor. Information about a possible IED placement was retrieved and caused a severe warning. Sensor information was delivered to the right vehicle just in time; therefore, the convoy stopped just before the IEDs location and could take appropriate actions. No injuries occurred or damage was suffered.

## 3.3 DISASTER RECOVERY

This scenario is based on the "Disaster Recovery in Cooperation with Civilian Organisations (CIMIC)" scenario from NATO document TN-1331 [1]. However, this is a complex scenario, and it is renamed and simplified here to demonstrate the advantages of CRs and CRNs. The figures from TN-1331 were adjusted to reflect the situation of this storyboard.

The scenario describes an area in which a natural disaster has happened (see Figure 3-2). German NATO forces secured the area and offer protection. They also do reconnaissance patrols to gather intelligence because enemy forces have taken advantage of the destabilized situation to infiltrate the area. At the same time, French NATO forces provide medical relief to victims. They also build temporary camps to host the displaced population. Both the German and the French forces brought their own MANETs. Both networks were configured to merge into one large ad hoc network to be able to use the advantage of relaying each other's messages. A relay is required because the distance between the area of operations and the headquarter is too large to be covered with a direct radio link. Therefore, a German relay vehicle is positioned halfway between the medical post and the headquarter. Other coalition posts are in the area as well and therefore sometimes a second route with three hops can be established, too, but this route is not preferred by the routing algorithm because there is an extra hop and less bandwidth. In addition, the links are unscheduled and not always available. The network can distinguish between restricted information and unclassified information and gives a higher priority to the restricted information. Reach-back from the headquarters is provided through a satellite terminal.

Three different vignettes of the scenario are described to show the possible difference between a non-Cognitive Radio Network, a non-cognitive network with cognitive radios, and a cognitive network.

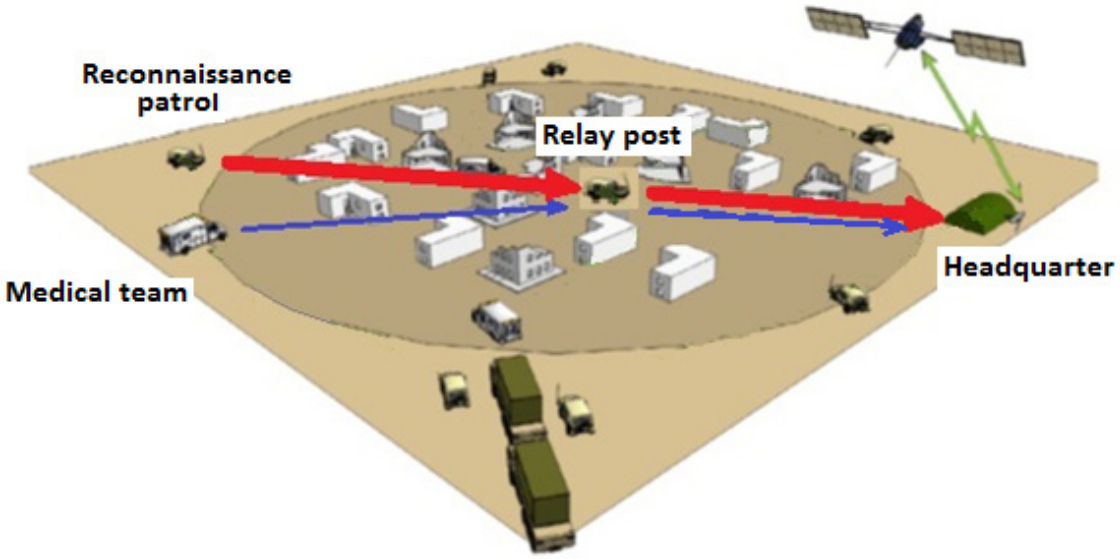



**Figure 3-2: Pictorial View: Disaster Recovery and Reconnaissance.**

### 3.3.1 Vignette 1: Ad Hoc Non-Cognitive Networks

#### 3.3.1.1 Description

To highlight the advantages of a CRN, we will first look at a situation where no cognition is available in neither the radio nor the network and see what happens (see Figure 3-3). In the first vignette, the German NATO convoy escorts a French medical NATO convoy on the way to the target area. On arrival, the French medical team starts supporting the local population, while part of the German convoy stays at the site for protection of the medical team, while another part starts reconnaissance of the environment. The insurgents manage to position a VHF radio jammer between the relay vehicle and the headquarters. Therefore, all communication with headquarters is blocked.

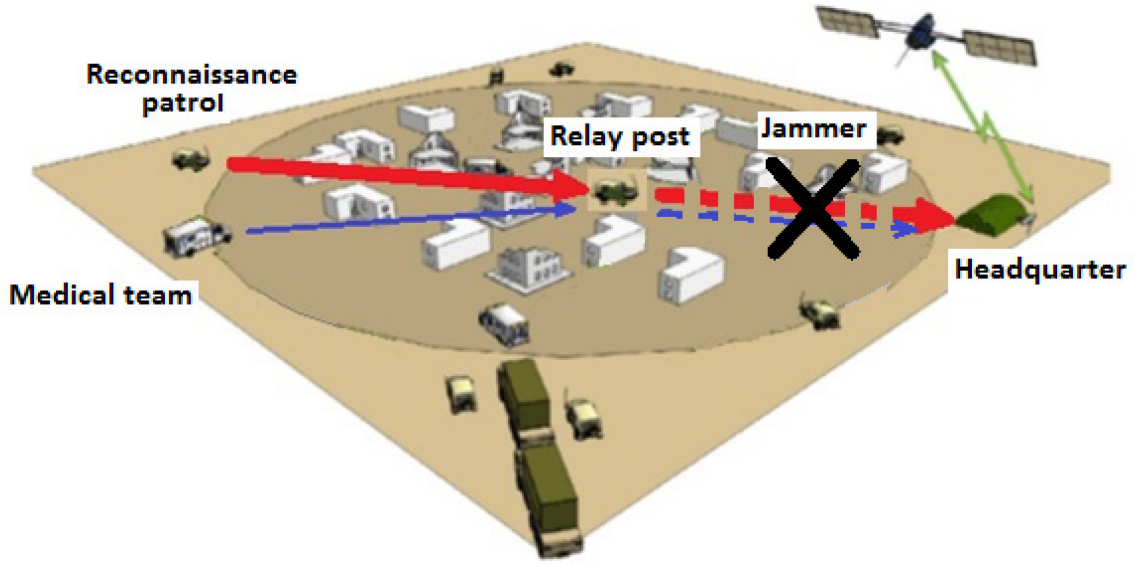



**Figure 3-3: Pictorial View: Vignette 1, Disaster Recovery and Reconnaissance.**

#### 3.3.1.2 Storyboard

The German NATO convoy finally entered the area around Lumpía after a long and dangerous trip from the southern compound near the airport. A convoy from the French medical emergency response team joined them at the rendezvous point to be escorted into the area, and together they continued the journey. The armed escort was necessary because recent reports mentioned armed groups of bandits that raided the area east of Lumpía, and this was exactly the place where the humanitarian convoy was heading to assist the population after a devastating typhoon had hit the region. At 14:00, the combined convoy arrived at the destination. The commander of the convoy immediately arranged a meeting with the local leaders to find out what the most urgent problems were, which help was needed and what information about armed bandits was available.

Right after the meeting, everybody started their work. The first priority for the French medical team was to build up tents, so the people whose houses were destroyed would have a place to stay. The German convoy split up. Part of it stayed with the rescue workers for protection, and the other part started a reconnaissance of the environment to check the information about the armed bandits.

Meanwhile, at the French medical team, Julie and Bernadette were well on the way building up the tents. The fourth tent was almost finished when their attention was drawn to a small boy and his mother. The woman seemed to be in trouble. She was pregnant and about to deliver a baby. Julie and Bernadette put her in the first tent on a stretcher. Julie was a nurse, noticed strange symptoms and suspected complications. Unfortunately, there was no doctor travelling with them because there were only three doctors in the area. Two of them were occupied elsewhere, and one had to stay at the headquarters. The only way to get medical advice was to contact the doctor at the headquarters over the radio. Fortunately, the French and the German networks had merged because the headquarters was too far away to be reached over a single radio link. A German vehicle was positioned halfway and relayed the signal to HQ. Soon, the doctor was reached, and Julie could discuss the complications and possible solutions with him.

In the meantime, Gunther was leading the reconnaissance patrol in the eastern part of the area in search of “armed uncontrolled forces”. From the meeting with the local leaders, Gunther understood that the bandits might not just be ordinary bandits but could possibly be uncontrolled parts of the army from the neighbouring country of Nassygorang. So, this could become a very sensitive political issue. They picked up fresh car tracks that went off-road to the east, and they followed these tracks the rest of the afternoon.

The landscape slowly changed, the forest became denser, so there were more opportunities to hide. When, early in the evening, Gunther's infrared sensors detected something, they immediately left the track and hid the vehicles in the bushes. Minutes later, five vehicles passed them. The first two were pickup trucks with heavy machine guns mounted, but the last three were armoured vehicles with registration signs from the regular army of Nassygorang. Gunther's team was able to capture everything on video, including close-ups from the light anti-tank and anti-aircraft weaponry. The last armoured vehicle carried a lot of impressive weird-looking antennas. It looked like forces from the neighbouring country of Nassygorang had invaded Sambala territory after all, and now they had evidence. Time to go back and report to headquarters!

Back at the camp, they used the VHF radio to report everything to headquarters. Due to the delicacy of the matter, HQ requested all the video materiel to be sent immediately. This would take several hours because of the narrow bandwidth of the VHF radio link. But the relay vehicle was positioned well, so the radio link should be reliable. Gunther started the file transfer at 21:17. Minutes after the file transfer started, it got stuck, too many errors. The file transfer was abandoned, and the relay vehicle was contacted. They said that their link with headquarters was jammed and no communications were possible with anything west of their position. Gunther wondered if it had anything to do with the armoured vehicle from the insurgents they had seen earlier today with all the strange antennas mounted.

Julie and Bernadette had finished a hard day's work, and most of the tents were finished. They were worried about the condition of the pregnant woman, so they took turns in looking after her. In the afternoon, the doctor at the HQ told them over the radio to inform him whenever the situation changed. Unfortunately, the situation deteriorated that evening. The pregnant woman was in more pain, the fever went up, and she was no longer able to answer simple questions. As a nurse, Julie realized that something had to happen now, but she did not know what. So, at 21:15, she decided to use the VHF radio to contact the doctor at HQ. She explained the new situation to the doctor and then she asked for advice. But there was no response anymore, just a lot of noise from the speaker. This was a very bad moment for the radio to stop working…

#### 3.3.1.3 Conclusion

In this scenario, the remote link from the relay station to the headquarters was jammed by the insurgents. The radio was not a CR; therefore, there was no action possible to mitigate the jamming. Manual efforts to change the frequency were not successful because the jammer followed the radio in the VHF band, and the option to change the frequency band to UHF could not be communicated because of the jamming. As a result, there was no communication possible for both the German reconnaissance patrol and the French medical team.

### 3.3.2 Vignette 2: Ad Hoc Networks of Cognitive Radios

#### 3.3.2.1 Description

The scenario is the same as in Vignette 1, except that this time CRs are used (see Figure 3-4). Therefore, the jamming on the remote link is recognized by the radios of the relay vehicle and at the headquarters, and a new frequency was negotiated.

#### 3.3.2.2 Storyboard

The storyboard is largely the same as in Vignette 1, up until the moment the insurgents start jamming the link to the headquarters. From this moment on, the CR selects another frequency for the link.

Gunther and his team arrived at the camp with the video recordings of the insurgents. When he reported to the headquarters that he had video images, headquarters requested the images to be sent immediately with high priority over the confidential network. Gunther started the file transfer at 21:17. At first, he noticed that the file transfer did not go as fast as he expected. He checked the signal-to-noise ratio of the link to the relay vehicle, and that was good. There was nothing more that he could do.

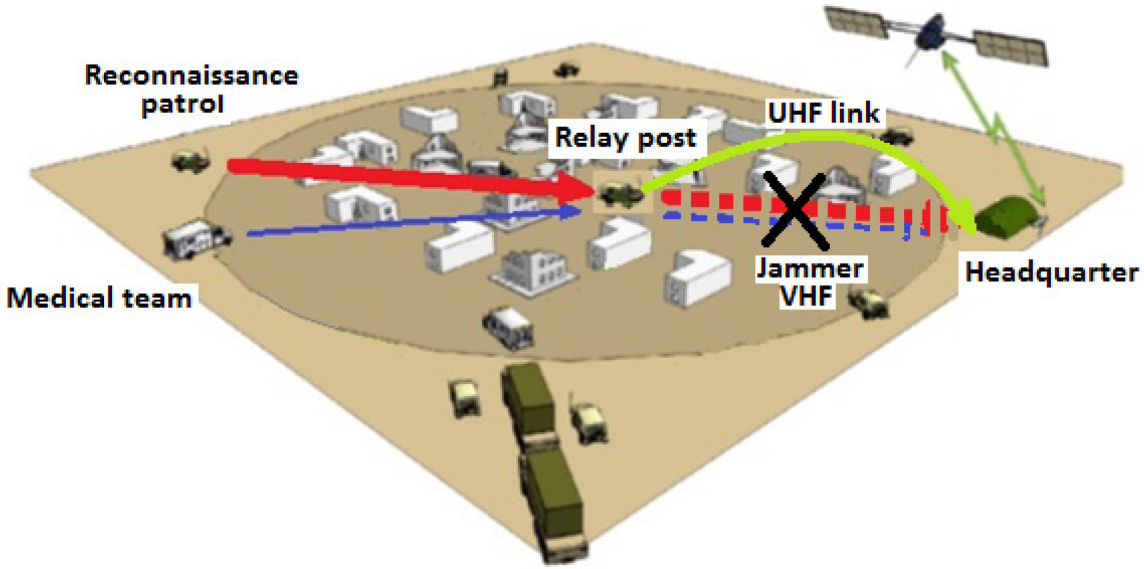



**Figure 3-4: Pictorial View: Vignette 2, Disaster Recovery and Reconnaissance.**

At the relay vehicle, the operators got a notification from their CR that the radio link to the headquarters was severely degraded and that the radio had negotiated a different frequency and had switched to that frequency. Six consecutive notifications were received because six times in a row the frequency was changed. Each time, the CR found a free frequency and switched to it, the jammer followed the radio to the new frequency and communication was disrupted again. After six times, the radio was programmed to switch the frequency band to UHF. Since the jammer was a VHF jammer only, communications were re-established on UHF. All this happened automatically, and no intervention from the operators was required. In fact, the operators saw the notifications once they returned from their coffee break.

Gunther was really annoyed. He had promised the headquarters to send them the video images. He knew how important the videos were for the peace talks that would take place on a diplomatic level in Lumpía the next morning. But the file transfer stopped, and there was nothing he could do about it. After five minutes, however, the file transfer proceeded again. Because of the long distance and the limited bandwidth, it took an hour and a half, and then the files were sent successfully. Gunther felt a tremendous relief when he got the confirmation from the headquarter.

Julie and Bernadette were still stuck at the medical post. The situation with the pregnant woman got worse, and her son started to panic. Five minutes later, the radio stopped making strange noises and the situation looked better, but no contact could be made with the headquarters. This was the moment that the jammer was mitigated by switching the remote link to UHF. But now the video transfer of the reconnaissance patrol was sent. It had a higher priority because it was a classified transfer, and it took all the available bandwidth for an hour and a half. When, late that night, the radio connection of the medical post was re-established, it could only be used to bring bad news.

#### 3.3.2.3 Conclusion

In this case, the cognition of the radio gives a clear advantage. The jamming of the insurgents could be mitigated by changing the frequency band. Therefore, the video images of the reconnaissance mission could be sent to the headquarters. Due to the sensitivity of the materiel, this file was sent over the classified part of the network. At the time the network was designed, it seemed a good idea to give the classified part of the network a higher priority than the unclassified part. Therefore, the German classified video transfer

overruled the French voice service and because of the amount of data, it fully occupied the available bandwidth for the duration of the transfer. As a result, the contact between Julie and the doctor was dropped when the video file transfer started. The sad thing was that there was another route available. However, despite the congestion on the main link, the alternative route was not considered by the routing algorithm because of the extra hop count.

### 3.3.3 Vignette 3: Cognitive Radios in a Cognitive Ad Hoc Network

#### 3.3.3.1 Description

The scenario is the same as in Vignette 2, except that this time, the network has cognitive capabilities (see Figure 3-5, below). The jammed link between the relay vehicle and the headquarters is a physical layer problem and is dealt with locally by the CRs. The congestion on the remote link, when the video file transfer starts, is a routing problem. It is recognized locally, and the information is conveyed to the other nodes. The cognitive routing algorithm of the network now routes traffic with a lower priority over the alternative three-hop link. This link has a higher hop count, more delay and less bandwidth and would not be considered by normal routing algorithms. The network cognition, however, uses the link to solve the problem of the congestion on the remote link.

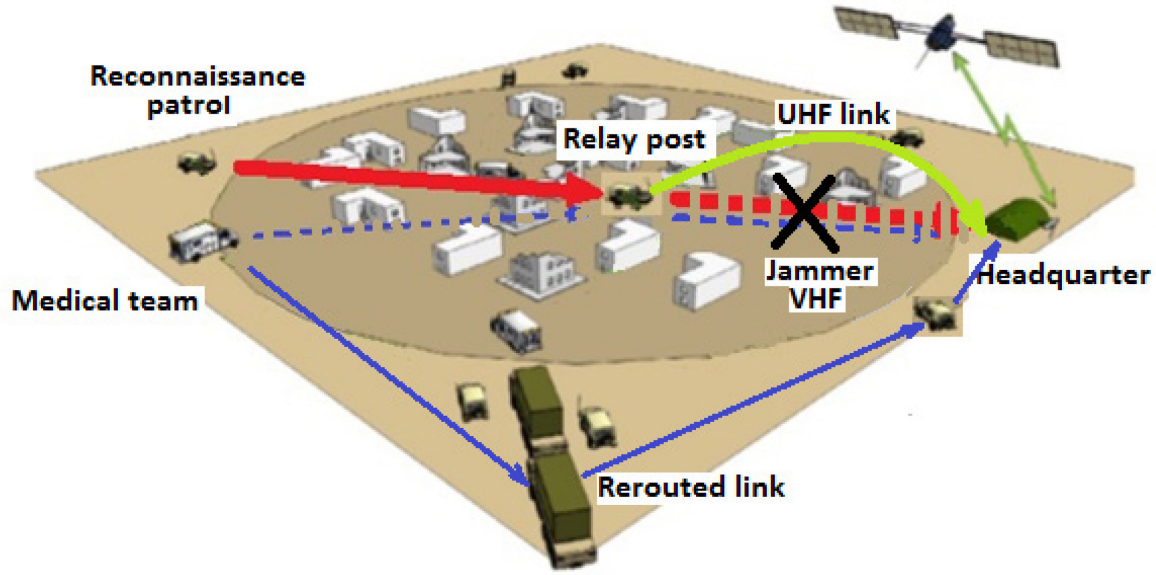



**Figure 3-5: Pictorial View: Vignette 3, Disaster Recovery and Reconnaissance.**

#### 3.3.3.2 Storyboard

The storyboard is largely the same as in Vignette 2, up until the moment the reconnaissance patrol starts sending the large video files to the headquarter over the VHF link.

Gunther started the file transfer of the video files and was worried because the transfer did not go well in the beginning. But, after a few minutes, the data started to flow and proceeded well.

At the medical compound, nurse Julie saw the condition of her patient deteriorate, and she decided to use the VHF radio to contact the doctor at HQ. She explained the new situation to the doctor and then she asked for advice. For some strange reason, there was an interruption in the radio traffic for a couple of minutes. After that, there was some delay on the line. This caused some trouble in the communication because a few times

in a row, they started to talk simultaneous or were both waiting for each other for a response. But they soon adapted to the delay, and they started to make plans. They did not know that the link between the relay vehicle and the headquarters was jammed, and the jamming was mitigated by the CRs, and furthermore, their access to the radio link was denied because of the higher priority of the video file transfer from Gunther. The cognitive network, however, was notified on the congestion of the remote link and an alternative route was looked for and found via several other coalition posts that could relay the transmission. Because of the multiple hops, there was more delay, but Julie was very happy to get the support from the doctor. The decision was made to operate on the woman and get the baby out with a C-section. Julie had never done this before, but with the directions from the doctor, she did a very good job. Bernadette assisted her and within 30 minutes, a healthy boy was delivered. The mother fully recovered, although it took a couple of weeks. She realized that without the medical help she received, things would not have ended so well. She was so grateful that she named the baby Julian Bernard Crahn after the nurse Julie, her colleague Bernadette and the Cognitive Radio Ad Hoc Network (CRAHN).

#### 3.3.3.3 Conclusion

In this vignette, both the radio and the network have cognitive capabilities. The cognition of the radio enabled the video transfer despite the jamming by the insurgents, like described in the previous vignette. The cognition of the network was able to deal with congestion on a remote link, thus enabling the voice connection of the medical team with the headquarters by rerouting it over a route that would not be used with standard routing protocols.

## 3.4 REFERENCES

[1] NATO Consultation, Command and Control Agency (NC3A), “Ad Hoc Networking for NATO – Operational Benefits”, Technical Note 1331, The Hague, February 2011.

# Chapter 4 – COGNITIVE RADIO NETWORKING TECHNOLOGIES

In this chapter, we will discuss the technologies that are considered as essential building blocks in operating CRNs. These are also the technologies that need to be either defined or developed specifically for military CRNs, since the existing solutions have been mainly targeted for civilian applications and scenarios and may not be suited as such. We assume that the CR along its spectrum management capabilities and available technologies to support CRN operations exists. We note that in our opinion, the CRN is more than just a network of CRs. The network level cognition process to advance end-to-end operational performance is also needed. This process will (most likely) operate as a distributed process in the node level and needs the cooperation between nodes.

Figure 4-1 shows key functionalities of the cognitive node and the CRN. The illustration separates the node centric functions (cognitive node, left) from the network-wide functions (cognitive network, right). CR is mentioned as an essential element in the node architecture, although it or its algorithms (e.g., spectrum sensing) are not developed under this study (refer e.g., to CR working group NATO IST-077). Similarly, the application layer and related QoS issues are included in the figure but not addressed in the study. Ultimately, the technical solutions to be proposed by this study must be applicable to any application and use case. We note, however, that examples of applications were mentioned in connection to scenarios and vignettes presented earlier.

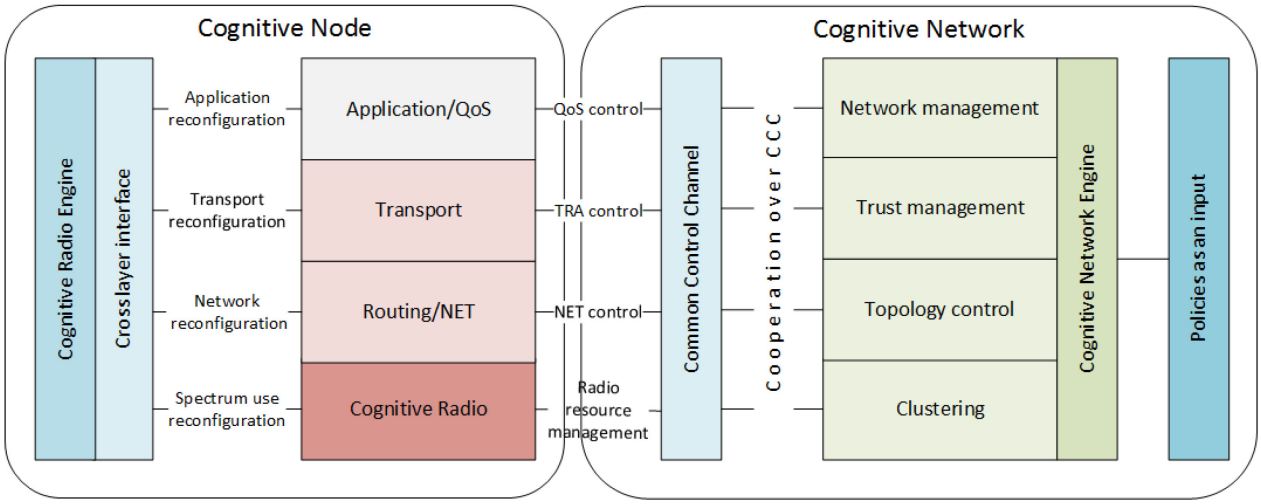



**Figure 4-1: Architectural View of the Separation Between Cognitive Node and Cognitive Network Functions.**

A key issue in the node-centric view is the inclusion of cross-layer functionality and the cognitive engine attached to it. These technologies make it possible to constantly reconfigure all layers of the radio node functions as advised by cognitive engine and possible policies and strategies therein. The cognitive network, on the other hand, requires the support of a Common Control Channel (CCC) as a key element to allow cooperative control over the whole network. The mentioned radio node layers can also use the CCC to perform network-wide reconfigurations of their operation parameters. This also includes that the CR nodes can manage or at least take part in the network-wide frequency use and coordination.

Cognitive networking is made possible by the cognitive nodes and a number of technologies that utilize the CCC for network-wide cooperative configurations. The technologies that have been judged as the most

important ones are clustering, topology control, trust management and overall network management. For example, cognitive routing and topology control are tightly coupled processes at the network level. Transport layer takes care of end-to-end connection management and congestion control. Clustering is a complex process that can be applied for many purposes in CRN operation. Objectives of network management include the overall network reliability, efficiency and capacity of data transfer.

In our view, the network management includes the goals, strategies and policies that are handled in the cognitive engine block, which ultimately dictates how the cooperative reconfiguration will and can be performed network-wide. Finally, trust management is needed for properly managing and evaluating the information exchanged between nodes in the CRN. Each of these technologies, as well as their significance in tactical/military cognitive networking, is further discussed below in Sections 4 to 4.7.

In order to adapt to the dynamic spectrum environment, the CR part of the cognitive nodes operating in a CRN (as depicted in Figure 4-1) perform spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility [1]. Each function influences different layers of the node and thus the operation of the whole CRN. This is well illustrated in Figure 4-2. The spectrum sensing process operates mainly in PHY and MAC layers, and it can provide information about the spectrum availability to the other functional processes and upper-layer protocols. The spectrum decision process is responsible for selecting appropriate channels based on the sensing results and spectrum sharing procedures. Spectrum decisions should also be based on the user (application) requirements resulting from the QoS assumptions. In order to allocate appropriate channels to the network, the nodes have to communicate using network layer. The spectrum decisions should also cooperate with the routing protocol to adjust the routes according to the routing metrics calculated based on the link characteristics. The spectrum sharing process is responsible for resource allocation to the CRN in order to avoid spectrum overlapping in the network and thereby lowering the possibility of interference and collisions.

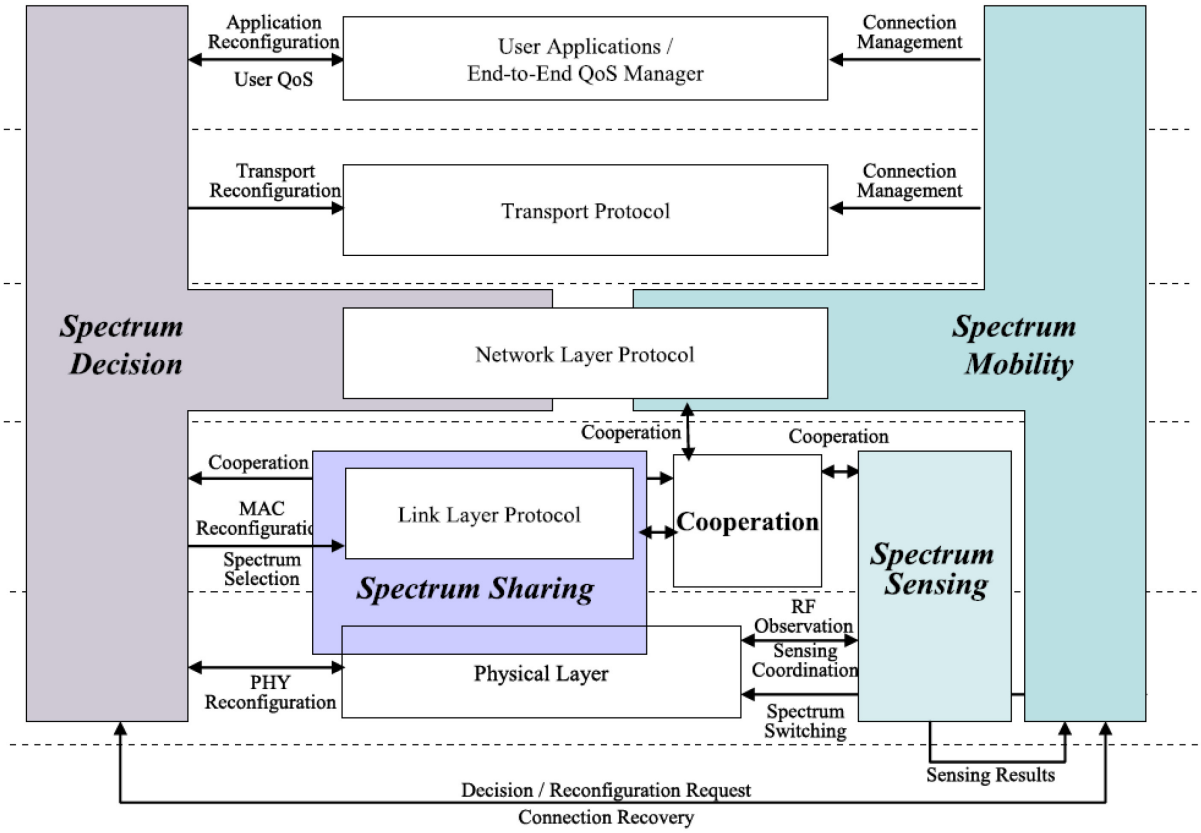



**Figure 4-2: Influence of CR on the OSI Layers [1].**

Most CRN solutions in this area are focused on the clustering algorithms implemented in data link layers of the nodes. Such solutions support controlled and hierarchical resource allocation, but also pose some problems connected with no effective network organization. Spectrum sensing activity allows detecting free bandwidth that can be used by the CRN. It leads to the spectrum handoff in some parts of the network and in consequence to appropriate reactions of the topology control mechanisms, routing, transport, and application protocols.

The next sections are focused on identification and description of challenges of the above networking issues, especially in terms of military requirements, and on exploring solutions for those challenges.

## 4.1 COGNITIVE ROUTING

### 4.1.1 State of the Art

Wireless ad hoc networks use a wide range of routing protocols, which construct typical routing tables, keeping only the next hop and metric information. Most of them are based on the proactive Optimized Link State Routing (OLSR) [2] or the reactive Ad hoc On-Demand Distance Vector (AODV) [3] protocols with some modifications to adjust them to a specific wireless environment. For example, to select links with the highest transmission quality instead of the shortest route, OLSR has been extended to calculate the Expected Transmission Count (ETX) metric [4]. Some of the routing protocols use geographical positions to find and select the best routes [5]. Others are equipped with mechanisms borrowed from nature (e.g., ant routing [6]). All of them can be used in the network layer of a CRN, but their effectiveness can be improved by using information from other layers.

Some proposals exist that are already tailored to specific types of CRNs (for example, Refs, [7], [8], [9]). They often do not meet military requirements in the area of reliable path (or multiple paths) selection and effective reaction on information from cognitive entities (route reconfiguration because of dynamically changing spectrum access or spectrum assignment policy). Very few of the proposals focus on Time Division Multiple Access (TDMA)-based radios, as they are rather uncommon in the civilian domain. A set of metrics should be proposed that is relevant from a military CRN's point of view and which can be effectively measured and used.

Many MANET routing protocols are based on shortest path metrics, but this rule is not always sufficient for CRAHNs. The very popular ETX metric can react on link quality, but its accuracy is dependent on the actual traffic exchanged over a particular link. Thus, some other metrics are proposed for non-military CRAHNs [10].

In the following, we present protocols specifically designed for CRAHNs. Currently, these protocols take into account the following routing metrics [11]:

- Hop count;
- End-to-end delay;
- Energy;
- Bandwidth;
- Route stability;
- Link and path quality; and
- Cumulative metrics.

In addition to that, the CRAHN's routing protocol should take into account PU activity, as well as identified multi-hop and multi-channel communication [12].

The example routing protocol proposed for CRAHNs named energy-aware routing protocol is described in [13]. It is based on the relative energy metric used to find and select the route, ensuring total power

consumption minimization in the whole network. The protocol is able to take into account available channels for each node and potential signal powers at each available channel. The authors in Ref. [13] propose to use following complex metric *W(i,j)*:

$$W(i,j) = P_{ij} \cdot \frac{L}{R} \cdot \left( \frac{E_{max}}{E_i - P_{ij} \cdot \frac{L}{R}} \right) \tag{4-1}$$

where $W(i, j)$, represents the energy weight of the link between $i$ and $j$ nodes (SUs), $P_{ij}$ is the transmitting signal power by the node $i$, $L$ is the length of the data in the session, $R$ is the communication rate, $E_{max}$ is the initial energy of each node, $E_i$ represents the current t energy of the node $i$, and the factor $E_i - P_{ij} \cdot \frac{L}{R}$ represents the reserved energy value.

The weights of the links are higher if the nodes have lower reserved energy. Thus, such links are avoided in the routes found by the routing protocol. The metric can be used both by proactive and reactive routing protocols. Essentially, the *W(i,j)* do not take into account the cognitive future of the network, but the intermediate nodes should also be selected based on the additional parameters, i.e., number of available channels in the nodes (nodes with more available channels are preferred).

A similar approach is proposed in Ref. [14], where an energy-based metric is completed by a latency factor, both used in multi-metric reactive protocol. The cumulative metric $M_{cum}$ is written as:

$$M_{cum} = \max \frac{E_{res}}{D} \tag{4-2}$$

where $E_{res}$ is the total energy of the end-to-end route, and $D$ is the average route delay. The route delay is especially important for real-time applications like voice.

The nodes can select the available channels (based on channels ranking list) during route discovery phase. Thus, CRAHNs can influence the appropriate channel selection (with lower interference, more stable, and using other criteria).

An on-demand routing protocol is proposed for TDMA-based CRAHNs in Ref. [15]. Both the routes and slots are selected based on the bandwidth requests. The energy-efficient routes are also used there, while a Dynamic Source Routing (DSR) protocol is proposed and a concept of route utility function $U_k$ is introduced:

$$U_k = \frac{E_{res,k}}{HC_k} \tag{4-3}$$

where $U_k$ is a route utility function for the $k$-th path, $HC_k$ is the total hop counts in the $k$-th path, and $E_{res,k}$ is a minimum residual energy of the $k$-th path.

Taking into account $U_k$, the preferable routes are those with higher energy left in the nodes between the sources and destinations, and additionally shorter ones (smaller *HC*). The authors of Ref. [15] propose to support routing by channel and slot assignment to ensure collision-free transmission. The solution advocates channel access scheduling to minimize data transmission conflicts among secondary users. It succeeds in distributing the traffic load among different SUs depending upon the residual energy of each node.

The Delay and Energy-based Spectrum Aware Reactive routing (DESAR) protocol for CRAHNs is described in Ref. [16]. The protocol supports bandwidth selection decisions by optimizing the routes in terms

of calculated transmission delays dependent on both a selected bandwidth and a number of nodes sharing the same bandwidth. An appropriate bandwidth allocation can influence the contention level decrease in the network, and in consequence the QoS is supported.

An Enhanced Dual Diversity Cognitive Ad hoc Routing Protocol (E-D2CARP) for CRAHNs is presented in Ref. [17]. In order to select the route, the E-D2CARP takes into account the following assumptions: Expected Path Delay (EPD), PU region avoidance, and joint path and spectrum diversity. The EPD is a metric that is dependent not only on the end-to-end delay of the packets sent over different paths, but also on the packet loss ratio registered at the links belonging to the paths. The route selection procedure allows avoiding the PU regions, which leads to interference reduction. To accomplish this goal, the SU CRs have to determine whether they are in the PU's transmission ranges at the specified channels. If yes, the CR routing signalling has to be able to inform the other nodes to avoid this region in their route selection (as shown in Figure 4-3).

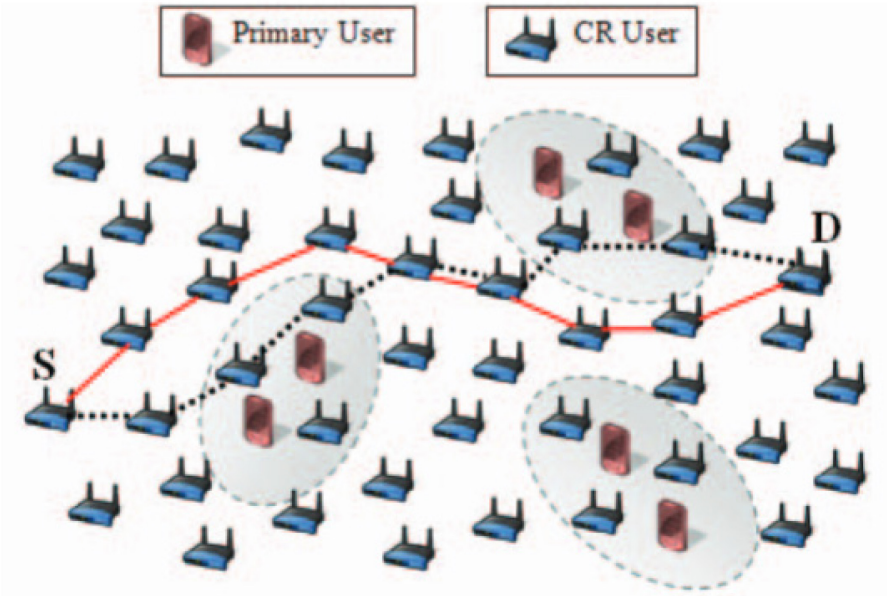



**Figure 4-3: PU Region Avoidance [17].**

Joint path and spectrum diversity solution gives a possibility to find multipath and multi-channel routes. Moreover, the SU can dynamically switch among different paths and channels while PUs are becoming active. Figure 4-4 shows the networks composed of PUs, which operate on two channels ch1 and ch2, and the network with SU nodes. If PU's network is not in operation, the SU's network can select the path based on EPD with any available channel (for example, ch2). If ch2 would be used by PU's network, some SUs can switch to ch1 without triggering a new route discovery process.

The E-D2CARP is an on-demand protocol, based on AODV with extension to support cognitive features of the multi-interface nodes. To find the paths, the Route Request (RREQ) messages are sent by the nodes over each non-occupied channel using all interfaces. Route Reply (RRPL) messages are also transmitted over available channels to the source node, thus many alternative paths (and channels) are known by the source and the intermediate nodes. If any SU detects some PUs' activity over a channel that has been already used, it must instantaneously disable this channel for data transmission and notify its neighbours about the PU activity detection. To do so, some free or the CCC channel can be used.

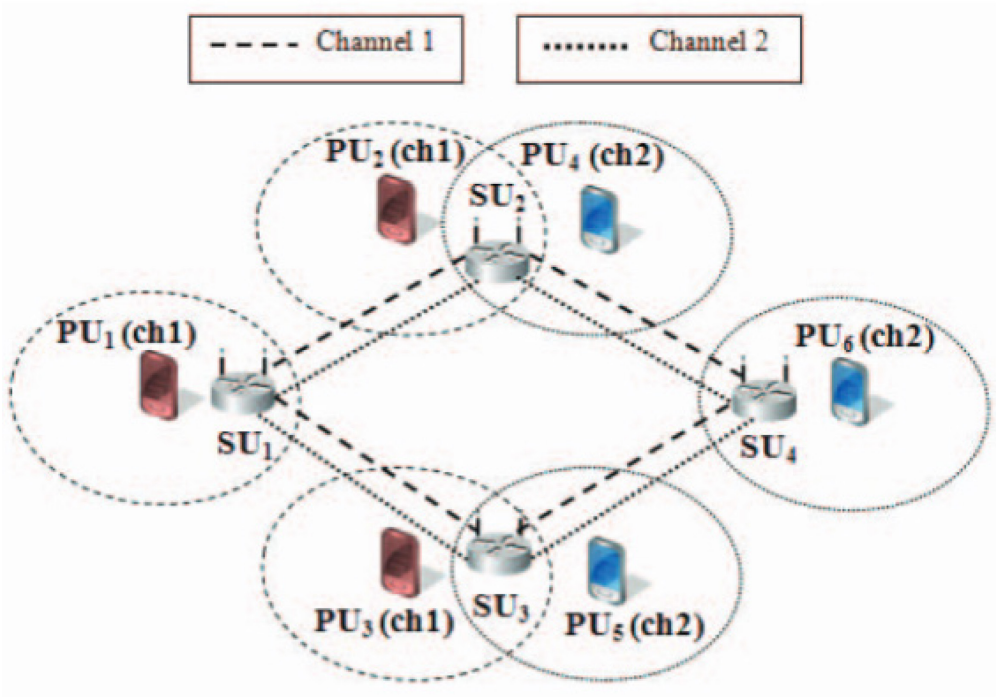



**Figure 4-4: Path and Channel Diversity [17].**

An anypath routing protocol for multi-hop CRAHNs is proposed in Ref. [18]. In an anypath routing scheme, a given node multicasts a packet to multiple candidate forwarders (i.e., the forwarding set of this node). This node's packet can be forwarded if anyone in the forwarding set has received the packet correctly. To avoid redundant transmissions, nodes in the forwarding set have different priorities. A node forwards the received packet only if no higher priority node has forwarded it. To apply an anypath routing scheme to a CRAHN, the multi-channel rendezvous problem (how two SUs tune to the same channel simultaneously) must be handled (for example, using CCC). The authors of Ref. [18] propose using the specific cost of the nodes, which is defined as the minimum number of transmissions required to deliver a packet successfully from source to destination. The calculation of the cost helps to determine whether the node should be included in the forwarding set or not. One can see that the cost is actually the function of link-availability, and thus the PU's activity. Since many candidate forwarders (with different priorities) are collected, the SU network is less vulnerable to PU activity. Moreover, the solution helps to solve the rendezvous problem of the multi-channel CRAHN without the CCC.

Following Ref. [11], we can compare in above-mentioned protocols proposed for CRAHNs (see Table 4-1).

**Table 4-1: CRAHN Routing Protocols Comparison.**

| Protocol | Metric | Type | CCC | Pros | Cons |
|---|---|---|---|---|---|
| Energy-aware routing protocol [13]. | Energy weight of the link. | Reactive or proactive | Yes | Avoids network partition. | Not good for large network. |
| Low latency and energy-based routing protocol [14]. | End-to-end residual energy and delay. | Reactive | No | Low latency. | Does not take PU's activity into account. |
| Energy-efficient routing protocol [15]. | Sleep and wake-up time. | Reactive | No | Data flow coordination. | Multipath scheme not considered. |

| Protocol | Metric | Type | CCC | Pros | Cons |
|---|---|---|---|---|---|
| Delay and energy-based spectrum aware reactive routing [16]. | Delay and path energy. | Reactive | No | Minimizes signalling overhead. Multipath transmission. | No efficient route maintenance mechanism. |
| Enhanced dual diversity cognitive ad hoc routing protocol [17]. | Path delay. | Reactive | No | Fast route recovery. Reduces interference from PUs. | High number of control messages. |
| Anypath routing protocol for multi-hop [18]. | Link availability | Reactive | No | Reacts on PU's activity without spectrum sensing. Reduces interference to PUs. | Higher transmission delay. |

Authors of Ref. [19] also compared three routing protocols for CRAHNs by simulation: Cognitive Ad Hoc On-demand Distance Vector (CAODV) [20], Spectrum Aware Routing Protocol for Cognitive Ad Hoc networks (SEARCH) [21], and Weighted Cumulative Estimation of Transmission Time (WCETT) [22].

CAODV is a reactive routing protocol based on the AODV protocol. It assumes that during the process of route establishment and packet delivery, the area of PU's activity is avoided, joint path and channel selection is applied to reduce the route cost, and multi-channel communication is provided to improve the overall performance.

SEARCH is a reactive protocol, which considers the path and the channel selection together to avoid the regions of the PU activities while forming a route. In the route setup phase, a RREQ is transmitted by the source on each channel that is not affected by the PU activity at its current location. It operates in two modes, which are Greedy Forwarding and PU Avoidance. Greedy geographic forwarding can decide which of the candidate forwarders of the RREQ should be chosen as the next hop to minimize the distance to the destination node. In the PU avoidance phase, the RREQ starts circumventing the affected region. Finally, the routes on the individual channels are combined at the destination by the joint channel-path optimization.

The WCETT protocol uses on-demand weighted cumulative expected metric to select the best path between source node and destination node. The commonly known ETX metric, used in typical ad hoc networks, can lead to a selection of highly loaded routes if the link packet loss rate is low. Thus, the Expected Transmission Time (ETT) metric was introduced to incorporate the throughput into its calculation. The WCETT protocol extends ETT to multi-channel networks [23]. It can help to select the paths in typical multi-channel CRAHN while CRs can switch the channels because of interference with PUs or jamming.

The performances of the three routing protocols were measured in [19] with respect to four metrics: packet delivery ratio, end-to-end delay, hop count, and routing overhead for the same environment in three different scenarios. It was concluded that SEARCH improved the PDR but still has lower performance in terms of end-to-end delay, hop count, and routing overhead compared to CAODV due to the fact that a lot of control packets are generated. It is also observed that CAODV is even better than WCETT protocol regarding PDR, end-to-end delay, hop count, and routing overhead. Thus, an unambiguous protocol selection depends on the CRAHN requirements, but the best results can be obtained if the regions of active PUs are avoided during route selection.

One of the interesting solutions on the routing mechanisms for CRAHNs is based on the artificial intelligence learning method known as the reinforcement learning, presented in Refs. [24] and [25]. The authors of Ref. [24] introduced Cognitive Radio Q-routing (CRQ-routing), which is based on the Q-learning method. CRQ-routing is a spectrum aware scheme that finds least-cost routes in CRNs taking

into account the dynamicity and unpredictability of the channel availability and channel quality. The CRQ-routing takes into account the PUs' and SUs' network performance by minimizing SUs' interference to PUs along a route without significantly jeopardizing SUs' network-wide performance. The CRQ-routing enables a SU to observe its local operating environment regularly and to subsequently learn an action selection policy through exploring various routes, and finally to choose routes with enhanced network performance (depending on definition: lower SUs' interference to PUs, lower SUs' end-to-end delay, lower SUs' packet loss rate, and higher SUs' throughput). The solution can be named cognitive, since it relies on the cognitive cycle. The Q-learning method allows to constantly learn based on the observation of the environment (i.e., PU activity, interference, …), update so called Q-function, then change the system state (i.e., change channel, route, …) to maximize the Q-function, and observe the environment again. If the indicated changes decreased the Q-function value, the other strategy is tried (i.e., another channel, route is selected…). Continuous observation of the CRAHN reactions on the changes leads to the system state that maximizes the Q-function and thus the network performance.

In Ref. [25], the authors propose a network architecture for CRAHNs that is based on the Q-learning methodology. Its main elements are shown in Figure 4-5. The Q-learning-based routing mechanisms require cross-layer interactions to learn the network current status and to enforce the system state change.

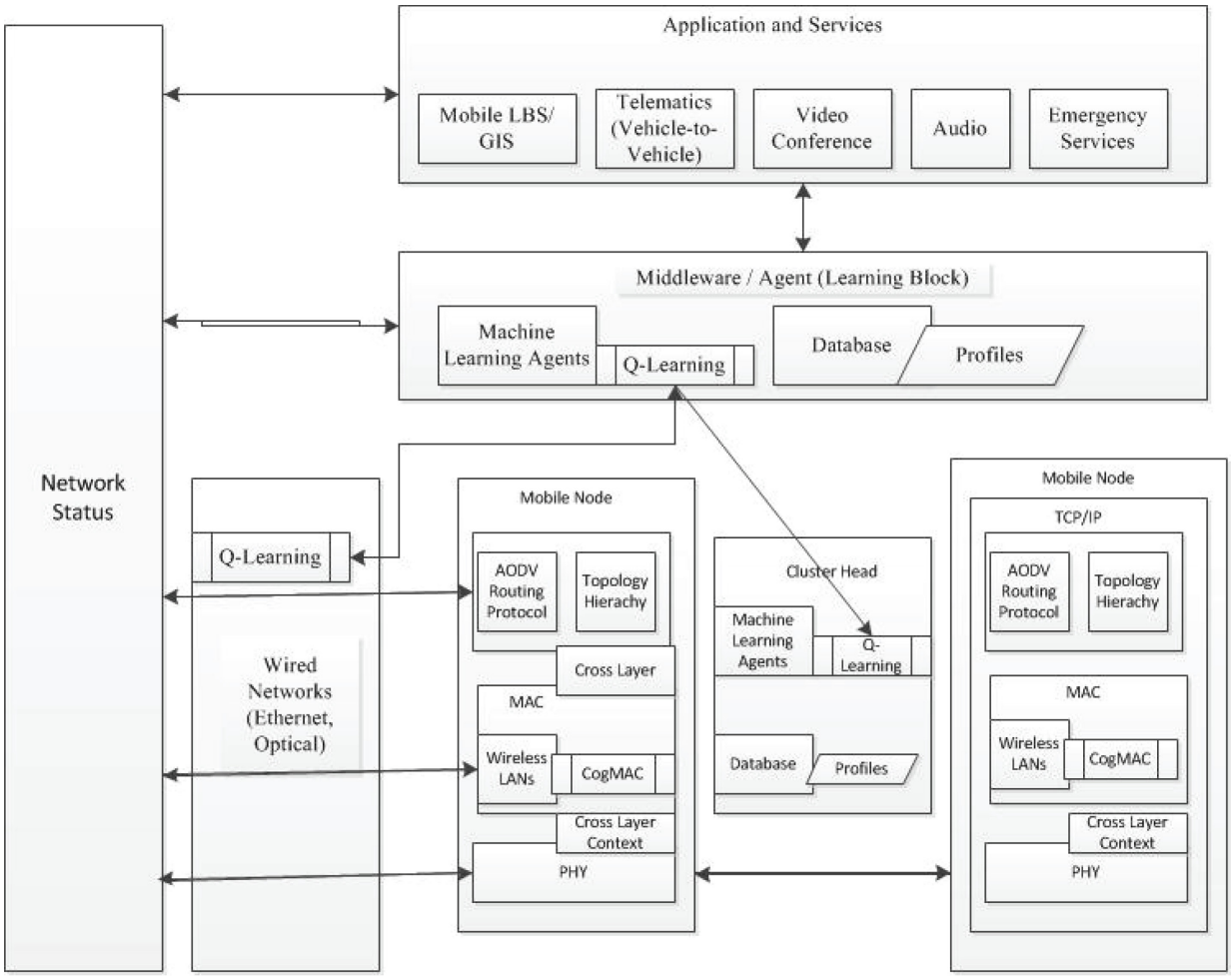



**Figure 4-5: CRAHN Network Architecture for Q-Learning Routing [25].**

Following Ref. [25], Figure 4-6 illustrates the cross-layer design approach, which explains the middleware layer QLS interaction with the other reconfigurable modules in the network layer. The applications inform the middleware management module about their end-to-end requirements. The Q-learning agent module receives the reward/penalty values and reconfigures the routing parameters to change the system state (change the routes, if required). Also, the routing protocol (AODV-based, in this case) supports the Q-learning module with the other information (i.e., route errors, end-to-end packet delay), thus the Q-learning module can take a decision on routing strategy to enhance a whole network performance. Thus, we can observe in a node operation a typical cognitive loop (denoted by arrows #5, #3 and #2).

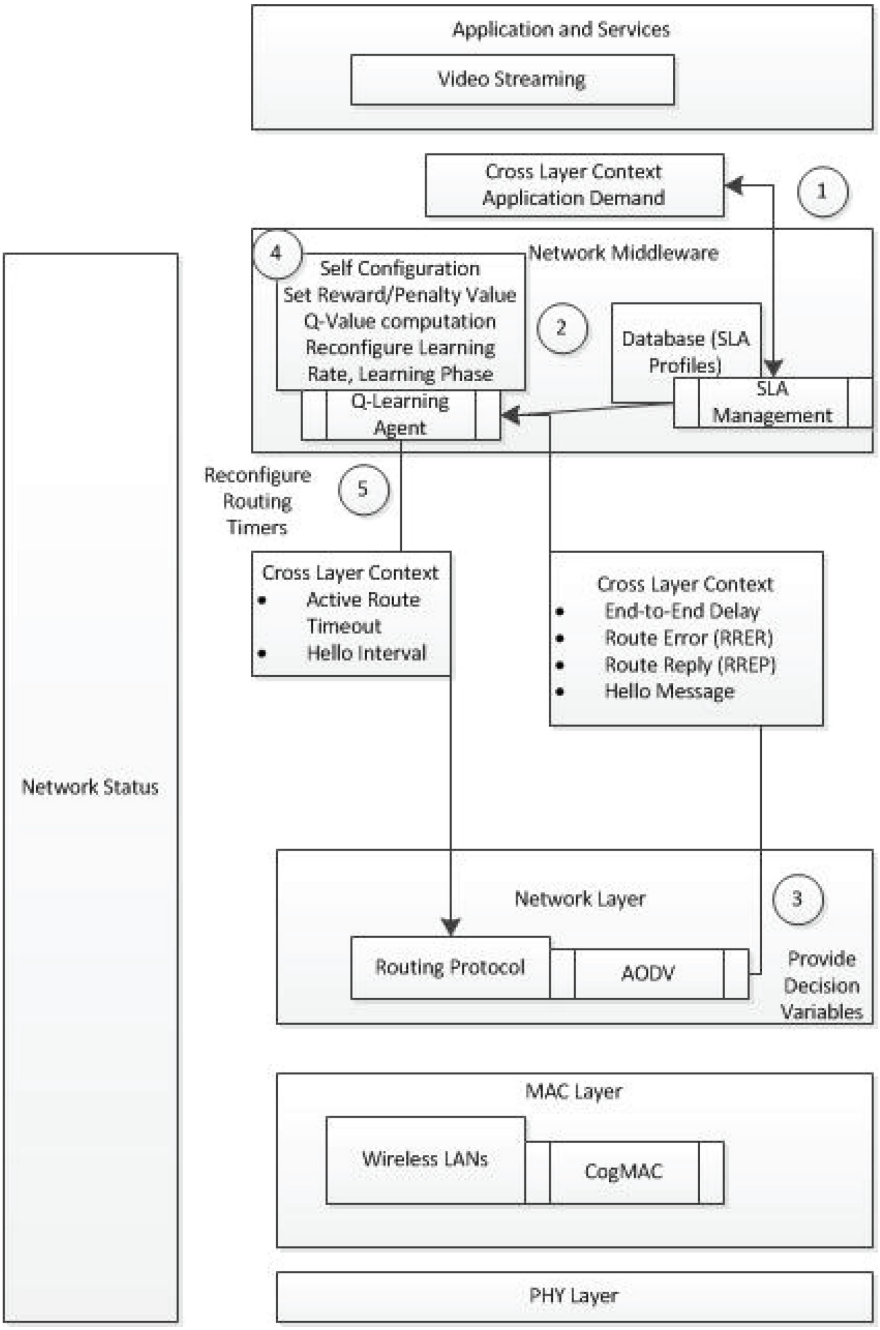



**Figure 4-6: The Cross-Layer Design in Q-Learning-Based CRN Node [25].**

Application of the artificial intelligence techniques in the CRAHNs seems to be promising because of its learning capability. The reinforcement learning mechanism is one of the methods used in some papers to support efficient routing strategies in fixed or slow changed network structures. Nevertheless, the military CRAHNs should consider similar techniques in the tactical domains. An additional effort is still needed to propose the solutions and to perform research on the artificial intelligence application in a military CRN.

### 4.1.2 Challenges and Recommendations for Routing in Military Cognitive Radio Networks

Considering the scenarios and vignettes presented in Chapter 3, as well as the recent activities in military SDR studies, we identified following challenges and recommendations for routing in military CRN:

- Routes have to be found quickly in a tactical CRAHN, even if the networks change (adapt) their waveform to cooperate with non-cognitive networks or with another cognitive network.
- Routing protocols in a tactical CRAHN should be able to cooperate with legacy routing protocols (non-cognitive networks) – route redistribution and fast convergence is needed.
- Routing protocols should be aware of frequent channel handoffs.
- Routing protocols should be equipped with a learning capability to calculate routing strategies and to exchange such strategies with other networks operating at the same region.
- Each node in a tactical CRAHN should be able to operate as a gateway to a fixed network; routing protocols must recognize multiple gateways.
- Routing protocols should be able to find routes avoiding regions where channels are frequently changed or jamming is identified.
- CRAHNs can be supported by information from outside the ad hoc network; routing protocols should use such information to build their metrics.
- Routing protocols should cooperate with a CRAHN hierarchical structure (with a cognitive clustering mechanism).
- Applications and transport protocols can influence route selection in a CRAHN, thus cross-layer information exchange is needed.
- As a tactical CRAHN can be based on handheld radios, routing protocols should also consider energy availability over the potential routes.

Routing solutions identified in Section 4.1.1 are dedicated to non-military ad hoc networks, where cognition is inbuilt in SU radios, which try to use channels dedicated to PU networks. Most of the solutions assume that routing protocols for CRAHNs have to construct complex metrics reflecting energy consumption of the nodes, level of interference measured in some region, spectrum availability, and PU activity. Thus, they are typically extensions of standard MANET routing protocols – mainly AODV. The challenges for routing in military CRN mentioned above essentially point out that all solutions can significantly support a tactical CRAHN, but they cannot be used in an initial form and without further investigations. Moreover, there are no unambiguous solutions for military CRs, and in consequence we cannot clearly propose one solution. Nevertheless, application of artificial intelligence techniques in CRAHNs produces promising results. The reinforcement learning mechanism is one of the methods used in some papers to support efficient routing strategies in fixed or slowly changing network structures. The military CRAHNs can consider similar techniques in the tactical domain, but additional effort is still needed.

## 4.2 COGNITIVE TOPOLOGY CONTROL

Topology Control (TC) is a technique used to model the network as a graph in order to reduce the cost of distributed algorithms, where the edges of the graph represent the connectivity. Especially in wireless ad hoc and sensor networks, TC is used to determine the required transmitting power, to lay the foundations for message routing, and to reduce interference between nodes. Accordingly, it can be seen as a middleware that connects routing and lower layers [26] and as a measure for saving energy.

There are two basic TC tasks, topology construction and topology maintenance. Topology construction is used to initially set up the graph, while topology maintenance is in charge of updating it. For the construction, the identification of available nodes is required, which is termed Neighbour Discovery (ND).

### 4.2.1 State of the Art

As energy conservation is especially important in Wireless Sensor Networks (WSN), several papers on TC have been published in this area (e.g., Refs. [27], [28], [29], [30], [31]). But, also regarding CRAHN, different aspects of TC have been analysed in literature, which take into account channel information or use decision-making algorithms, like fast neighbour discovery [32], [33], [34], jamming evasive neighbour discovery [35], or topology control for multi-channel CRAHN [36].

In Ref. [37], a survey is presented, which describes the challenges and solution proposals for TC regarding wireless ad hoc networks in general with an additional focus on WSN. A taxonomy of the topology control techniques found in literature is set up, which serves as a basis for the following analysis of TC for military CRAHN. It is depicted in Figure 4-7 and differentiates between homogeneous and non-homogeneous approaches.

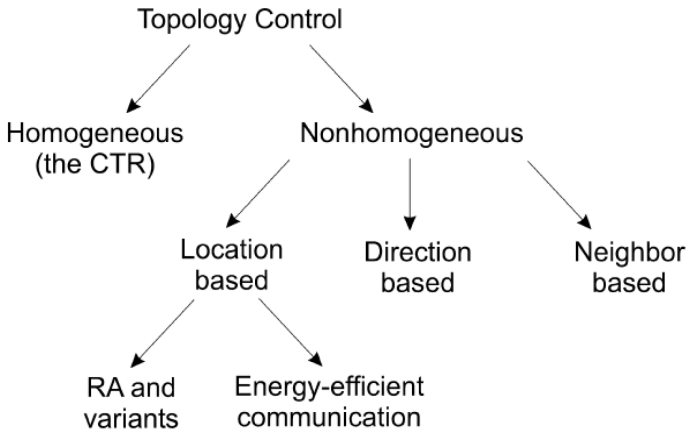



**Figure 4-7: A Taxonomy of Topology Control Techniques [37].**

In the homogeneous case, all nodes have the same transmitting range, which must be large enough to satisfy the needs of the network (Critical Transmitting Range, CTR). A minimal CTR leads to minimal energy consumption on a network-wide level; therefore, TC is, in addition to managing the network topology, a measure to optimize energy consumption of the whole network, although in this report, the focus is on topology management. Energy optimization on a single transmission is usually referred to as power control [37].

In the non-homogeneous case, nodes may have different transmitting ranges. Consequently, different approaches for computing the topology are proposed, based on the information that is used. In the neighbour-based approach, only the ID of the neighbour nodes is known, and the nodes are ordered to a criterion-like distance

or link quality. If a node does not know its own position but can estimate the relative direction to its neighbours, the direction-based approach will be used. If the position of each node is known, the location-based approach will be used. This information can be used in a centralized approach for determining Range Assignments (RA) or, in a distributed approach, to set up energy-efficient communication.

Several papers focus on ND in CRAHN. In Ref. [38], a distributed ND algorithm is proposed for nodes with one transmitter and multiple receivers. Ref. [32] describes a fast ND algorithm, which makes use of both control and data channels. Another fast ND algorithm is proposed in Ref. [33], which uses the Chinese reminder theorem and has few requirements. Ref. [34] proposes a fast ND algorithm specifically for heterogeneous multi-hop CRAHN. In Ref. [39], the results of ND regarding the ACROPOLIS Network of Excellence, which is supported by the European Commission's Framework Programme 7, are presented. A jamming evasive ND algorithm is presented in Ref. [35], which is asynchronous. Other asynchronous ND algorithms are proposed in Ref. [40] and Ref. [41].

Further papers analyse the effects on TC when using several channels. Ref. [42] proposes bi-channel-connectivity for robustness against PU activities. In Ref. [36], a TC solution for CRAHN using different channels for their links is presented. Cognitive small-cell networks under heterogeneous traffic are investigated in Ref. [43]. Ref. [44] presents both a centralized and a distributed TC algorithm for achieving robustness in multi-hop networks.

Furthermore, mathematical tools are used to optimize TC. In Ref. [45] and Ref. [46], game theory is used for decision making. As TC requires multi-objective optimization, Ref. [47] proposes a solution based on Ant Colony Optimization. Ref. [26] and Ref. [48] use link-availability prediction for providing more reliable topologies.

TC, specifically for clustered networks, is analysed in Ref. [49] and Ref. [50].

### 4.2.2 Challenges for Topology Control in Military Cognitive Radio Networks

As mentioned above, several challenges for TC in wireless ad hoc networks have been identified in Ref. [38]. Namely, these are energy conservation, limited bandwidth, unstructured and time-varying network topology, as well as low-quality communications. In addition to that, for wireless sensor networks, further challenges regarding operation in hostile environments, data processing, and scalability are identified, which may also be worthwhile considering for military application. Furthermore, the following challenges for the application of TC for CRAHN in a military context need to be analysed.

#### 4.2.2.1 Updates

In mobile networks, TC messages are usually sent regularly for keeping the topology up to date. In a military operation, the restraint of emissions is important for not being reconnoitred, e.g., during radio silence. Nevertheless, too few messages might lead to incomplete or outdated topology information. Therefore, a trade-off needs to be found. Furthermore, if keep-alive messages are used inside a network, it must be made sure that their restraint does not lead to problems.

#### 4.2.2.2 Resource Unavailability

In addition to the restraint of emissions, it can happen that messages are not correctly transmitted due to resource unavailability, e.g., caused by hostile jamming as described in the vignette in Section 3.3.1.2. In a CRAHN, this unavailability of resources will lead to a reaction, like a change of the transmission channel. Such a reaction may have an effect on routing or clustering and may lead to data loss until all changes are applied.

#### 4.2.2.3 Network Heterogeneity

It can be expected that for a military mission, there will be different kinds of radios for different tasks, which indicates the prevailing existence of heterogeneous networks. Therefore, topology control needs to support the interoperability of different nodes.

#### 4.2.2.4 Mobility

Especially in mobile situations, there is a risk of communication loss. But, as in military operations, the ability to communicate is essential, high QoS will be required for TC. Another aspect of mobility is that networks may split or merge, as described in the vignette in Section 3.2.2.2. The merging process requires that nodes need to be able to discover each other at any time. Nevertheless, being detected by hostile forces is undesirable.

#### 4.2.2.5 Security Aspects

Crucial information for many TC algorithms is the location of the network nodes. But, in the military environment, location information is usually classified. Therefore, security measures are required in order to handle this information.

### 4.2.3 Recommendations

In contrast to TC for non-cognitive networks, TC for military CRAHN must be able to consider frequency information for topology construction and maintenance. In addition to other parameters like link quality, transmission power, or inter-node distance, frequency availability should be taken into account when setting up the topology.

As frequency availability may be different for dispersed nodes of a network, information about the availability must be shared already during the ND process. Further information exchanged during the ND process must be analysed regarding its classification – e.g., node positions must not be forwarded unencrypted.

When information about all nodes in the network has been exchanged, the construction process needs to be terminated in order not to exhaust resources, which indicates the transition to Topology Maintenance. Discovery and termination must be achieved in a given time frame, which depends on the selected ND algorithm. Examples for algorithms with determined termination can be found in Ref. [32], Ref. [30], and Ref. [31].

#### 4.2.3.1 Updates

Updates are required when there are significant changes in in the topology. In addition to that, communication failures may be an indicator for the need to update topology information. Therefore, it is recommended to not only transmit updates in fixed regular intervals but to also observe the status of the network for changes (node movement, failures …) and to immediately update the topology information in case the observations show that this is beneficial.

#### 4.2.3.2 Mobility

Mobility usually leads to changes in the topology. Changes can, for example, be related to frequency availability, node positions, or to nodes joining or leaving the network. Especially in a highly mobile operation, topology changes constantly. The more a node moves, the higher is the need to update the topology information, as both position and frequency availability change.

#### 4.2.3.3 Data Processing

Data processing means aggregation and compression of sensor data for the exchange with other nodes. In CRAHN, this is mainly important for sensing data, but can also be used for any other control information. For example, in Ref. [51], a method named “hard combining” is described, which aggregates one sensing result into one information bit.

#### 4.2.3.4 Scalability

It can be expected that modern networks are scalable up to their maximum size. In the military domain, network sizes are usually related to the military unit size. Therefore, networks should be optimized for these sizes in operational scenarios.

#### 4.2.3.5 Frequency Agility

While TC is usually concerned with a limited set of frequencies on a link (in most cases one), TC for CRAHN must regard all available frequencies on the link. The selection of a frequency for a link must be in line with the selected clustering algorithm. In addition to that, TC must be informed about changes conducted by the decision-making entity on time.

When preparing the move to a new frequency, most important is that this frequency is detected to be unused at all nodes. Any unused frequency can be selected dynamically, as long as it is negotiated between all devices.

Nevertheless, for ND frequencies cannot be negotiated. Either there is a fixed frequency, which, in the case of interference, will impede discovery, or the frequency may change, which will lead to a delayed discovery. The more frequencies are possible for ND, the longer the ND process may take. Therefore, there must be a trade-off between agility and discovery time.

Other solutions might be multi-channel radios, full-duplex radios, or radios that support broadband network discovery, where the occupied segments are analysed for discovering other nodes.

#### 4.2.3.6 Network Heterogeneity

In a heterogeneous network, different technologies can be used, but require the formation of different clusters or subnets. Gateway nodes are required, that can connect the different technologies, thus facilitating interoperability. Nodes in the same cluster need to be able to detect and to communicate with each other. Nodes with different technologies need gateway nodes to communicate with each other. An example for this is described in the vignette in Section 3.2.2.2.

#### 4.2.3.7 Energy Conservation

For mobile and deployable networks, energy conservation is important. There are different energy conservation techniques in a radio, but most important is the reduction of transmission power. TC is used to set up routes between the nodes and, therefore, helps to reduce transmission power. TC for CRAHN adds a further option for this by allowing for frequency changes. The lower the frequency, the higher is the transmission range. As the typical military frequency bands (HF, VHF, and UHF) are rather narrow, it needs to be tested if using lower frequencies effectively has advantages.

#### 4.2.3.8 Limited or Unavailable Resources

Limited or unavailable resources usually lead to low-quality communications. In order to avoid degradation of user traffic performance, it is necessary to keep control traffic at a reasonable rate. If supported by the

waveform, different waveform modes using lower bandwidth or the switch to a different frequency can be a first approach to keep the ability to communicate.

In addition to that, it is important that TC cooperates with the decision-making entity for being informed about the changes early. TC must further be informed how other nodes can be reached. For that, cross-layer effects need to be taken into account.

Furthermore, TC must be stable enough to cope with radio silence. This means that, even though nodes may move while no TC messages are exchanged, communication must be possible when radio silence is over. In many cases, when radio silence is over, there is a high need for communication, so that the network must not be flooded with TC updates more than necessary.

## 4.3 COGNITIVE DATA TRANSPORT

### 4.3.1 State of the Art

CRNs require efficient end-to-end data transport control algorithms. Standard Transport Control Protocol (TCP) and User Datagram Protocol (UDP) are not designed for wireless networks. Some modifications proposed in literature can be used in typical ad hoc networks [52], but they are not efficient enough for CRNs. Transport layer protocols have limited knowledge of the network conditions in between the end nodes. Standard TCP is responsible for congestion control and data transmission rate adaptation of the source nodes to the receiving possibility of the destination nodes. It was designed for typical wide area fixed networks, where congestion comes mainly from intermediate nodes overloading. The modifications for wireless ad hoc networks provide the mechanisms that are able to identify a source of data segments loss: node overloading or wireless link characteristics (data segments loss because of signal fading and interferences or node mobility).

CRNs pose new challenges regarding data transmission control. Data segments can also be lost or delayed because of spectrum mobility (handoff) and spectrum sensing. TCP will react on such situation by decreasing the transmission window. Nodes could inform the source that it is a transitory state caused by the cognitive entities. Moreover, intermediate nodes that are particularly engaged in cognitive procedures can also work as something like proxy nodes for TCP transmissions. In CRNs the large bandwidth variations can appear in some segments of the network according to PUs activity. Thus, the network can significantly increase or decrease the throughput. TCP cannot adapt its transmission rate to such events in an effective way, especially in case of high data segment Round Trip Time (RTT). Thus, new bandwidth estimation methods have to be elaborated, that can use CRs characteristics. Some example proposals for bandwidth estimation can be found in Ref. [53] and Ref. [54].

Cognitive data transport solutions for military CRNs should propose updated or completely new connection management and congestion control mechanisms. They should take into account at least information on spectrum sensing, spectrum change, route failure, and mobility prediction. One of the example transport protocol for CRAHNs is presented in [55] – the authors named it TCP CRAHN. It defines the following stages: connection establishment, normal, spectrum sensing, spectrum change, mobility predicted, and route failure. Each of these states reflects the cognitive network behaviour and its influence on the node that has to control the data transmission. Similar assumptions are taken in TCP Friendly Rate Control for Cognitive Radio (TFRC-CR) [56], where the following states are proposed: normal, PU detected, PU exit, slow start, resume, and paused. Both TCP CRAHN and TFRC-CR can be taken into account during cognitive data transport mechanism elaboration, but there are still many challenges in CRAHNs that must be addressed. First of all, the solutions should be compatible with standard TCP and UDP protocols. The data transport connections can be initiated in fixed networks, where TCP or UDP is a standard protocol. Secondly, control messages should be reliably delivered (TFRC-CR and TCP CRAHN provide many control messages, but they can be discarded even if sensing or spectrum mobility is performed in some intermediate nodes).

### 4.3.2 Cognitive Transmission Control for Military Cognitive Radio Ad Hoc Networks

Transmission control protocols act in the transport layer of the OSI model. Their main role is to support packets transmission between the source and destination nodes, while the network cannot guarantee reliable end-to-end communication. TCP is one of the typical protocols located in transport layer [57]. It is used for congestion control and congestion avoidance. Its common implementations are developed to react on packet losses caused by congestion in the intermediate nodes and buffer overflow in the end nodes. Additionally one can find a set of solutions for wireless networks, where packets can be lost due to bad links (because of interference, signal strength fluctuation) or node mobility [58]. Differentiation of the source of the packet loss can be helpful for transmission window adjusting. In CRAHNS, we have additional reasons to build the knowledge at the transport layer about the decision taken by the cognitive entities at the PHY/MAC and other layers. For example, the decision on a channel switch can help to stop the transmission by the end nodes to avoid buffer overflow in the intermediate nodes. It can also help to adjust the congestion window after such an event.

Taking into account military CRAHNs' specific requirements, the cognitive transport protocol has to be equipped with the mechanisms, which allow:

- Identification of the intentional breaks in data transmission at the intermediate nodes caused by the sensing procedures;
- Identification of channel (spectrum) handoff at the intermediate nodes;
- Collection of link quality measures (connected with channel identification) at the path from source to destination;
- Prediction of intermediate node mobility; and
- Explicit congestion, buffer overflow and route failure notification.

Figure 4-8 presents a sample multi-hop CRAHN, where the packet transmission has to be controlled between a source (CR1-S) and a destination (CR6-D) node. The transport protocol has to be supported by cognition powered by the information listed above. Unfortunately, most of the sources of the information are in the path between the CR1-S and CR6-D. The links between the pairs of nodes can use different channels (c1, c2, etc.) which can be switched by at least one node in the path. Switching of the channels, cogitative entities located at the network layer or standard routing protocol mechanisms can lead to the route change between the CR1-S and CR6-D. The source and the destination nodes have to learn and build knowledge about the conditions of the transmission and, based on it, they have to decide on the sizes of the transmission or advertised windows, selective acknowledgment, and other transmission parameters.

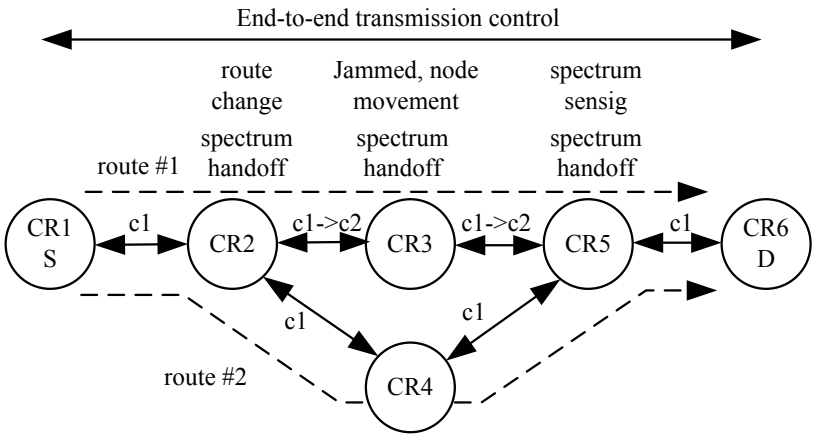



**Figure 4-8: End-to-End Transmission Control in a CRAHN.**

On the other hand, military CRAHNs operate under the umbrella of the set of policies imposing rules and limitations on traffic handling, quality of service (priorities, pre-emptions, and time characteristics), and security, but also on the DSA functionality. This is another source of information that the source and destination can use during transmission control. Moreover, military CRs can often gather information from outside of the CRAHN (i.e., using multi-interface radios/gateways). All of this information can support the transmission mechanisms in decision on the effective end-to-end communication.

We assume that the military CRAHN's nodes have to be able to communicate both with other nodes in the CRAHN and the nodes outside the CRAHN. Thus, they have to be equipped with standard TCP, updated by the cognitive cycle and used during the communication in the area of the CRAHN. The Military TCP (M-TCP) must hold backward compatibility with standard TCP (or its specific implementation). To be supplied by information, the M-TCP Cognitive Engine (M-TCP-CE) has to interact with both native TCP and other layers as shown in Figure 4-9.

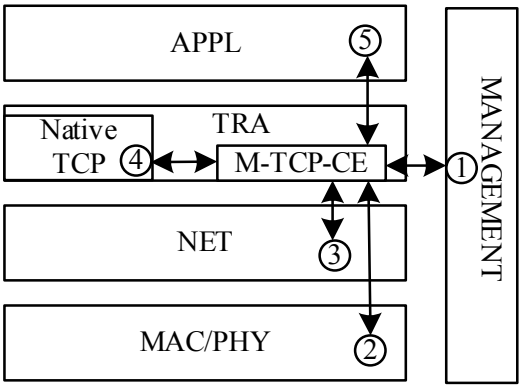



**Figure 4-9: M-TCP-CE Interactions.**

After the analysis of the current transmission control solutions, many required features can be found in TCP CRAHN proposed in [55], TCP Collaborative Bottleneck Analysis (TCP CoBA) proposed in [59] and some further TCP improvements in [60]. The proposal of the M-TCP-CE functional structure is shown in Figure 4-10.

The cognitive cycle shown on the left side of Figure 4-10 can be represented by the M-TCP-CE state diagram (right side of Figure 4-10). In order to perform the decision on new TCP parameters that have to be updated during transmission as well as globally in the node, the Cognitive Engine (CE) has to observe many metrics. Based on them, the current state of the network is learned. The M-TCP-CE state diagram is composed of eight states. State #1 is responsible for collecting the initial parameters of the transmission path. It is based on standard TCP Three Way Handshake (3WH), updated by a set of options, modified (added) by the intermediate nodes, and used by the source and destination nodes. Similar to [55], the options are carried by the TCP SYN messages (sent in opposite directions). There are the following initial parameters collected by the end nodes (supplied by each node in the path): node IDs (IP address), timestamps, and time dependencies concerning sensing operation (moments of sensing, sensing duration). The SYN messages allow the intermediate nodes to register the flow IDs and the IDs of the end nodes to get the possibility of sending direct notifications about relevant metrics. Moreover, the nodes in the path are informed about the flow requirements on the bandwidth and priority supplied by the end applications (APPL req). This information can be used by the NET queuing rules and routing, and by the MAC/PHY cognitive engines to support channel management in the part of the network where the current transmission is handled (for example, the selection of stable channels with high data rate waveforms or channels with low bandwidth and low probability of signal interception – potential usability of this information is wired, but the paper does not define the solutions for lower layers). In the current state of the M-TCP-CE concept, it is assumed that both

source and destination nodes have to agree on using cognitive functionalities. If one of them is not able to support the M-TCP-CE (i.e., the connection is terminated outside the cognitive network), both nodes use their standard TCP implementation.

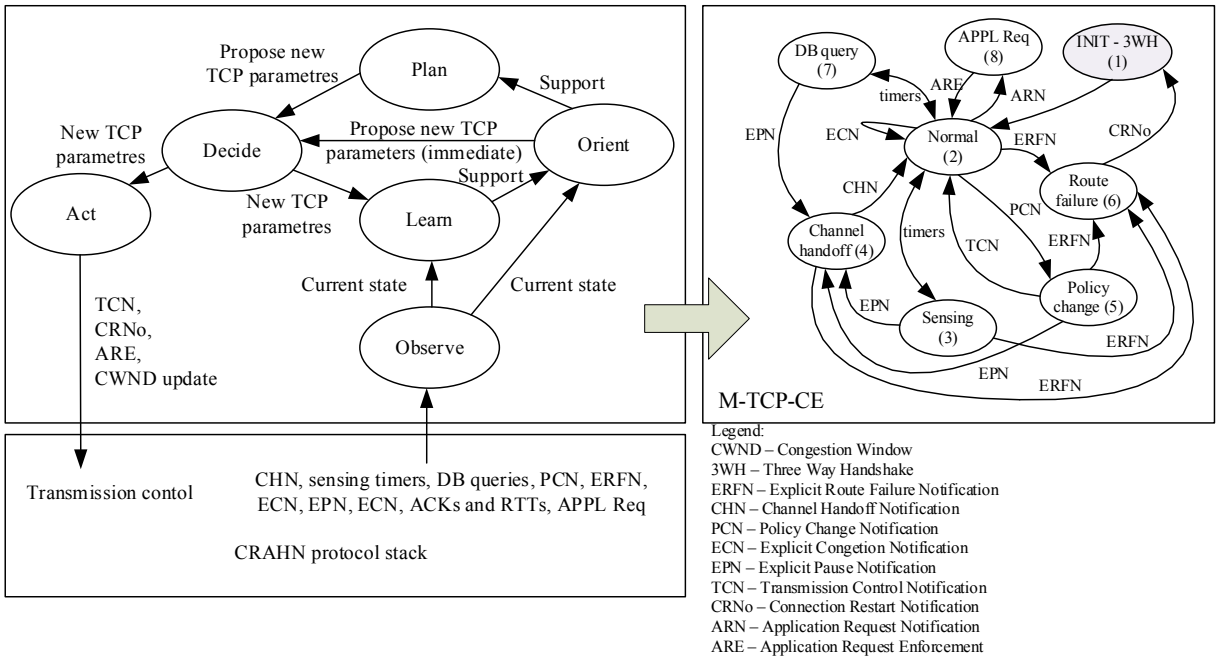



**Figure 4-10: M-TCP-CE Internal Structure and State Diagram.**

After completion of the initial parameters, the M-TCP-CE moves to the "Normal" state (state #2), where the TCP performs its typical functions (depending on the implementation) [55]. Now, the state can be changed as a reaction on the observed metrics. The "Sensing" state can be reached in starting time of the sensing procedure run in each intermediate node (identified during initial state). Initially, it is assumed that sensing procedures performed at the MAC/PHY layers require breaking the transmission. If other sensing implications into the transmission control are identified (depending on military waveform solutions), they have to be taken into account in the "Sensing" state. Transmission brakes typically lead to the RTT and Packet Loss Ratio (PLR) increase. If the source node does not stop transmission for some time, the intermediate nodes can reject the packets because of buffer overflows. Thus, it is reasonable to enforce TCP in a source node (Orient->Decide->Act) to stop the transmission before the sensing events and recreate it later with the same Congestion WiNDow (CWND) size. If the waveforms are able to adjust the sensing time, a source node can send requests to intermediate nodes to reduce this time, depending on the application's requirement (required higher bandwidth learned in "APPL req" state). One of the methods used to regulate the sensing time and used to increase transmission efficiency can be found in Ref. [55], but it should be verified according to the sensing method used in specific military waveforms.

During this state, the end nodes can receive the information (in CCC) about channel handoff (EPN – Explicate Pause Notification), what enforces moving to "Channel handoff" state. The EPN can be generated by each intermediate node. Source and destination nodes have to suspend transmission until the new links are ready. From Ref. [55] and Ref. [61], we can learn that standard TCP cannot effectively track the changes of an available bandwidth in a path between source and destination. Such situation can be especially noticeable in tactical CRAHNs, where the accessible channels can be jammed, subjected to interference, and locally highly loaded. Additionally, the military CRs can switch transmission (waveform) between HDR (High Data Rate) and LDR (Low Data Rate), including LPI/LPD (Low Probability of Interception / Low Probability of Detection) modes. Informing the source and destination node's transmission control mechanisms about the

changes (at least, on available bandwidth) significantly accelerates CWND adjustment. On the other hand, the end nodes can influence the channel selection by sending the notification about the applications requirements (learned in "APPL req" state). For example, the highest priority streams would require the most stable channels in the path. The indicator of channel stability can be the channel accessibility rate. Channels that are often released because of interference, jamming, or simply occupation by other networks sharing the same spectrum can be indicated as less stable. If the new channel is selected, the intermediate node has to inform the end nodes on the new channel (link) characteristics (available bandwidth, links quality, channel stability), which can be used to set up an appropriate CWND size, timeouts, and maximum segment sizes (MSS). It sends the Channel Handoff Notification (CHN) message. The M-TCP-CE reactivates an updated CWND (taking into account new conditions) and moves to the "normal" state.

In case of military networks, the channel handoff can also be initiated by other sources than spectrum sensing performed by radios. It has been assumed that the CRAHN is able to periodically check the external database (DB), which is supplied by the prevailing information about the geographical channel usage or channel handoff requirements. Being in a "DB query" state (state #7), the end nodes' transmissions can be explicitly paused (*via* an EPN) if new channels must be allocated by the network. After these events, the mechanism moves to "Channel handoff" state (state #4) and then (after receiving a CHN) to "normal" state (state #1). A newly available set of channels can also be notified and allocated by the tactical radio network management system *via* distribution of updated policies. After a Policy Change Notification (PCN) message is received from the management system, the "Policy change" state (state #5) is reached. The updated policy can concern channel handoff, which implicates EPN and moving to "Channel handoff" state (state #4), but also new transmission rules, i.e., new priorities, acceptable bandwidth requirements, receding buffer size updating, and others. In case these rules need to be applied, a Transmission Control Notification (TCN) is carried to TCP for updating its standard parameters.

Modification of the end-to-end communication parameters in certain states can lead to route failures. Thus, the intermediate nodes should send Explicit Route Failure Notifications (ERFN) to the end nodes if the route has to be reactivated. In some cases, the TCP connections should also be re-established if the end nodes receive the Connection Restart Notification (CRN) message, generated by the intermediate nodes that cannot retransmit buffered packets because of route failures.

### 4.3.3 Cognitive Transmission Control and Other Layers' Interactions

The cognitive transmission control mechanisms rely on metrics coming from all layers. In order to support the TCP, the notifications generated by intermediate nodes have to reach the source and destination nodes. Additionally, it can be assumed that M-TCP-CE is a part of a radio's cognitive engine, where other layers are also equipped with their own cognitive cycle mechanisms. Additionally, military tactical radio networks must be supported by the management system that is able to deliver a set of initial network parameters and policies before a mission, update them during the mission and collect the learned values after the mission. Generally speaking, in a fully cognitive network, the management system should also be based on a cognitive cycle, allowing learning and updating policies. Figure 4-11 shows a composition of cognitive entities responsible for supporting the protocols stack. All of them are part of the radio cognitive engine. We can distinguish separate cognitive cycles (cognitive engines) for MAC/PHY (Dynamic Spectrum Access/Management – DSA/DSM), NET (Cognitive routing) and TRANSPORT (Cognitive transmission control) layers. Each cognitive cycle is oriented to optimize functions of the layer for which it is responsible. The rest can be considered as an external environment that should be observed.

The main function of the DSA/DSM cognitive cycle is effective spectrum utilization and, what is important for military radios, automatic spectrum management (sharing) in multilateral operations. While a cognitive routing is responsible for finding the paths to destinations' nodes, taking into account (learn) many metrics connected with the channel handoffs (i.e., channel selection stability), link quality, path bandwidth, application requirements, and routing rules from the policies. As pointed out in Figure 4-10, many metrics

and messages are observed to support particular states. The main goal of the cognitive transmission control mechanisms is goodput value maximization by acceleration of a transmission window scaling. Nevertheless, decisions taken by a particular cognitive cycle influence the actions performed by other cycles.

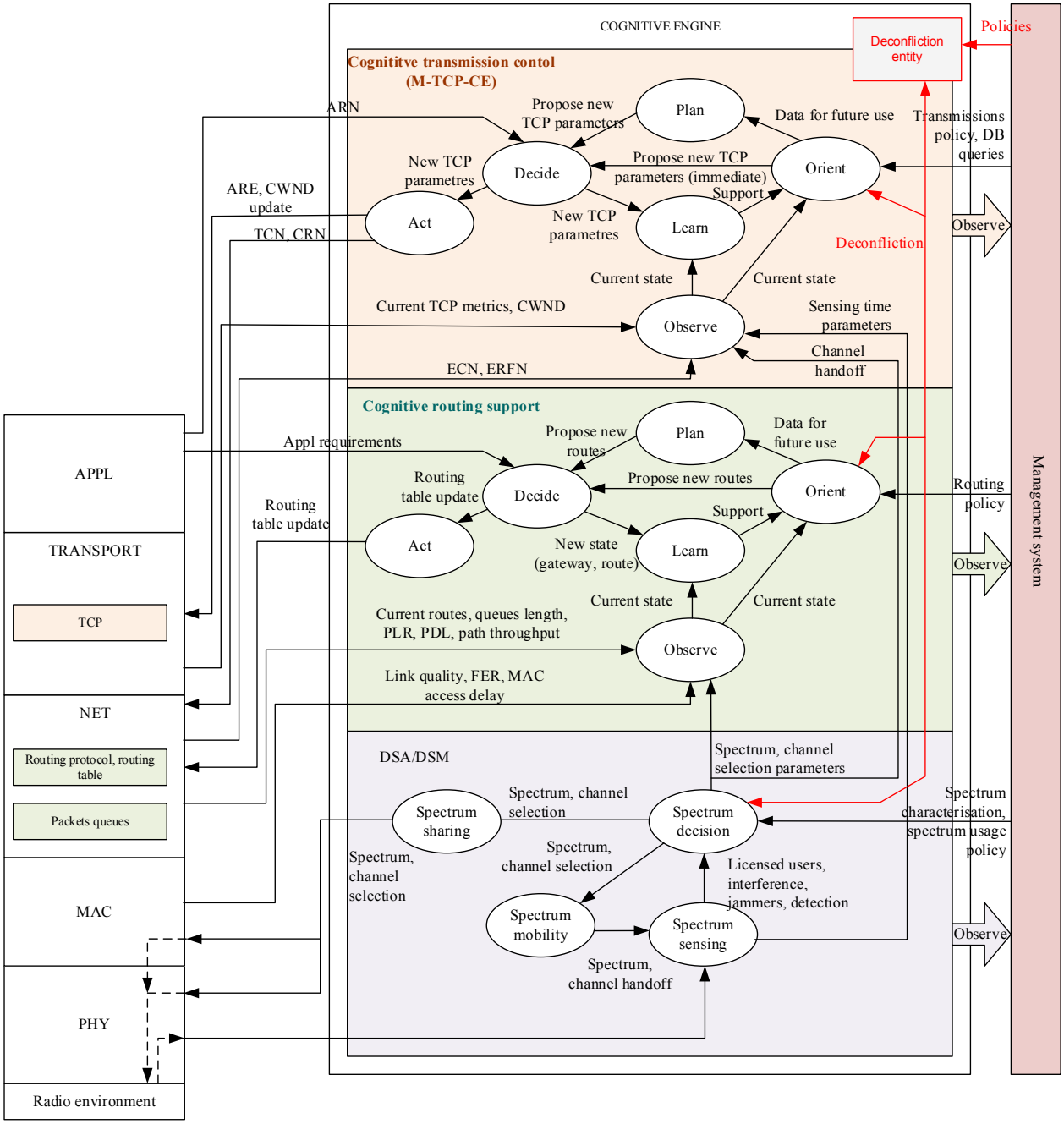



**Figure 4-11: M-TCP-CE as a Part of a Radio Cognitive Engine.**

Let us focus on the MC-TCP-CE interaction with other CEs. The M-TCP-CE exploits the DSA/DSM entities by receiving the sensing timing parameters and channel handoff information. The cognitive routing procedure requires the same information. The M-TCP-CE can decide to update the CWNDs of an active TCP flow which uses the current routes, but at the same time the cognitive routing entities can decide on changing the route because of their local preferences. Thus, deconfliction is required before both CEs will

take their decisions – a common decision should be prepared. To do so, a common Deconfliction Entity (DE) should be used that collects all information from all CEs that should be checked during orientation and before taking the decisions. The DE should be supported by the management system, from which it receives updated policies and higher-level guidance for deconflicting cognitive events.

## 4.4 COGNITIVE CLUSTERING

### 4.4.1 State of the Art

Clustering is a topology management mechanism, which aims to provide network optimization and operational enhancement by organizing network nodes into logical groups. Most importantly, clustering aims to provide network scalability and stability. The optimization goal for clustering can be energy efficiency, spectrum usage efficiency, fluent cooperation between related nodes and many others. Clustering is a well-studied process in traditional networking concepts.

Clustering algorithms can be categorized in at least three ways:

1) Application platforms, i.e., types of nodes that are concerned. Typical examples would be sensor platforms, handheld communication devices, and vehicle-mounted devices. They have not only different energy reserves but also different traffic patterns. These and other dissimilarities affect the objectives and methods of clustering, and, in fact, whether the clustering is needed at all.
2) Objective of the clustering, i.e., reason why clustering is being done. Several reasons can be identified in some/many cases. These are discussed more below.
3) Clustering algorithm type. Basically, for cluster formation, two processes need to be defined: the cluster head selection and the way the member nodes select and join a cluster. In addition, there often needs to be methods for managing the clustering in more dynamic networks. Dynamics may either involve node mobility or e.g., variation in the channel availability, as is the case with CRNs.

#### 4.4.1.1 Platform Types

In this study, we limit our discussion to consider only wireless networks operated for human-to-human communication needs. We do not consider e.g., sensor networks and clustering methods specifically designed for them (for those, see, for example, Ref. [62], [63], [64], and many others). That being said, we may still need to consider energy efficiency as one of the objectives of clustering, at least when handheld devices are considered.

Furthermore, we consider only ad hoc networks, where there is no preselected/preset structure in the network and no network master can control the whole network (at least, at the start of the network operation). The very specific problem that we will deal with is related to the cognitive aspect of the ad hoc network. This affects both the objectives for clustering, as well as the clustering methods. For purely ad hoc network solutions, one can see, for example, Ref. [65].

#### 4.4.1.2 Objectives for Clustering

In the following, objectives for clustering in general cases are listed, although only ad hoc networks are concerned.

##### *4.4.1.2.1 Dominating Set-Based (DS-Based)*

Clustering endeavours to determine the DS for a MANET, where the number of mobile nodes participating in route search or routing table maintenance can be reduced, as their function becomes ‘familiar’ and only

DS mobile nodes are required to perform them (e.g., Ref. [66]). This is therefore used for making the routing functionality in the network as simple as possible, which should reduce the required signalling traffic in the network. Actually, one could think that this should be done in cooperation between routing layer and clustering. One could perform first e.g., the OLSR route search and form the clusters based on the found structure. In the case of OLSR, the cluster heads would be a selected set of the MPR nodes. This would need some experimenting and possibly some research.

#### *4.4.1.2.2 Flooding-Based Clustering*

Flooding-based clustering addresses MANETs that are characterized by scanned bandwidth, radio interference issues and no fixed infrastructure, circumventing the need for more effective (specified) techniques requiring complex protocols. Flooding, as the term suggests, is the dissemination of information (overall and without explicit direction) to reach all the nodes in the network. Each node redistributes all of the information to all of its neighbours until there is inundation of the entire network without any computation requirements or maintenance of routing tables, thus avoiding network delay. The role of clusters in the flooding could be that only Cluster Heads (CHs) flood the packets to their own clusters, while cluster members do not flood. Therefore, this limits the number of transmissions in the flooding process, making it faster and more energy efficient.

#### *4.4.1.2.3 Low-Maintenance Clustering*

Low-maintenance clustering schemes aim to reduce cluster maintenance cost and 'greedy' resource consumption through the provision of stable cluster architecture for upper-layer protocols. This is achieved through prevention of re-clustering requirements and/or minimization of explicit control messages for clustering. The general aim is to make the control messaging in the networks simpler and more efficient. Examples of low-maintenance clustering are the following:

- Lowest-Identifier Clustering algorithm (LIC), identifier-based clustering [67];
- Highest-Degree, connectivity-based clustering [67]; and
- Least Cluster Change (LCC) [68].

#### *4.4.1.2.4 Mobility-Aware Clustering*

Mobility-aware clustering will group mobile nodes with similar characteristics together according to their speed of movement – the chief reason for network topology changes. Similarly paced nodes are gathered into the same cluster allowing a tightening of intra-cluster links with corresponding stability realized in the presence of mobile nodes in motion. By keeping the nodes with similar mobility in one cluster, the cluster remains more stable and the required signalling messaging is reduced. Examples of mobility-aware clustering are the following:

- Mobility-Based Metric for Clustering – MOBIC [69]; and
- Mobility-Based d-hop Clustering Algorithm [70].

#### *4.4.1.2.5 Energy-Efficient Clustering*

Energy-efficient clustering manages battery energy of mobile nodes more sensitively in a MANET. Fine calibration of energy requirements through elimination of redundant energy consumption by mobile nodes, or balance among different mobile nodes can greatly impact the projected network lifetime. Low energy use is due to low number of bits sent or lower energy/power used for transmissions. This aspect mainly concerns low-power devices, such as sensors and their networks. Examples of energy-efficient clustering are the following:

- Power-aware connected dominant set [71];
- Hybrid Energy-Efficient Distributed clustering (HEED) [72]; and
- Stable Cluster Algorithm (SCA) [73].

#### *4.4.1.2.6 Load-Balancing Clustering*

Load-balancing clustering schemes attempt an even distribution of mobile nodes to each cluster to create similarly sized clusters, thus sharing the load on the network by this arrangement. This has the benefit of extending the lifetime of the network as a whole and implementing fairness among nodes. Examples of load-balancing clustering are the following:

- Degree-Load-Balancing Clustering (DLBC) [74]; and
- Adaptive Cluster Load Balance Method [75].

#### *4.4.1.2.7 Combined-Metrics-Based Clustering*

Clustering considers multiple metrics in a cluster configuration, with particular interest in cluster head decisions, weighting the parameters according to their attributes pertinent to a particular application requirement, allowing an adaptive response as justified by the needs. With the consideration of more parameters that might include mobility speed, node degree, cluster size or battery energy, cluster heads can be better selected without bias given to mobile nodes with specific attributes [76], [77], [78]. Examples of combined-metrics-based clustering are the following:

- Weighted Clustering Algorithm (WCA) [79];
- Entropy-Based Weighted Clustering Algorithm [80]; and
- Weight-Based Clustering Algorithm (WBCA) [81].

### 4.4.1.3 Clustering Algorithm Types

Partly overlapping with the above classification and lists of clustering methods, Ref. [65] provides the following classification on algorithms (Table 4-2). References to the actual algorithms can be found in this review paper.

**Table 4-2: Classification on Clustering Algorithms.**

| Type | Algorithm |
|---|---|
| Identifier-Based Clustering | Lowest ID Clustering Algorithm. |
| | Max-Min D-Cluster Formation Algorithm. |
| Connectivity-Based Clustering | Highest Connectivity Clustering Algorithm (HCC). |
| | K-Hop Connectivity ID Clustering Algorithm. |
| | Adaptive Cluster Load Balance Method. |
| | Adaptive Multi-Hop Clustering. |
| Mobility-Aware Clustering | Mobility-Based D-Hop Clustering Algorithm. |
| | Mobility-Based Metric for Clustering |
| | Mobility-Based Framework for Adaptive Clustering. |

| Type | Algorithm |
|---|---|
| Low Cost of Maintenance Clustering | Least Cluster Change Algorithm. |
| | Adaptive Clustering for Mobile Wireless Network. |
| | 3-Hop Between Adjacent Cluster Heads. |
| | Passive Clustering. |
| Power-Aware Clustering | Load-Balancing Clustering (LBC). |
| | Power-Aware Connected Dominant Set. |
| | Clustering for Energy Conservation. |
| Combined Weight-Based Clustering | Weighted Clustering Algorithm. |
| | Entropy-Based Weighted Clustering Algorithm. |
| | Vote-Based Clustering Algorithm. |
| | Weight-Based Adaptive Clustering Algorithm (WBACA). |
| | Connectivity-, Energy- And Mobility-Driven Weighted Clustering Algorithm (CEMCA). |

#### 4.4.1.4 Further Classifications for Clustering

Clustering metrics, as listed by Ref. [82], are channel availability, geographical location, signal strength / channel quality, and node degree. In addition to these metrics, intra-cluster distance is mentioned; clustering may aim for single hops or multiple hops within certain clusters.

The illustration below (Figure 4-12) summarizes the classifications provided by Ref. [82].

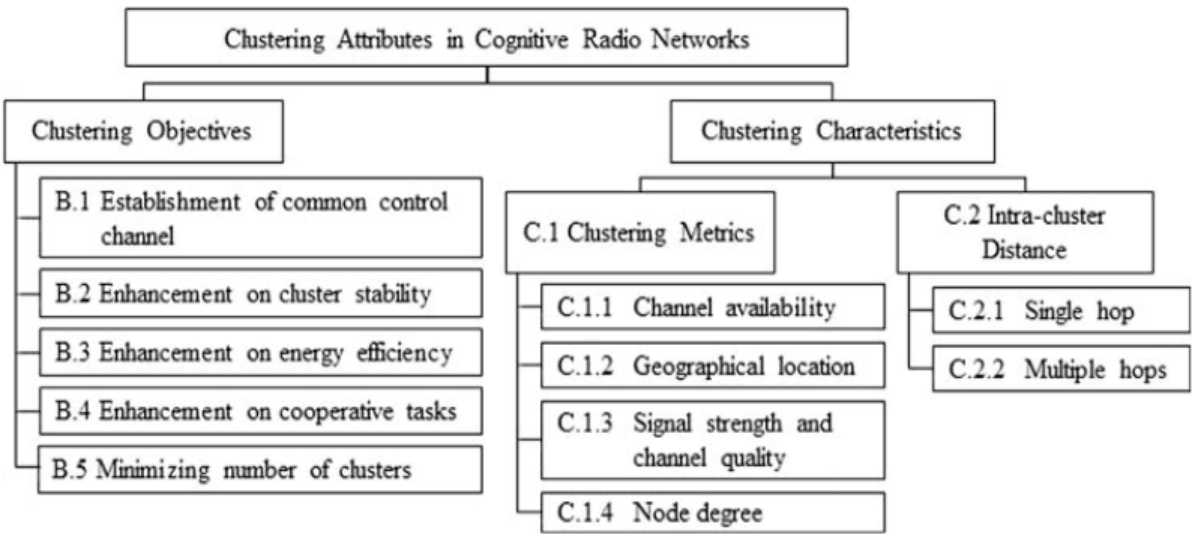



**Figure 4-12: Taxonomy of Clustering Attributes in CRN [82].**

The authors of Ref. [82] present a survey of clustering algorithms that follows one or some of the objectives or characteristics. For more information, we refer to this survey.

### 4.4.2 Objectives and Challenges for Clustering in Military Cognitive Radio Ad Hoc Networks

The following is a list of objectives for clustering in CRNs according to Ref. [82]. Each list item is accompanied by short discussion and analysis regarding tactical/military cases:

1) Finding a common control channel.

   When using clustering, a global control channel is not necessary. This may be helpful in many ways. Ref. [83] assumes that the control channel is used in CRNs for coordinated spectrum sensing, medium access control, and routing, among other things. Since channel use in cognitive networks is dynamic in CRNs, also the control channel and its assignment need to be dynamic. The authors propose a control channel assignment method, where each cluster can have a different channel for control. Note that the control channel can mean e.g., actual separate channel in multi-channel networks, separate time slot allocation in TDMA-based networks, or even frequency hopping sequence (or Code Division Multiple Access (CDMA) code) in spread spectrum systems.

   Since the channel usage (e.g., existence of PU) can vary in different parts of the network, it is natural to assume that nodes located physically close to each other are able to find the common control channel more easily than nodes far away from each other. Therefore, clustering could be based on the nodes' ability to utilize a CCC. Actually, when the channel assignment is changed, it would be necessary to have more than one candidate control channel available within a cluster, so that the migration to a new channel is as smooth as possible.

   In tactical networks, however, one of the main problems is possible jamming or interference that may harm the network operation. In these cases, the same argument of having several channels available for the control channel role is still valid.

2) Establishing cluster stability, i.e., intra-cluster and inter-cluster connectivity in the case that there is variability in the channel availability.

   The aim of cluster stability is to avoid re-clustering, in cases where channel usability changes at some part of the network. Two important aspects are the number of common channels within a cluster and the number of common channels between neighbouring clusters. In Ref. [84], cluster stability depends on the number of common channels within clusters as well as on the number of common channels between clusters. Moreover, the algorithms in Ref. [84] tend to use better-connected nodes as gateway nodes between clusters, which should enhance the robustness.

   Tactical mobile nodes need consideration of the mobility of each node. To that end, one should consider e.g., how likely it is that nodes will stay connected in the near future (e.g., for the duration of the mission time).

3) Energy efficiency from the point of view of network lifetime extension.

   Concerning clustering, rotating the cluster head role from node to node may still be applied in order to target fairness issues. Power management may not be applicable and is an inefficient way to try to minimize energy use anyway. However, energy efficiency or energy usage fairness among network nodes can be used as one critical parameter in cluster formation, even though the clusters are not specifically used for energy saving.

Ref. [85] proposes an energy-efficient MAC-layer protocol for clustering in infrastructure networks. In simplicity, clustering helps reducing the transmission of spectrum sensing data frames. The protocol includes a low power "whispering" period, during which every node sends its observation data concerning possible existence of PUs at a certain frequency. This data is furthermore used to decide which nodes actually need to send their observation data in the next phases. The system, however, is dependent of the cognitive base station. Energy efficiency of cooperative spectrum sensing reporting is addressed also by Ref. [86]. The authors apply multi-hop-based reporting of measurement to the fusion centre from cluster heads, with the goal of reducing energy spending.

4) Enhancement on cooperative tasks.

An important cooperative task in CRNs is cooperative spectrum sensing, and clustering can be designed to support this task. It is possible to imagine several possibilities how this could be done. For example, clusters could be defined so that each cluster covers as much area as possible, preferably the whole network geographical area. If each cluster senses a dedicated part of the spectrum, it is possible to create a reliable spectrum map with spatial information included by combining the sensing results of all overlapping clusters.

Alternatively, each cluster could perform the full spectrum sensing in its own area. In this approach, the spectrum sensing task can be divided among the cluster members. Again, combining all the sensing information over all clusters, one can have a complete spectrum map.

The authors of Ref. [87] have a different approach. They propose a clustering algorithm, where clusters are formed based on the similarity of spectrum sensing results of the nodes. The result is that nodes within a cluster have a common spectrum map, which makes management of the spectrum dynamics easier. Moreover, by sharing the sensing results to neighbouring clusters, a complete spectrum map can be formed (again).

Attack prevention and mitigation is relevant in all networks, but especially so in military networks. Nodes can e.g., cooperate on finding out the locations of jammers at certain frequencies by combining individual observations and observing locations. Usually this type of combining should be performed at one selected node, the so-called Fusion Centre (FC). In the case of a clustered network, each cluster may have its own FC. There has been some research on the security issues concerning the use of FCs in critical information processing. Especially critical in CRN cases, there is an attack type called Spectrum Sensing Data Falsification (SSDF). This attack involves a malicious user in the network, which deliberately sends false spectrum sensing data in order to hinder the network operation.

In any case, any kind of malicious activity in the network needs to be prevented, or at least its effect to the networked operations mitigated. In this, clustering can be used as a method to insulate potential harmful effect to only one part of the network. Clusters operating using a different frequency are not affected by the jamming, and they can also be warned of the potentially bad frequencies.

## 4.5 MANAGEMENT OF COGNITIVE RADIO NETWORKS

Network management means a wide variety of functions, activities, methods, and procedures to administrate, operate, and reliably maintain networked systems. To that end, objectives of network management include the overall network reliability, efficiency and capacity/capabilities of data transfer. Obligatory management functions may need to take place centrally, but they may reside either inside or outside the network itself. Moreover, the cognitive cycle (Observe, Orient, Plan, Decide, Act, and Learn) will have influence on the management aspects and can also be influenced by them. We also point out the role of policies in dictating

how networks are allowed to be operated and therefore setting the limits to management functions as well. Policies have elementary aspects to start up and operate the network.

In military and especially tactical context, due to the temporal nature of the networks (deployable networks, mobile networks), configuration of a network will be done before the mission, whereas during the mission monitoring and the defined autonomous/real-time management functions can be applied. Finally, after the mission collected information is analysed. This is principally different from ordinary fixed network setups.

### 4.5.1 State of the Art

One of the main computer networks management protocol is Simple Network Management Protocol (SNMP). Although it is not designed for ad hoc networks, specifically, it is often a part of IP-based radio networks. It is based on manager-agent architecture, where each node is equipped with a Management Information Base (MIB), which is updated by agents during node operation. The updates can be based on new policies sent by the manager to agents.

General network management principles and technologies are briefly listed next. The main areas of network management according to the Operation, Administration, Maintenance, and Provisioning (OAMP) model as described in IETF RFC 6291 are:

1) Network operation: This includes monitoring of the network functions to rapidly, efficiently address and fix problems as they occur and preferably even before users become aware of problems.
2) Network administration: Situation awareness and monitoring including inventory tracking of network resources such as links, nodes and routes. In addition, monitoring and updating network device's software may be included in this function.
3) Network maintenance: Timely repair as well as necessary upgrades to all network resources including preventive and corrective measures.
4) Network provisioning: Configuring network resources to support the requirements of a particular service or a policy.

In the OSI systems, the network management functions are categorized in five different management areas, according to ISO/IEC 7498-4: Fault, Configuration, Administration, Performance, and Security (FCAPS):

1) Fault Management: Reliability, availability, survivability, quality assurance, alarm surveillance, fault localization, fault correction, testing, trouble administration;
2) Configuration Management: Network planning and engineering, installation, service planning and negotiation, provisioning, status, control;
3) Accounting / Administration: Usage measurement, pricing, corrections, finance, enterprise control, user and role administration, authentication and authorization;
4) Performance Management: Performance quality assurance, performance monitoring, performance management control, performance analysis; and
5) Security Management: Prevention detection, containment, recovery, security administration.

The FCAPS model can be seen as bottom-up or network-centric, while the Fulfilment, Assurance, Billing (FAB) model looks at the processes more from top down, as it is customer-business centric. The Information Technology Infrastructure Library (ITIL) model, which is a set of practices for IT service management and is used by many telecommunication service providers, is more about business processes.

Network management comprises a wide variety of functions, activities, methods, and procedures to administrate, operate, and reliably maintain networked systems. There exist standards and proposed solutions

for wired and even ad hoc wireless networks. Ref. [88] provides a brief description of typical management solutions and proposes a novel Cognitive Network Management Protocol (CNMP) especially suited for cognitive wireless ad hoc networks based on clustered hierarchical structures. The cluster head nodes act as intermediate managers between the central management entity and the node-level manager clients. This way, both the fine-grained local information, as well as the network-wide situation, can be utilized in the network management (see Figure 4-13).

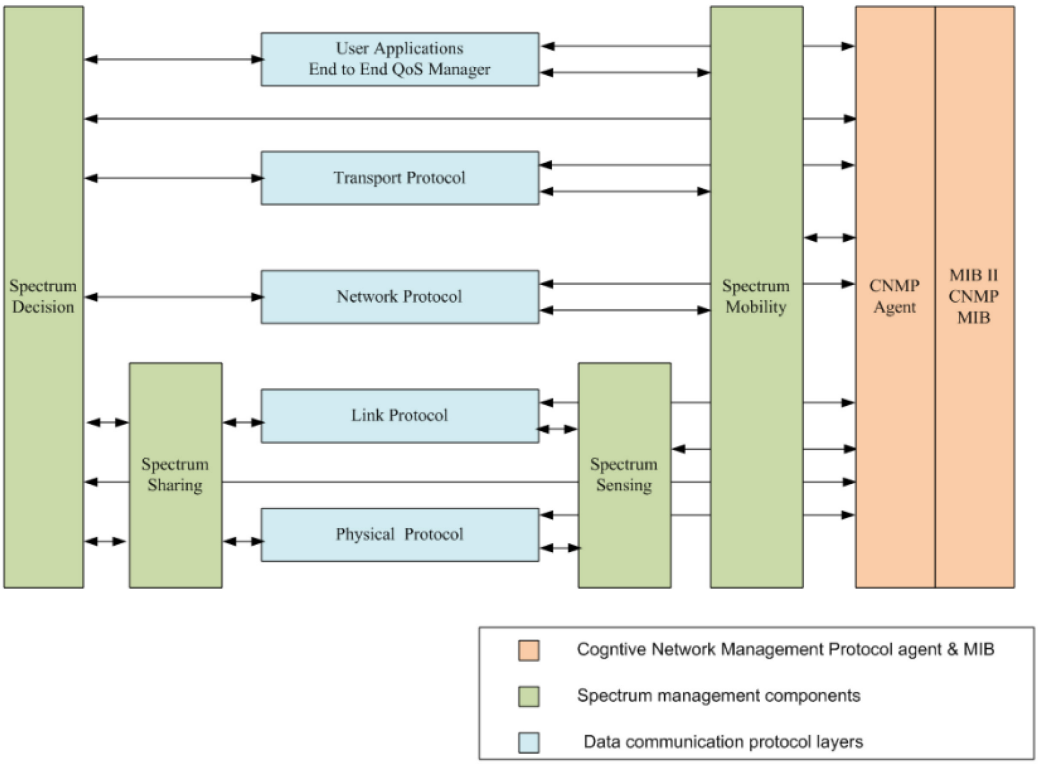



**Figure 4-13: CNMP as Suggested by Ref. [88].**

A policy-based radio network management mechanism is proposed by Ref. [89]. As shown in Figure 4-14, in addition to context and profiles, the policies are key input parameters to the operation of the cognitive network.

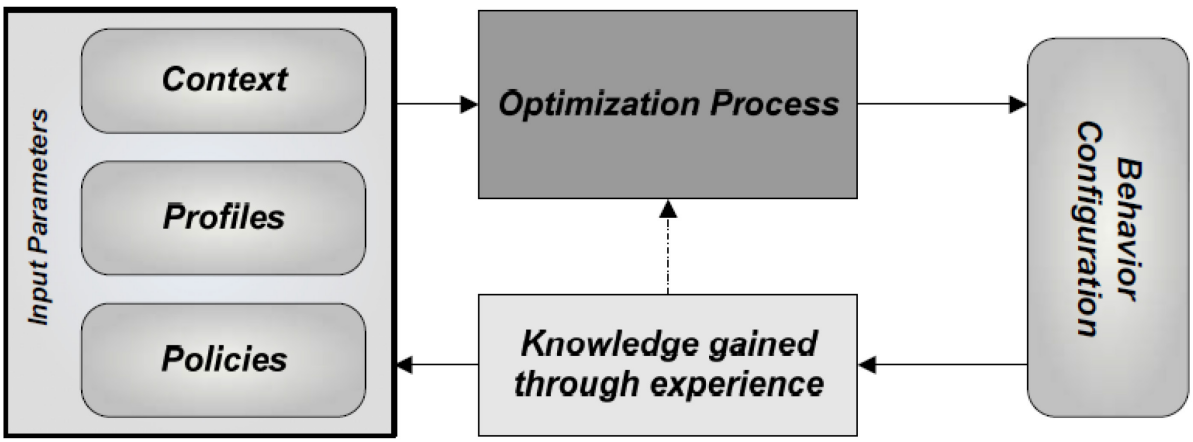



**Figure 4-14: CRN Operation Principle, as Presented in Ref. [89].**

There exist several other proposals for possible solutions of cognitive network management that incorporate the idea of policies as one of the drivers in the cognitive process. For example, the Cognitive Network Management System (CNMS) aims to provide automated, policy-based real-time network management for CRAHNs [90]. It is a policy management framework designed to mitigate the need for centralized network management, reduce operator hands-on time, and increase network reliability. The CNMS includes a mechanism to adapt at run-time to unanticipated network conditions, as well as the related distributed learning functions, as depicted in Figure 4-15.

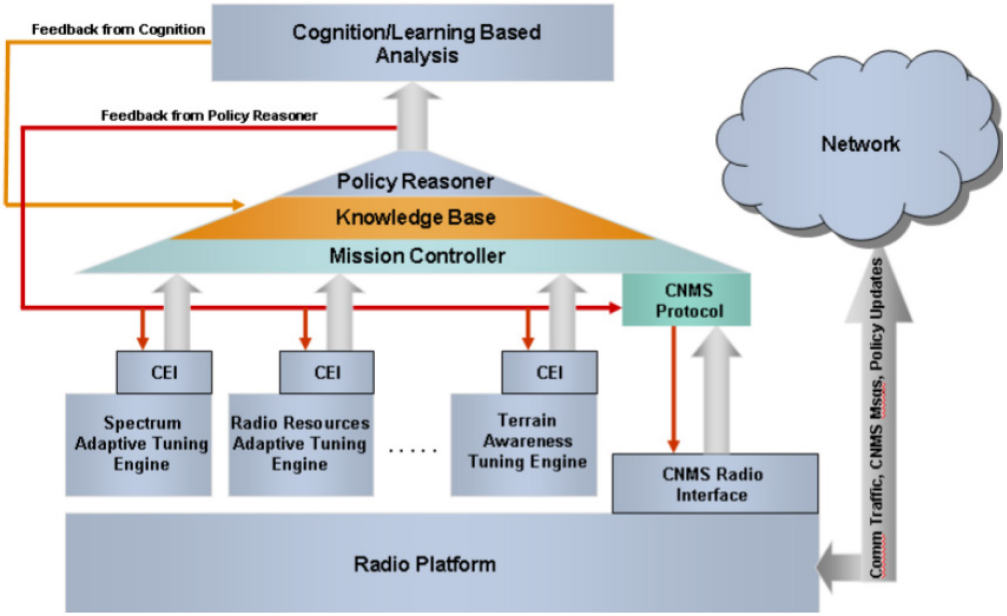



**Figure 4-15: Cognitive Network Management System (see Ref. [90]).**

The main conclusion that can be drawn from the state of the art is that Cognitive Network Management systems require at least the following functions and features:

- Interfaces to manageable entities (a.k.a. “knobs”);
- Management Information Bases (MIBs);
- Policy, profile, and contest (mission rules) databases;
- Knowledge database; and
- Analysis modules, knowledge and policy interpreters.

### 4.5.2 Challenges for the Management in Military Cognitive Radio Networks

Objectives of network management include the overall network reliability, efficiency and capacity/capabilities of data transfer. Traditionally, network management does not include end user terminal equipment. However, this notion may be challenged by CRN especially in CRAHNs (see Ref. [91]), as end-user devices will become essentially the only active elements in the network and its management. In infrastructure-based networks, network management can be limited to cover interconnected access points, but in CRAHNs the network management function needs to be extended down to each node in the network, i.e., to the end user devices. However, as a gradually emerging feature, the autonomous and cognitive management processes may very well be first applied to network infrastructure devices, similar to the Self-Organizing Networks (SON) paradigm currently being brought into civilian cellular networks. It would even be possible that only part of the network devices would be autonomously managed, while others, e.g., legacy devices, are manually managed.

In a military context, the basic advantage of cognitive management is that the management processes can be, to some extent, automated during missions. The remaining question is how far and in which situations and concerning what functions it can be automated for being conducted by a cognitive engine.

From the management point of view, novel challenges in military/tactical CRAHNs as compared to legacy networks include at least the following issues:

- Goals and related management policies are set on mission basis and may differ drastically from one mission to another. A methodology to transfer mission specific policies into management principles needs to be decided.
- Knowledge and network information need to be transmitted and managed in a distributed manner and with different levels of security concerns.
- Cognition can take over management functions and, therefore, reduce the need for manpower and training resources. There will be a need to balance human control and autonomous management. What is left for human control may be related to longer time-scale management goals and occasional critical situations, while autonomous management function makes routinely the short time-scale adjustments.
- Isolated sections of the network may, and most often will, exist temporarily. At those times, the management will completely rely on autonomous functions (We do not expect the soldier to concentrate on network management issues during a mission.). If there is a need for a safe mode for those occasions, then it must be investigated (e.g., tighter limits for autonomous adjustments would be effective if the network is not connected).

As already pointed out, the networks are typically operational for a specific mission only, which can take from several hours to months, depending on the mission and network. Therefore, there is a need to consider the management in different operational phases; practically that would mean, before mission, during mission, and after mission. The five different network management functionalities, as well as policy management, are split into the mentioned three mission phases in Table 4-3 below. Although e.g., Ref. [92] presents a range of military operations across a conflict continuum and similarly Ref. [93] depicts a more complex mosaic of military activities in a conflict, our focus in this report is the life-cycle of CRAHN in a military operation or a mission. Therefore, for our purposes, it suffices to consider the network management aspects against deployment phases of the network itself, namely: planning, preparation, and configuration “before mission”, “during mission” and “after mission”.

One should note that we have included the policy management in the table, although it is not part of FCAPS. To our understanding, policies are essential managed elements to be considered in military context, as we have pointed out earlier.

The key observation is that only during the mission execution, the network management needs to be performed more or less autonomously by the cognitive network management functions and not during the preparation or evaluation. On the other hand, and equally importantly, the feedback available after mission can be analysed carefully and lessons identified can be fully utilized in preparing the network for the next mission.

Another key observation is that all the management functions are not necessarily handled within or by the same cognitive process. This would imply that some of the functions can be more autonomous than some others. Also, it would be possible to give part of the network management duties to central managers, e.g., those included in the SDN based architectures. We propose that there is going to be a gradual evolution from manual management to autonomous learning systems. This is the case especially during critical mission phase. In the less time-critical phases before and after mission, the management functionalities and their readiness for autonomous management can be more easily tested before fielding.

**Table 4-3: Management Functionalities with Respect to Mission Phases.**

| Management Function | Before Mission | During Mission | After Mission |
|---|---|---|---|
| *Policy Management* | • Update and configure policies to match mission requirements. | • Apply policies in all autonomous reconfiguration and management processes.<br>• Mission time policy changes. | • Review of the impact of the applied policies. |
| *Fault Management* | • Analyse previous faults.<br>• Set up mitigation strategies.<br>• Identify faults to be monitored. | • Recognize, isolate, correct and log faults (autonomous process).<br>• Select and apply the mitigation method(s). | • Check the logs to find obvious trends, etc.<br>• Check the correctness of the autonomous fault management process.<br>• Input to cognition process. |
| *Configuration Management* | • Network and device setup according to given mission requirements. | • Track configuration changes made by autonomous engine.<br>• Mission time configurations. | • Assess the performance and success of the configurations used during mission. |
| *Administration Management* | • Accounts for user.<br>• Access management. | • Block compromised users.<br>• Adding and removing users. | • Assess the performance and success of the autonomous processes. |
| *Performance Management* | • Implement lessons learned from previous missions.<br>• Update the mission goals and related performance metrics. | • Monitoring of the network performance using defined metrics.<br>• Real-time adjustments by CNE according to policies.<br>• Traffic shaping, etc. methods. | • Evaluation of the mission time-critical performance metrics. |
| *Security Management* | • Provide cryptographic keys and initial security materiel.<br>• Update security infrastructure, certificates, etc. | • Trust management.<br>• Identify compromised users.<br>• React on security incidents.<br>• Manage different classification levels. | • Assess the performance and success of the autonomous processes. |

#### 4.5.2.1 Policy Management

Policies are used to facilitate decision making for spectrum, clustering, routing, security, QoS and many other parameters influencing the network behaviour. Policies set configuration borders and conditions for changes that can take place in the network and are therefore of crucial importance in the more or less autonomous CNR management. Furthermore, the policy management must take into account all cases where policies are changed. The questions remain whether it should be possible to change the policies during missions and, if so, how the policy changes are performed so that it is taken into account all over the network.

#### 4.5.2.2 Fault Management

Faults can be expected or unexpected, e.g., an alarm due to hostile jamming is something expected, a software error is not expected, but nevertheless needs to be logged by the fault management. It is not necessary for the functioning of a CRN but is an additional service to the operators and can be utilized in the after-mission phase.

Three possible actions in case of alarms during the mission phase are:

- The cognitive system may automatically react on the fault/alarm and just inform the network supervisor and/or log the event.
- The cognitive system may offer solution strategies to the network supervisor and let him select one.
- The cognitive system may inform the network supervisor without taking any action.

#### 4.5.2.3 Configuration Management

Target is automatization, therefore, manual configuration in the planning phase is just the initial configuration, after that the network should be able to reconfigure itself. Therefore, a more complex initial configuration for regulating the automatization should lead to less manual reconfigurations during the mission. This is again a question of finding the proper balance (trade-off). It is possible to list required inputs for allowing automatization based on the cognitive cycle. These include policies, strategies, waveforms and all their parameters (unfortunately quite a lot of information). How and in which format this is given to the management process is an open question.

#### 4.5.2.4 Accounting/Administration

Since there is no crucial difference to “normal” ad hoc networks, this is not in the focus of our report.

#### 4.5.2.5 Performance Management

Target is again automatization and, therefore, cognitive performance management takes into account more parameters. This may lead to an increased sharing of performance values over the network, and several issues need to be considered:

- How to manage global performance characteristics.
- Performance management is affected by and affecting the configuration management, because every change to improve the performance is part of configuration management. Also, changes in the configuration will most likely affect the performance.
- Any optimization based on several parameters usually leads to several local optima; therefore, it may be that the global optimum is not found directly. Learning might help to find the global optimum. Learning should also include the history and lessons learned from previous mission. Before mission and after mission performance management are essential in this sense.

- How can performance be improved? For example, by:
  - Rerouting traffic;
  - Changing frequency allocation;
  - Changing clustering;
  - Topology changes;
  - Change traffic priorities / queuing management;
  - Change waveform / waveform parameters; and
  - Change transmit power.

#### 4.5.2.6 Security Management

Since there is no crucial difference to "normal" ad hoc networks, this is not in the focus of our report.

#### 4.5.2.7 Related Issues and Challenges

Besides the FCAPS functions, there are other, partly supporting, issues that need to be considered when network management is designed.

The need for monitoring of the network in a CRN is increased compared to legacy networking, as the objective of CRN is to automate management processes. Monitoring provides also crucial input to the learning process and helps to improve effectiveness of the networking in the future and supports the planning of the network.

Due to huge amount of information generated and available in the network, one needs to define which information is gathered and where this information is needed. Examples are frequency related information and propagation conditions, node/neighbour node status (load, battery conditions). In order to avoid excess control information overhead, there must be a balance between user traffic and management information about other nodes.

Is the monitored information forwarded to the user during lifetime (during mission)? Which user needs this information? Situation awareness of the network and its performance are related to the expected lifetime of the mission (network).

The network will have a set of objectives, defined by the mission goals. Objectives therefore define how the network is ultimately configured. Network level objectives (goals) are:

- Lifetime;
- Connectivity;
- Latency;
- Bandwidth; and
- Fairness, etc.

How are these issues managed in relation to performance and configuration management?

The process to capture, select, and share appropriate historical data of the performance of the network, which may include node-level data, is in general referred to as knowledge management. Obviously, this process supports policy management and learning (as well as most of the management issues). It is again important to carefully design what data needs to be collected, distributed and stored. This will be mainly data which relates to the network level objectives, e.g., latency of messages, used bandwidth, etc.

By default, in an ad hoc network knowledge is based on a distributed data collection. However, in military context network-wide collective knowledge will most likely be classified, at least some of it; therefore, the visibility of locally stored knowledge to other devices will be limited, and there will be a number of alternatives between distributed and centralized modes of the use of network knowledge. Most likely, there must be a distinction between knowledge used by the cognitive engine at the local level and the network level.

Frequency management is a technical task of the node, but it is guided by policies at the network level. Other technical methods at the node level (but at higher layers) are traffic shaping, load-balancing, and route selection. In order to handle these issues at the network level, a feedback channel for applications and related priority management is needed.

The actual architecture of the management structure in CRAHNs needs to be defined by answering the following issues: How are the management entities interconnected? Is management a centralized or a distributed task? Who can influence the configuration of a radio? How can management information be exchanged?

## 4.6 TRUST MANAGEMENT IN COGNITIVE RADIO NETWORKS

### 4.6.1 State of the Art

Frequently, the level of trust is assessed based on direct interactions, observations and recommendations, as proposed by Bao and Chen [94]. Sometimes, to overcome untrustworthy recommendations, the data collected for other objects are weighted depending on the sender trust level, as described by Li and Kato in Ref. [95].

The different quality of data sources used for trust assessment also needs to be considered. The solution, proposed by Buchegger and Le Boudec [96], assumes that the trust rating changes according to the evaluation function, which allocates different weights to various types of behaviour. The object assigns the highest weights to events identified by it, lower for those that are observed by its vicinity and the lowest for information collected from historical reports. Some authors incorporate additional information into the trust evaluation process that refers to security policy [96], certificates exchange [97], or risk assessment [98].

Typically, the trust management schemes presented in the literature consider the observed events without their detailed analysis. A symptom of abnormal behaviour, e.g., packet forwarding failure observed in the neighbouring node, as considered by Junfeng *et al.* in Ref. [99], can be the consequence of the node's selfish behaviour, but also caused by node disconnection, communication interferences or low battery level. Furthermore, only few solutions consider the effects of dynamic changes of IoT infrastructure. The concept presented by Bao and Chen in Ref. [100] incorporates time-dependent parameters for trust evaluation, takes into account multiple social relationships among object owners and advocates the use of three trust properties, i.e., honesty, cooperativeness, and community interest.

The trust evaluation process is based on the data originated from the variety of information sources of different quality, trustworthy, and complexity that have to be combined into a coherent and accurate whole. This calls for implementation of appropriate information fusion techniques to reduce the risk of incorrect or imprecise identification of potential threats. The probabilistic inference is the most frequently used technique for the object's trust level assessment, e.g., described by Han *et al.* [101]. Some authors, for instance, Chen *et al.* [102], propose using fuzzy logic to handle the concept of partial belief, where the belief value may range between "completely trust" and "completely do not trust". If the source data are conflicted and/or uncertain, some authors, for instance, Konorski in Ref. [103], recommend using Dempster-Shafer evidence theory, allowing knowledge to be distinguished from lack of knowledge and, in the consequence, facilitating the verification of an exclusive set of hypotheses on the object's trust level.

Ref. [104] points out that trust management mechanisms are required to identify the malicious secondary users and to check signalling in the CCC. The most solutions for CRNs are devoted to detection of the SUs transferring false sensing information. Literature presents some attacks using fake sensing information. The examples are Byzantine attack [105] or Spectrum Sensing Data Falsification attack [106].

In the case of infrastructure-based CRNs, the SU's access point (base station), that is responsible for information fusion about of bandwidth availability, takes a decision on channel assignment to the SUs. In Refs. [107], [108], [109], [110], [111], [112], trust management procedures are proposed, which are based on signalling monitoring exchanged between SUs and access points to capture the fake messages.

In Ref. [113], Kalaiselvan and Kavitha propose a trust assessment model for CRs, where a level of trust to other nodes is calculated, based on direct observation of the node (signalling generated by this node) and based on reputation concerning a given node, identified and sent by other nodes. The direct observation leads to the Bayesian analysis, and the reputation system is based on Dempster-Shafer theory. The trusted nodes are taken into account in routing selection.

The authors of Ref. [114] propose a set of mechanics named SMTD (Security Management based on Trust Determination), which intrudes modules responsible for node authentication, interaction, configuration, exchange and collection of trust level information and security reactions.

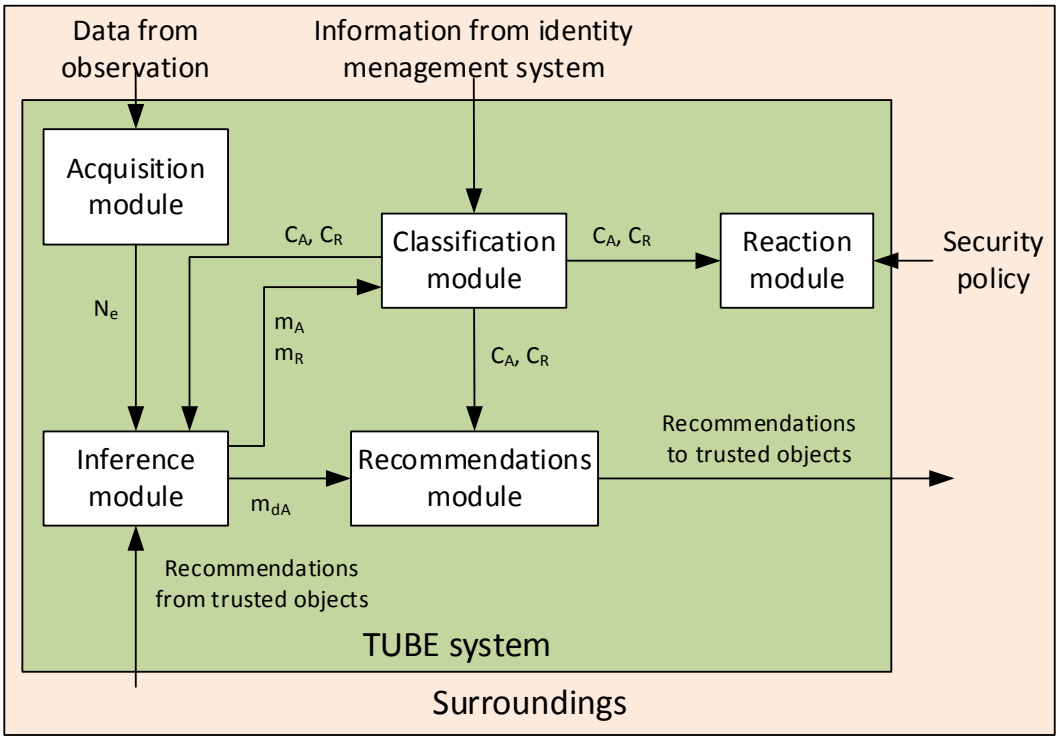
### 4.6.2 Challenges and Proposals for Trust Management in Military Cognitive Radio Networks

Assuming that the main elements of the military CRs are cognitive engines that require mutual communications, effective trust-management systems have to be applied in the CRAHNs. The nodes exchanging the signalling messages, that are required to build knowledge about the spectral environment (i.e., cooperative sensing-based) or to support dynamic spectrum access and management (i.e., cognitive routing, topology control), must trust other nodes. If the cognitive engine of the authenticated node tries to send false information (e.g., about sensing results), the rest of the network will completely collapse. Thus, in military CRNs, especially in military CRAHNs, it is proposed to take into account a solution similar to TrUst-Based situation awarEness system (TUBE) [115].

The TUBE system performs three major functions: collecting information about the environment, trust evaluation and classification of the nodes, and suggesting reactions to identified threats in order to ensure the communication security. It is composed of the following modules (Figure 4-16):

- Information Acquisition;
- Inference;
- Recommendations;
- Classification; and
- Reaction.

The assessment of the environment is performed by continuous monitoring of the neighbouring objects' behaviour. However, in many cases, the knowledge acquired by a single element is insufficient for correct assessment of the current situation; therefore, the exchange of information with other trusted objects is needed. Additional information on the object's security features is reached from the identity management system. An advanced inference technique is used for classification of the object's allowance – based on the security policy rules – to adapt the traffic control mechanisms and to reduce the impact of detected threats.




$m_{dA}$ / $m_A$ - values of basic belief assignment for hypothesis concerning performed actions based on observation / observation and recommendations
$m_R$ - values of basic belief assignment for hypothesis concerning recommendations correctness
$C_A$ / $C_R$ - nodes class concerning performed actions / recommendations correctness
$N_e$ – events notification

**Figure 4-16: The TUBE System Architecture for Military CRAHNs.**

The acquisition information module is responsible for capturing and analysis of transmitted cognitive signalling messages (and user packets if needed), as well as for preliminary assessment of the events. The object behaviour is assessed based on its cooperation with the signalling message forwarding (if they are resent by neighbouring nodes) and correctness of all signalling messages exchanged between the nodes.

The inference module is responsible for evaluation of the objects based on the results of direct observations and recommendations. However, recommendations can be biased or outdated, so they have to be verified before being used for classification purposes. The module performs the following functions:

- Direct evaluation concerning performed actions;
- Recommendation verification;
- Direct evaluation concerning recommendation correctness; and
- Evaluation concerning performed actions based on both observed actions and verified recommendations.

An observed symptom of abnormal behaviour can be triggered by different events. Moreover, the input data can be unreliable, incomplete and/or conflicted, so it is decided to use inference and classification processes (DSm) proposed by Dezert and Smarandache [116]. This allows a set of primary and secondary hypotheses to be defined on the node behaviour that improves the quality of potential threat detection. In case of direct evaluation based on performed actions, we consider the following set of hypotheses: cooperating, uncertain cooperating, egoistic, suspect egoistic, honest, uncertain honest, liar, and suspect liar.

During direct evaluation concerning performed actions, the values of basic belief assignment *m()* are calculated for each hypothesis. The value of $m_{dA}()$ depends on the number of events that correspond to the hypothesis and on the time of the observed event:

$$m_b(x_1) = \frac{\sum_k w_k \cdot n_{1k}}{\sum_k w_k \cdot \sum_i^{|D^\Theta|} n_{ik}}, \tag{4-4}$$

where:

- $m_{dA}(x_1)$ – basic belief assignment for hypothesis $x_1$;
- $D^\Theta = \{x_1, x_2, \ldots, x_N\}$ – set of all hypotheses, where $|D^\Theta| = N$;
- $n_{ik}$ – the number of events evaluated as $x_i$ in $k$-th time slot; and
- $w_k$ – the event weight for $k$-th time slot.

In many cases, the knowledge gained by a single object is inadequate for a comprehensive assessment of the current situation. Therefore, it is necessary to exchange information with other trusted components in the network. This action is performed by the recommendations module. Recommendations are sent periodically using a dedicated protocol. They contain the values of $m_{dA}()$ for each hypothesis and the timestamp.

During a campaign, the trusted objects may change the behaviour to achieve their specific goals or because they were captured by the opponents, and – in consequence – they can transfer incorrect recommendations. Verification of recommendation correctness and detection of liar nodes is a multistage process performed based on information derived from direct observation, recommendations, historical data, authentication mechanism, and information on the node location.

The inference module discards self-promoting recommendations and those that are sent by untrusted objects. The module checks the ability to verify received recommendations based on the accumulated knowledge. If such information is unavailable, a decision about including a received recommendation is made based on sending the object's classification concerning recommendation correctness.

Each verified recommendation contributes to the assessment of the related object. During direct evaluation concerning recommendation correctness, the following set of hypotheses on the object is considered: honest, uncertain honest, suspected liar, or liar. The value of *m()* for each hypothesis on recommendation correctness depends on the number of events that correspond to the hypothesis, the event timestamp, and the event-dependent weight (for instance, abnormal events are taken with higher weight). Recommendations consistent with the current knowledge or derived from the reliable nodes are included in the object's evaluation. The classic DSm rule of combination is used for fusion of direct evaluation concerning performed actions and recommendations.

The classification module is responsible for the final assessment of the objects based on information gained from the identity management system and the results of direct evaluation. The objects are separately classified in terms of recommendation correctness as honest or liar and in terms of performed actions as coalition, partner, egoistic or malicious. The results of classification significantly contribute to the situation assessment of the IoT environment and can be used by the reaction module to provide an appropriate action, which can reduce the impact of detected threats.

The efficiency of the TUBE system and its robustness to complex reputation attacks was tested by simulation in the Riverbed Modeler simulation tool. A standard WLAN node was extended to include TUBE modules as depicted in Figure 4-16. The OLSRv1 routing protocol with its standard configuration was used for multi-hop transmission. The acquisition module was able to collect information on correctness of signalling message

forwarding. The dedicated UDP-based reputation dissemination protocol was used for recommendation dissemination. Nodes assessed their surroundings every $t_t$ = 30s, while the recommendations were disseminated every $t_r$ = 60s.

The experiments were focused on verification of misbehaving objects detection and robustness of TUBE system to selected reputation attacks as well as on assessment of the system efficiency.

Figure 4-17 shows the network structure used for simulation. The lines between the nodes represent the communication links (the free space propagation model was assumed).

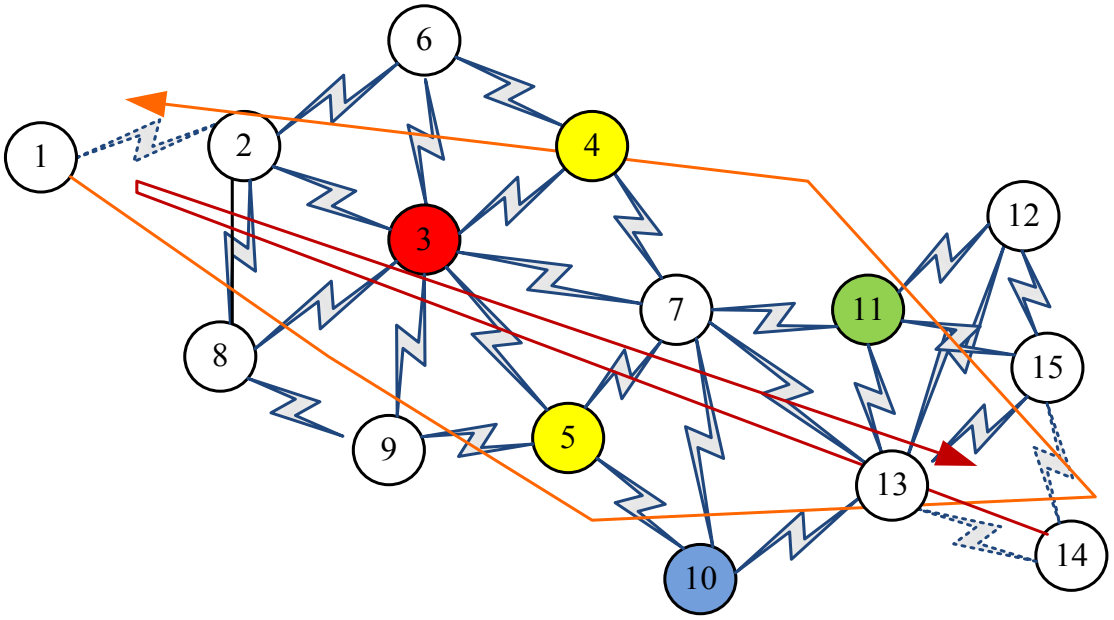



**Figure 4-17: The TUBE System Architecture for Military CRAHNs.**

Four nodes i.e., #3, #4, #5 and #10 are captured by an opponent during operation and from that time accomplish different attack strategies. Node #3 drops forwarded data packets, sends correct routing protocol messages and performs typical self-promotion attacks by dissemination of wrong recommendations on itself. Nodes #4 and #5 work correctly, but nastily disseminate wrong recommendations on neighbouring surroundings. Node #10 forwards the recommendations correctly but disrupts network operation by sending incorrect signalling messages.

Partner node #11 works correctly and forwards incoming messages but is unable to receive and disseminate recommendations as it does not use the TUBE system. The remaining nodes behave correctly. Nodes #1 and #14 move along the trajectory shown by the arrows. Each node also generates user traffic using 2048-byte UDP/IPv6 packets per second to randomly selected nodes.

The TUBE system implemented in all coalition CR nodes (even in the captured ones) categorizes the remaining nodes in terms of performed actions to the following classes: “coalition” (C), “malicious” (M), “partner” (P) (cannot send recommendations) or “egoistic” (E), and in terms of recommendation correctness to: “honest” (H) or “liar” (L). Some nodes, due to lack of information on performed actions, can be classified only based on the recommendations and are denoted by CR, MR, PR, or ER, respectively. Moreover, some nodes cannot be classified at all due to lack of data required for trust-based assessment and are denoted by N.

The results of the final node classification in terms of performed actions are shown in Table 4-4. Node #3 is correctly classified as "egoistic" (E) by all evaluating nodes, including those that do not communicate directly with it. Nodes #4 and #5 are correctly classified as "coalition" (C or CR) since they correctly forward packet and routing protocol messages. Node #10 is correctly classified as "malicious" (M or MR) however we should notice that neighbouring evaluators do not need additional recommendations for classification. And finally, node #11 is also recognized as "partner" (P or PR). Only node #12 is not classified by node #9, due to lack of required data (N).

**Table 4-4: CR Node Classification in Terms of Performed Actions.**

| | | Evaluating Nodes | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 6 | 7 | 8 | 9 | 12 | 13 | 14 | 15 |
| Evaluated Nodes | 1 | - | C | C | C | C | C | C | C | C | C |
| | 2 | C | - | C | $C^R$ | C | $C^R$ | $C^R$ | $C^R$ | C | $C^R$ |
| | 3 | E | E | E | E | E | E | $E^R$ | $E^R$ | E | $E^R$ |
| | 4 | C | $C^R$ | C | C | $C^R$ | $C^R$ | $C^R$ | $C^R$ | C | $C^R$ |
| | 5 | C | $C^R$ | $C^R$ | C | $C^R$ | C | $C^R$ | $C^R$ | C | $C^R$ |
| | 6 | C | C | - | $C^R$ | $C^R$ | $C^R$ | $C^R$ | $C^R$ | C | $C^R$ |
| | 7 | C | $C^R$ | $C^R$ | - | $C^R$ | $C^R$ | $C^R$ | C | C | $C^R$ |
| | 8 | C | C | $C^R$ | $C^R$ | - | C | $C^R$ | $C^R$ | C | $C^R$ |
| | 9 | C | $C^R$ | $C^R$ | $C^R$ | C | - | $C^R$ | $C^R$ | C | $C^R$ |
| | 10 | M | $M^R$ | $M^R$ | M | $M^R$ | $M^R$ | $M^R$ | M | M | $M^R$ |
| | 11 | P | $P^R$ | $P^R$ | P | $P^R$ | $P^R$ | P | P | P | P |
| | 12 | C | $C^R$ | $C^R$ | $C^R$ | $C^R$ | N | - | C | C | C |
| | 13 | C | $C^R$ | $C^R$ | C | $C^R$ | $C^R$ | C | - | C | C |
| | 14 | C | C | C | C | C | C | C | C | - | C |
| | 15 | C | $C^R$ | $C^R$ | $C^R$ | $C^R$ | $C^R$ | C | C | C | - |

In order to identify threats caused by the nodes sending incorrect recommendations, an additional classification in terms of recommendation correctness has to be considered. The results of such a classification are presented in Table 4-5.

On the whole, all hostile nodes are classified correctly in terms of recommendation correctness, except the classification of node #3 by node #1. It is caused due to the movement of node #1 outside the communication range of node #3 that initially works correctly in the beginning of simulation. We should notice that recommendations are exchanged between neighbouring nodes only, so, many nodes are unclassified due to lack of required data. Moreover, node #11 cannot be classified because it does not exchange recommendations.

The TUBE reaction module takes into account the results of both classifications and adapts traffic control mechanisms to improve the network security and increase the efficiency of communications.

The results confirm that implementation of the TUBE system in a CRN can significantly reduce participation of untrusted cognitive machines in military CRAHNs.

**Table 4-5: CR Node Classification in Terms of Recommendations Correctness.**

| | | Evaluating Nodes | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 6 | 7 | 8 | 9 | 12 | 13 | 14 | 15 |
| Evaluated Nodes | 1 | - | H | H | H | H | H | H | H | H | H |
| | 2 | H | - | H | N | H | N | N | N | H | N |
| | 3 | H | L | L | L | L | L | N | N | L | N |
| | 4 | L | N | L | L | N | N | N | N | L | N |
| | 5 | L | N | N | L | N | L | N | N | L | N |
| | 6 | H | H | - | N | N | N | N | N | H | N |
| | 7 | H | N | N | - | N | N | N | H | H | N |
| | 8 | H | H | N | N | - | H | N | N | H | N |
| | 9 | H | N | N | N | H | - | N | N | H | N |
| | 10 | H | N | N | H | N | N | N | H | H | N |
| | 11 | N | N | N | N | N | N | N | N | N | N |
| | 12 | H | N | N | N | N | N | - | H | H | H |
| | 13 | H | N | N | H | N | N | H | - | H | H |
| | 14 | H | H | H | H | H | H | H | H | - | H |
| | 15 | H | N | N | N | N | N | H | H | H | - |

## 4.7 RELIABLE EXCHANGE OF CONTROL INFORMATION

The exchange of control information is one of the most important characteristics of modern communication systems, which must cope with dynamic changes of the spectral and spatial environment. Considering CRN, there are several entities, which need to exchange such control information.

One of them is the networking, which regularly updates topology information for obtaining and maintaining multi-hop routes. Ad hoc networks moreover transmit HELLO messages for allowing nodes to join the network and to check whether an apparently silent node is still alive.

In addition to that, also the CR related entities exchange control information. First of all, spectrum sensing results are synchronized for identifying common communication channels. Furthermore, channel changes must be negotiated. And the tasks of cognition will most probably not be limited to channel management.

Moreover, trust management requires control information exchange for identifying unreliable nodes. Negotiations whether a node correctly forwards messages and therefore can be trusted will also take place on the control channel.

CRN will need to organize the exchange the control information of all these techniques in an optimal and safe way with a focus on end-to-end optimization, which may require even additional control resources but must not impair user data traffic.

### 4.7.1 State of the Art

In literature, basically two approaches for exchanging control information are proposed. Several papers propose to use a CCC, which is a logical channel constantly available to all nodes of the network [117], [118], [119], [120], [121]; others propose to avoid such a static control channel and to choose a control channel dynamically, as required, because they claim that the static CCC principle has several drawbacks, such as extra channel resources or additional complexity [122], [123], [124], [125].

Many relevant papers regarding CCC are written for civilian purposes and therefore assume the PU/SU concept. This is a hierarchical approach, in which the PU is a licensed user (higher priority user), who does not use his spectrum at all times. Therefore, an SU, which is usually a CR or CRN, reuses the spectrum if not occupied by the PU. This requires that the SU evacuates the spectrum immediately when the PU claims it. This concept can be transferred to the military domain by regarding the PU as any kind of emerging interference impairing the communication of a military CRN, leading to appropriate reactions in the CCC of the network.

Ref. [126] gives a very good overview about the design of static and dynamic CCC in literature, in addition to Refs. [117], [118], [119], [120], [121], [122], [123], [124], [125]. It classifies CCC design schemes and compares solutions presented in literature according to the classifications. Figure 4-18 shows these classifications. It basically differentiates overlay and underlay channels. While overlay differentiates specifically between in-band and out-of-band allocation, underlay channels carry Ultra-Wideband (UWB) signals for both in-band and out-of-band usage. Channel allocation in in-band CCCs can be sequence-based (using frequency hopping) or group-based (using neighbour coordination or clustering). Out-of-band channels are termed dedicated here, but as shown in Ref. [127], they can also be sequence- or group-based.

For comparing the CCC design schemes proposed in literature, the following design properties were identified: In addition to the type of scheme (sequence-based, group-based, dedicated, or UWB) and the allocation (in-band, out-of-band), the coverage of the CCC is given and indicates whether this CCC is used locally for a subset of nodes or globally for all nodes. Furthermore, the number of radio transceivers required for the design scheme is compared, as well as whether the CCC design requires the synchronization of nodes and includes mechanisms for neighbour discovery. Further metrics indicate whether the proposed schemes address the challenges of control channel saturation, robustness to PU activity, the evaluation of CCC coverage, and control channel jamming.

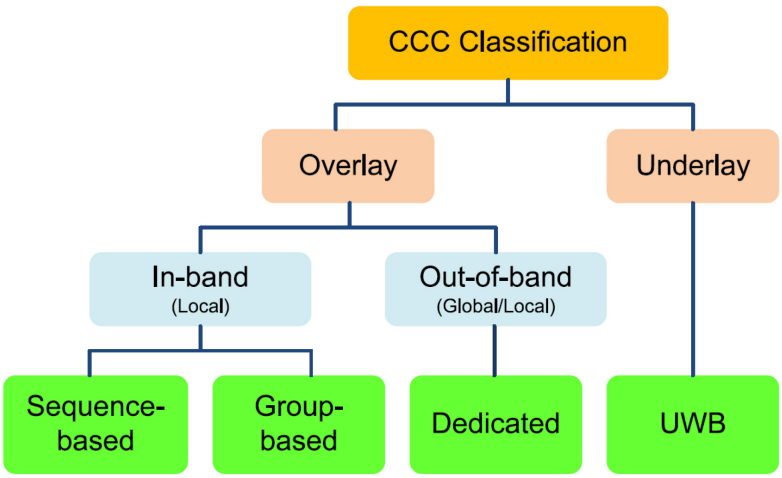



**Figure 4-18: CCC Classification [125].**

Table 1 in Ref. [126] lists the properties of all handled design schemes. In addition to those schemes, Ref. [117] proposes a distributed multi-hop UWB design for exchanging control information, which offers a discovery protocol and outperforms an in-band signalling solution. In Ref. [118], game theory is used to assign as few as possible frequency channels as common control channels in the network. Ref. [119] proposes a model to analyse CCC saturation for Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) MAC layers. A proposal how to use the CCC for configuring the MAC is described in Ref. [121]. Ref. [122] proposes a fully distributed broadcast protocol in multi-hop CRAHNs with a dynamic CCC. In Ref. [123], spectrum sensing information is transmitted to a fusion centre over a dynamically selected control channel, which saves the dedicated channel resources for a CCC without degradation of Receiver Operating Characteristic (ROC) performance. Dynamic assignment of control channels to clustered CRN is investigated in Ref. [124]. Ref. [125] describes a MAC protocol, which dynamically assigns control channels to a centralized CRN.

### 4.7.2 Challenges for the Control Channel in Military CRN

In Ref. [126], four design challenges for control channels are proposed. The first challenge is to avoid control channel saturation, the second one robustness to interferences (like PU activity), the third one is coverage, and the fourth one is security. A fifth challenge for CRN is inherently end-to-end performance.

#### 4.7.2.1 Control Channel Saturation

The control channel of a CRN has to carry different kinds of messages:

- Hello messages, for finding other nodes and for keeping connections alive;
- Topology control messages, for setting up and maintaining the topology of the network;
- Routing messages, for setting up and maintaining routes;
- Sensing information exchange messages, for sharing sensing information;
- Channel change messages, for initiating a channel change;
- Trust management information exchange messages;
- Collected knowledge exchange messages, for system-wide learning capability; and
- Probably many more, dependent on the selected algorithms.

These messages can be either proactive or reactive, meaning that they are either self-initiated (e.g., regularly sent hello messages) or just react on other events (e.g., channel change messages reacting on changes in the spectrum occupancy). All messages must be transmitted concurrently on demand with different priorities by all nodes of the network. It must be ensured that all messages can be delivered on time, which means that the control channel must possess sufficient resources for avoiding saturation. But, the more resources are dedicated to transmitting control information, the fewer resources remain for transmitting user data. Therefore, a trade-off must be found.

#### 4.7.2.2 Robustness to Interferences

As described above, control channels can be either in-band or out-of-band. In case there is a licensed out-of-band control channel, the CRN may be PU on this channel. In the civilian world this is the most promising way to avoid interferences with other users, but in the military context a dedicated control channel exhibits a Single Point of Failure (SPoF), which is subject to jamming for hostile forces. Furthermore, for technically realizing an out-of-band control channel, either the radio front-end must be able to change its frequency fast or more than one front-end is required, which may lead to co-site effects. Jamming resistance can also be achieved by using UWB signals or frequency hopping. The latter can also be an approach for robustness to interference on in-band control channels.

When using a non-hopping in-band or unlicensed out-of-band control channel, the CRN must react on an emerging interfering signal by changing the frequency as soon as the interference is detected. That requires the capability to initiate a channel change despite the presence of the signal. The channel change message must either be transmitted on a different channel, which requires a second radio front-end (as proposed in Ref. [128]) or the signal needs to have good correlation characteristics for being detected by a possibly interfered receiver.

#### 4.7.2.3 Coverage

Not all nodes in a network need to use the same control channel all the time, e.g., *via* clustering, the network can be split into several subnets using different control channels. It is only required that it must be possible to exchange control information between all nodes.

As discussed above, a control channel can be rather static and thus provide a pre-planned coverage of all nodes, or it can be dynamic and only connect few nodes on demand. While a static control channel setup is subject to non-deliberate and deliberate interference, a dynamic control channel requires more overhead for setting up connections.

Especially in mobile applications the range of the control channel must be regarded. UWB signals, for example, have a very small range and can, therefore, only be used in networks, in which the maximum distance of a node to its next neighbour is not more than 100 m [117].

#### 4.7.2.4 Security

It has already been mentioned that the control channel exhibits a SPoF, because nodes in a CRN cannot communicate without a working exchange of control information. Moreover, confidentiality, integrity, and availability are important issues for the CCC in CRN. It must be verified that control information from neighbours is not corrupted.

#### 4.7.2.5 End-to-End Performance

Control messages in CRN have different priorities. Some messages, like frequency change messages, must be transmitted extremely fast. Therefore, the network needs to have a good end-to-end performance with low message latency.

One source for latency is the forwarding of messages over several hops, if the final receiver of a message is out of the range of the original transmitter. The fewer nodes are directly connected, the more messages need to be forwarded, which consumes resources of the forwarding nodes and introduces latency to the messages. In addition to the processing latency, inter-cluster communication in clustered networks leads to further latency, as the gateway nodes, which forward the message, need to switch the transmission frequency.

In addition to the latency, also prioritization of messages plays an important role regarding performance. Especially in military networks, not only the QoS must be regarded, but also the military structures.

Furthermore, it must be planned which group communication schemes are needed (unicast, broadcast, and/or multicast).

### 4.7.3 Co-Existence Between Networks

In NATO operations, several Nations often use different waveforms in the vicinity of each other, as, for example, described in the vignette in Section 3.2.1.2. Today, interferences between those systems are avoided by giving each Nation a set of frequencies with exclusive right to use, but still there are unconfirmed

reports of interference between friendly forces. When CRNs will be fielded in the future, this exclusiveness will probably be abolished for the sake of spectrum sharing. Therefore, new ways of avoiding interference between systems from different Nations need to be introduced.

A promising approach is that, even though networks from different Nations do not exchange user data, control information might be exchanged to ensure co-existence alongside each other [129]. This exchange requires some kind of CCC, and with that, identical protocols, as well as the capability to synchronise with each other, become compulsory. Therefore, a common standard for such CCC is necessary. In the civilian world, there are already task groups dealing with this topic (e.g., IEEE 802.19 and 1900.2). Their work includes existing waveform standards like IEEE 802.11, 802.15, 802.16h, and 802.22. It should be noted that 802.11af and 802.22 already aim at using CR techniques.

Co-existence between networks implies that those networks automatically manage to share the available spectrum, while avoiding interferences concerning both user and control data, apart from the co-existence control information. Possible spectrum sharing solutions include using different frequencies, using TDMA on the same frequency, or achieving orthogonality on the PHY layer.

Such an important feature, available to many different kinds of communication systems, appears to be a good point for hostile forces to attack. Therefore, security must be regarded when preparing the co-existence standard.

### 4.7.4 Recommendations

#### 4.7.4.1 Design

As depicted in Figure 4-18, there are basically two approaches for control channel design, overlay and underlay control channels. Underlay is associated with UWB signals, which are robust but have low range. Therefore, underlay can be recommended for a rather static infrastructure network setup with small distances between the nodes, e.g., in a base camp.

In mobile applications, overlay control channels are required. Overlay channels can have a large range but are more vulnerable to interferences. As the control channel exposes a SPoF, it needs to be designed carefully. For example, in a centralized system the central entity can be regarded as SPoF. A proposal for a distributed CCC is described in Ref. [122]. Moreover, using a fixed physical channel is not recommended as it can be easily jammed. On the other hand, a purely adaptive control channel, which can dynamically evacuate interfered frequency bands, impedes neighbour discovery.

A possible solution could be frequency hopping. Frequency hopping waveforms are more difficult to jam than fixed frequency waveforms. Nevertheless, they can be discovered by all nodes that know the used frequencies or the hopping pattern. The hopping pattern must consider heterogeneous channel availability. An example for an adaptive frequency hopping algorithm is given in Ref. [130].

The question of whether a static or a dynamic CCC is advantageous, depends on the amount and the frequency of control traffic. A static CCC requires that all devices know the same hopping pattern, while a dynamic CCC only requires that the used frequencies are known. One or more of these frequencies are observed, so that it can take several time slots until transmitter and receiver have found each other. In an infrastructure network, which is rather static and therefore does not require many updates on topology and frequency availability, a dynamic CCC might be sufficient. For a mobile network operating in a hostile environment, there might not be enough time to negotiate a CCC, therefore, a static CCC appears to be advantageous.

Figure 4-19 gives a visual impression of how to characterize static and dynamic CCC regarding performance, flexibility, and the danger of saturation. While a dynamic CCC can flexibly adapt to the information exchange needs and thus avoid saturation, the negotiations for setting up the CCC impair the performance. Purely static CCCs do not need such negotiations but, on the other hand, cannot adapt to varying control information exchanges.

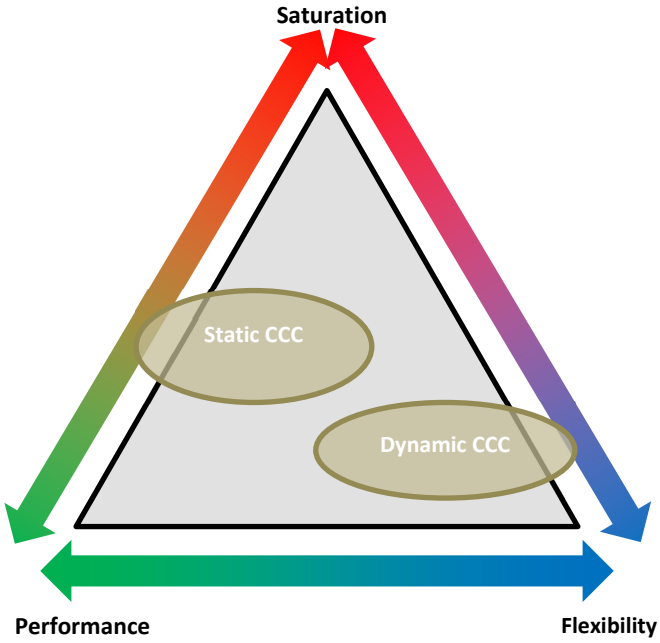



**Figure 4-19: Comparison of Static and Dynamic CCC.**

In general, it might be an option to adapt the CCC to the current situation, i.e., to use a different CCC design in a jamming situation than in a highly mobile situation.

#### 4.7.4.2 Control Channel Saturation

For avoiding saturation, sufficient bandwidth must be dedicated to the control channel. The analysis of control channels regarding saturation is described in Ref. [119]. In Ref. [120], a proposal to divide the control channel into several sub-channels, which can be dynamically allocated for a transmission, is described.

In general, a variable bandwidth allows for a dynamic trade-off between control and user data but is a challenge for topology construction. Dependent on the environment, there could be channels with different bandwidths and link quality or a combination of smaller adjacent channels.

#### 4.7.4.3 Robustness to Interferences

As the control channel is crucial for maintaining the system, the evasion of deliberate or undeliberate interference has high priority in the design of the CCC. Especially a suddenly appearing signal, like a PU starting to use his channel, requires an appropriate reaction of the system. This reaction must be common for all affected nodes, which means that they e.g., initiate the evacuation to a new channel at all nodes at the same time. Due to the interference, it is usually not possible to negotiate a new common frequency when this interference has been detected. Therefore, it is important that reactions on upcoming interferers must be pre-planned. Then, it is sufficient to initiate the common evacuation.

One solution for this initiation process is emitting signals with good correlation characteristics, which can be detected despite the interference. When using CDMA with predefined spreading codes, different notifications are possible. When two radio front-ends are available, the notification regarding the evacuation of the interfered channel can be given *via* the second front-end on a free channel. A similar idea to this is presented in Ref. [128], where only one front-end is assumed, but with a wideband receiver. This wideband receiver segments the spectrum into smaller channels *via* software, thus obviating the co-site effects of two front-ends. Nevertheless, the distance between the used channels is limited by the capabilities of the receiver, e.g., bandwidth, hardware filters. A frequency solution is proposed in Ref. [131]. There, a multiple rendezvous control channel is presented, which assumes different hopping patterns of the receivers known to the transmitters, so that multiple control messages can be sent at one time.

#### 4.7.4.4 Coverage

The nodes reached by a CCC determine its coverage. If there is a dynamic CCC, coverage will be just a communication pair. In a clustered network, there will be a control channel for each cluster, and the coverage is inherently limited to this cluster. Consequently, it is the task of the clustering algorithms to take care of the coverage.

In a UWB network, coverage can be extended using multi-hop communication. A corresponding protocol is proposed in Ref. [117].

The inclusion of legacy devices into a CRN, as, for example, described in the vignette in Section 3.2.2.2, is always dependent on the capabilities of those legacy devices. A general approach for their inclusion is the development of a proxy for that purpose.

#### 4.7.4.5 Security

Avoiding a SPoF in CCCs is crucial for CRN. According to Ref. [126], possible solutions for this are spread spectrum techniques, dynamic control channel allocation, and the use of jamming-resilient key distribution techniques for protecting vulnerable information (e.g., location). Spread spectrum techniques are a general measure for avoiding jamming but become inefficient when the spreading sequences get known to the jammer.

Integrity of control information can be verified *via* trust management. This is elaborated in detail in Section 4.6.

Further security aspects in networks are addressed in other groups, so we refer to their reports and to literature for more information.

#### 4.7.4.6 End-to-End Performance

As CRN technology – in contrast to CR technology – focuses on end-to-end optimization, one important aspect for the CCC is end-to-end performance. As elaborated in Section 4.7.4.1, a static CCC is set up faster than a dynamic CCC, because there is no need to negotiate or identify the used frequency band.

Also, clustering has a large impact on end-to-end performance, as frequency changes at cluster boundaries introduce latency. Solutions for this might be using a second front-end (for communicating on two frequencies in parallel, if not needed for channel evacuation as described in Section 4.7.4.3) or larger clusters. Larger clusters imply fewer clusters and, therefore, fewer boundaries, but on the other hand, they require more transmission power. Moreover, larger clusters with more devices need more control messages for cluster-internal organization, which needs to be regarded when looking at control channel saturation.

One effect of bad end-to-end performance is control message latency. The impact this latency has may vary dependent on the type of message. For example, late topology control or routing messages may lead to

significant latency or loss of wrongly routed messages. Delayed hello messages should not have direct impact, but the exclusion of a node from the network due to several omitted hello messages must be avoided. Late sensing information exchange messages may lead to wrong channel change decisions. Rather critical are late channel change messages, as they may lead to exclusion of nodes from the network. Delayed trust management information exchange may lead to wrong trustworthiness decisions. In order to minimize the impact of message latency, prioritization of message types is important. Also, the support for unicast, broadcast, and multicast may allow for systematic distribution of control information.

## 4.8 SOFTWARE DEFINED NETWORKING TECHNOLOGY

Rapid development in the field of Software Defined Networking (SDN) is evident within the scientific literature. For example, the IEEE Xplore-database had 483 SDN related articles in 2012, whereas the same query yielded a total of 2130 articles in 2016 (as of 14.10.2017).

SDN is a paradigm for centrally controlling the network traffic by programmable procedures. With SDN, network is managed and controlled through the use of software. Network devices merely forward traffic. The SDN paradigm has evolved from the need to manage traffic within huge datacentres and has subsequently been expanded to fixed networks including corporate wide as well as multi-national data networks [132], [133].

The basic principle of SDN is to separate control traffic from data into separate control and data planes, whereby routers within the data plane can be simplified to switches controlled by the software of the control plane [134], [135], [136]. The SDN technology is seen to alleviate network planning, operating and management processes. Research has also considered deploying this technology in a partial manner leading to hybrid-architectures, where only a portion of the network devices adhere to the SDN principle (typically at the edges of the network) [137].

As can be seen in the Figure 4-20, the architecture comprises two major entities, the controller and the Data Forwarding Element (DFE). Such an architecture supports three main tenets, namely those of:

1) Separation of the control logic and data forwarding;
2) Logically (not necessarily physically) centralized control; and
3) Programmability of network functions.

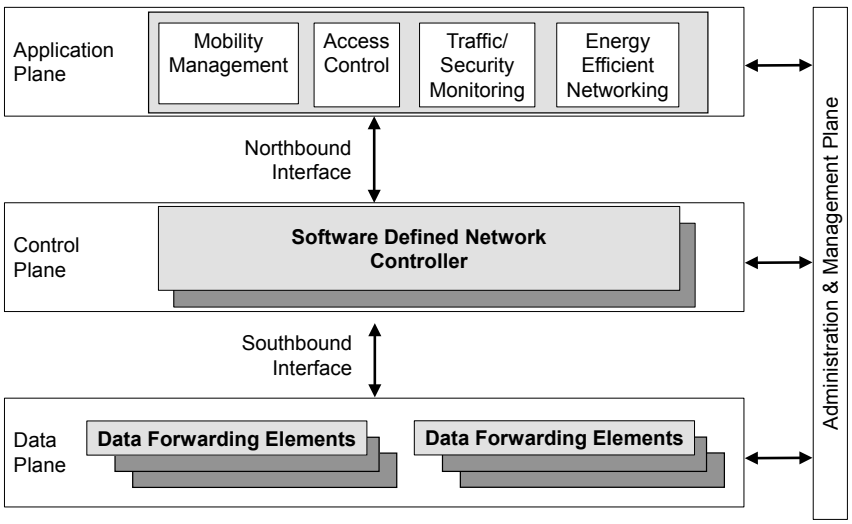



**Figure 4-20: Basic Principle of the SDN Architecture.**

Logically centralized control has been proposed to incorporate additional features, for example, to distribute the control function over the network in order to avoid single points of failure. Distributed control could be robust and resilient and could also dynamically adjust to changing network topologies [138].

A concept of Network Function Virtualization (NFV) is a similar concept aiming to implement network functions through the use of general-purpose computing devices. Such virtualized functions could be load-balancing, network security, and intrusion detection. SDN together with NFV could be used for dynamic network resource (e.g., radios) management and service orchestration [138]. Network slicing means setting up multiple virtual client networks within a shared physical network, whereby a CRN could serve multiple communities of interest through network slicing. Both SDN and NFV support network slicing [135], [139].

The three driving principles of SDN, in essence, mean that the control of the networking functions, most importantly the routing or forwarding of data packets, is removed from routers and switches into more generally available centralized CPUs. Each of such controllers can control the packet forwarding in a large number of routers and switches. The technology has been realized in several initiatives and standards, such as Forces (RFC 3746, 2004) and OpenFlow (Open Networking Foundation, ONF). OpenFlow is the most popular implementation framework in the industry.

### 4.8.1 Software Defined Networking in Wireless Networks

Originally, SDN technology has been aimed for wired infrastructure. However, recently ONF has been advocating the idea of extending the SDN control all the way to the wireless edge routers [140]. The idea is to be able to optimize the RAN resources and to improve the QoE of mobile users and applications. Following this idea, at least MobileFlow [141], SoftCell [142], and SoftRAN [143] architectures have been proposed. It should be noted that in these technologies the OpenFlow (based) messaging is applied at the very edge of the wireless network only. SDN control messages do not reach the Mobile Nodes (MN). Among the first papers to really propose to extend the OpenFlow signalling into the wireless (i.e., SDWN) are Refs. [144], [145], and [146], which also provide an implementation of the proposed architecture.

Both the challenges and possible benefits of using SDN in the wireless environment have been studied, e.g., in Ref. [147]. On the possible benefits (or opportunities), SDN controllers can help co-located base stations[1] to plan for their frequency and power use in order to minimize mutual interference. Mobility issues can be solved by the possibility to enhance user connectivity and QoS and by allowing SDN controllers to decide the most suitable connection on behalf of the user (see also Ref. [148]). In a sense, SDN could allow more complex connectivity management to the terminals than what is possible by the terminal itself. Related to this issue, SDN can also aid the terminal in making soft handovers between networks, e.g., by duplication of the packets sent during handover process. For example, mobility between heterogeneous wireless networks using SDN technology (OpenFlow) is addressed in Ref. [145], where the SDN signalling is extended to the end nodes (see Figure 4-21). The purpose is to aid the MN mobility between heterogeneous networks. MN also send network status information and measurements to the coordinator using the OpenFlow signalling.

The solution is verified in experimental setup and performance measurements, including estimations of OpenFlow overhead. A similar solution, with experimental setup, for managing node mobility in load aware manner is proposed in Ref. [149], although here the SDN signalling reaches only the SDN aware-access points, not the end nodes. Both layer 2 (within network) and layer 3 (between IP networks) mobility assisted with OpenFlow signalling is proposed in Ref. [150].

[1] "Co-located base stations" is a term rather used in civilian fixed infrastructure-based networks. In a military CRN, a multi-channel node could be considered in a similar manner.

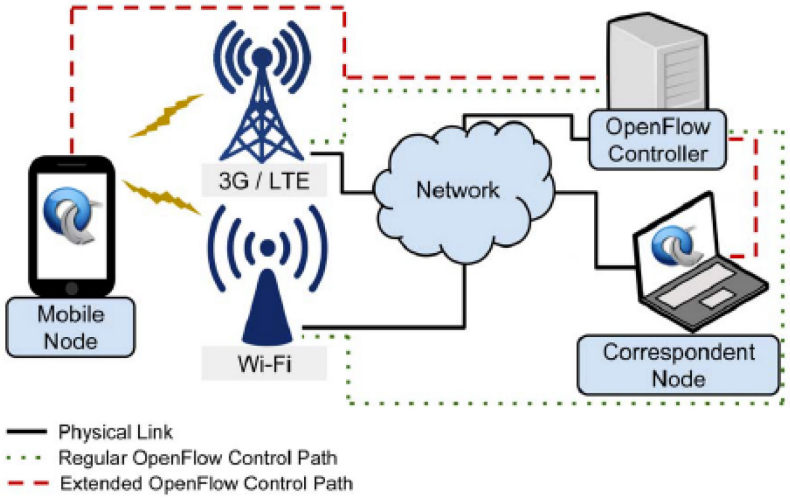



**Figure 4-21: SDN Signalling to the Mobile Nodes [146].**

The challenges of using SDN in the wireless include the concept of slicing, which may turn out to be a difficult operation, due to limited number of orthogonal channels in the first place [147]. TDMA would require coordination and accurate timing between base stations (and SDN coordinators), while frequency division requires to sacrifice some of the bandwidth for guard bands. Random channel access, on the other hand, cannot address fairness between users and networks. Another problem is related to monitoring of the channel and network state as well as the overall network topology, which are considerably more difficult tasks in the wireless than in the wired network. This fact may prevent the SDN coordinator(s) to make fully justified decisions related to traffic engineering and QoS/QoE.

The authors of Ref. [151] and Ref. [152] deal with SDN as a way to perform mesh routing in a centralized way. The routing process is assisted with an SDN coordinator, which is supposed to have a good, overall view of the network topology at all times. It can receive the neighbourhood information from all the mesh nodes and construct the network topology from that information. This reduces the signalling and leads to faster route convergence. In this solution, it is always the responsibility of the controller to make route decisions; the hello messaging is used only to discover the neighbourhood of each node. One can ask whether fast route convergence or effective ad hoc routing is needed in the, presumably, static network, such as typical mesh, which operates as a backbone for mobile nodes.

Message and purpose in Ref. [153] are the same as in previously mentioned papers, i.e., to use the SDN controller as a mesh routing assistance entity. OpenFlow is seen as a tool to simplify mesh network management from a central server, in this sense the SDN controller could also be used to host the cognitive controller. The possible downside is that if the control is completely given to a central controller, it may not be always available, especially in the wireless environment. Anyway, this paper describes test network case studies on the performance regarding balancing the traffic between gateways (traffic engineering).

Also, Ref. [148] proposes an architecture for using OpenFlow, in particular, in the WMN, in order to bring in more flexible routing and mobility between networks. Their proposal takes into account several special requirements of the wireless networks, including the need to react to sudden topology changes, the lack of the clear notion of a point-to-point link, and the need to take into account the lower bandwidth of wireless communications. The architecture is depicted in Figure 4-22, where NOX refers to the network operating system.

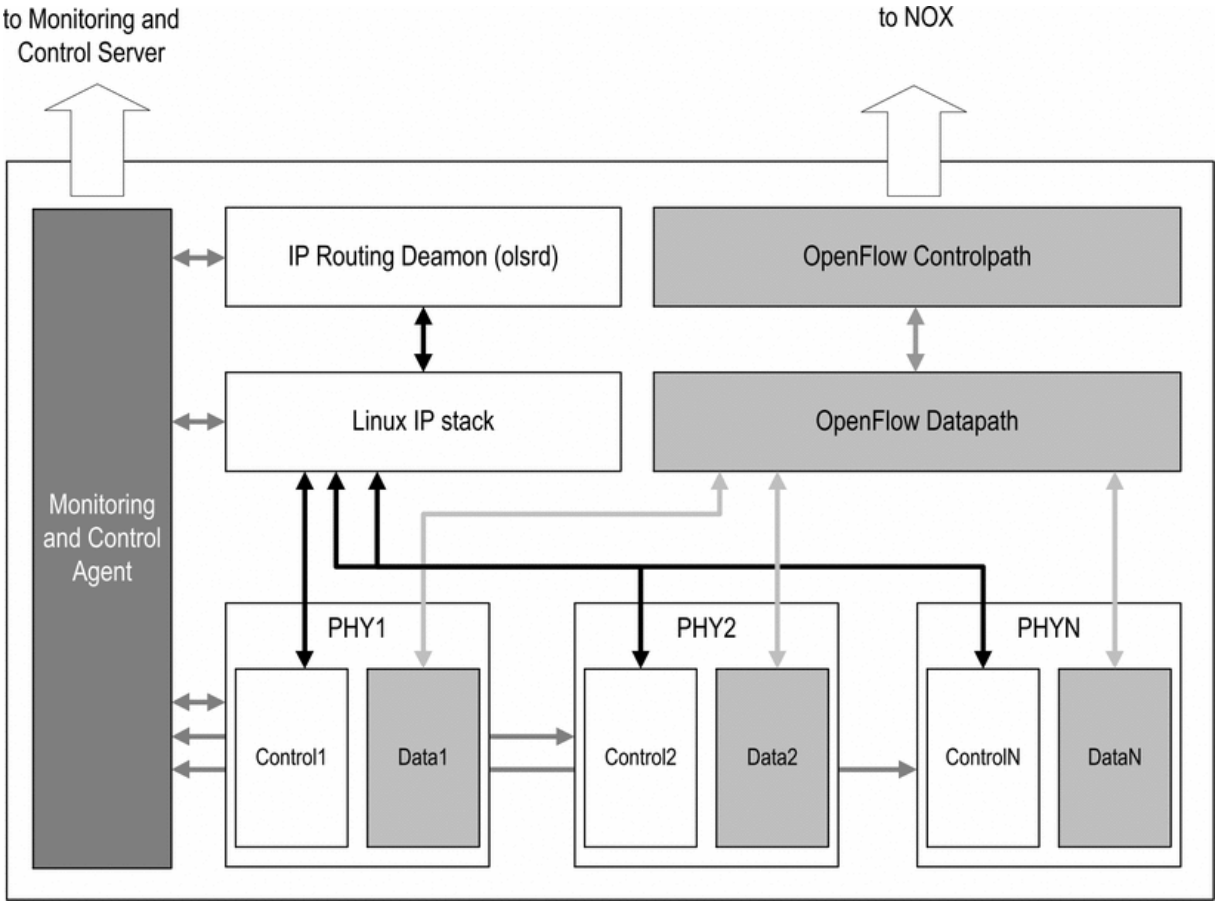



**Figure 4-22: SDN-Enabled Mesh Node Architecture, by Dely *et al.* [148].**

Each of the wireless interfaces is split into two virtual parts. The parts are separately used by the data and control paths. Experimentation with rather simple network setup revealed some potentially serious problems in the OpenFlow performance. When compared to standard OLSR routed network, the achievable throughput diminished from about 20 Mbits/s to about 13 Mbits/s, and even more if the number of forwarding rules were added. Similarly, the additional control overhead caused by OpenFlow rule implementation rises rapidly with increasing number of rules needed. This limits the scalability of the OpenFlow-based solution. On the other hand, in Ref. [154], the overhead due to OpenFlow is not considered a serious problem. It seems that the added value of the SDN solution needs to be considerable to justify the loss in overall network performance.

### 4.8.2 Architecture Proposals Combining Software Defined Networking and Cognitive Radio Networks

A general proposal for LTE spectrum agile networks is described in Ref. [155]. The authors propose and prototype a software defined network architecture with the OpenFlow protocols for heterogeneous network spectrum sharing in the TV white space (see Figure 4-23). The purpose is to utilize SDN/NFV to manage interferences and to enable dynamic spectrum sharing. No attention is given to other networking aspects in this paper.

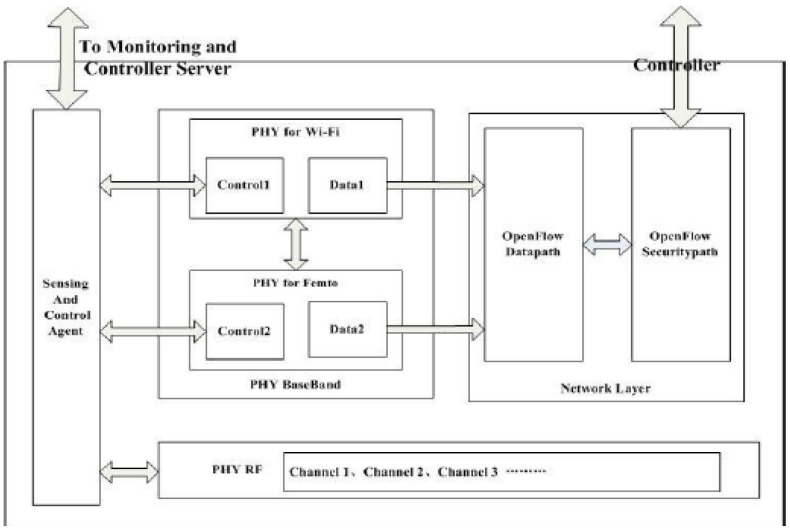



**Figure 4-23: Data/Control Decouple Architecture, Proposed by Sun *et al.* [155].**

Another proposal for combining SDN and CRN for the purpose of spectrum management is given in Ref. [156]. The following is a direct quote summarizing the idea:

> "*Cognitive networks leverage from CRN, that constitute its radio part, to provide promising solutions for spectrum scarcity by using dynamic spectrum sharing mechanisms. SDN, on the other hand, increases networking dynamism by introducing programmability in network elements and logically centralizing the control plane of the network".*

To that end, a framework for Software Defined Cognitive Networks (SDCoN)[2] is proposed, which merges the concepts of SDN and cognitive networking for dynamic resource sharing in wireless networks. A mapping of CRN and SDN is proposed (Figure 4-24). The elements of both architectures are grouped into three layers, end-to-end goals, cognitive process, and Software Adaptable Network (SAN).

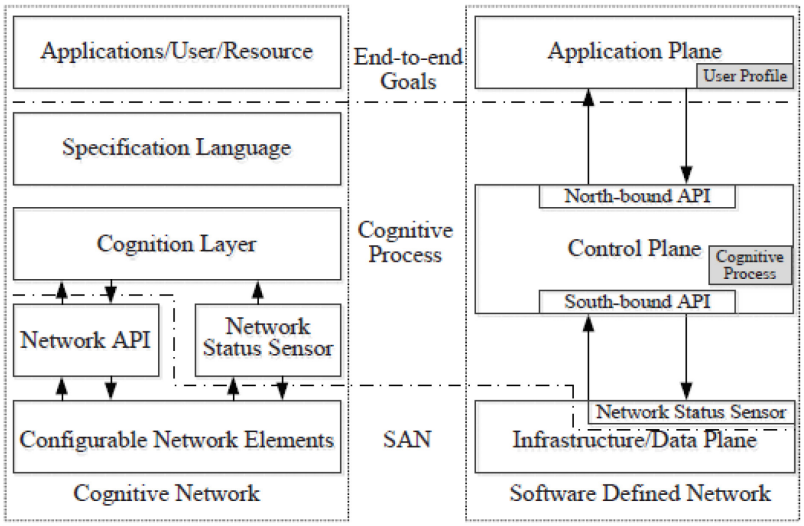



**Figure 4-24: Cognitive Network and Corresponding SDN Architecture, as Proposed by Ahmad *et al.* [157].**

[2] The IST-124 on Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency final report recommendations suggest cognitive SDN.

The operation is described as follows [157]:

> *"In SDCoN, a network operating system or the SDN controller maps the entire network to services and applications that are implemented on top of the control plane. The end-to-end goals are realized in the form of SDN applications. Similarly, the cognitive engine is implemented in the SDN application plane that receives the network status information from a cognitive process module in the controller."*

This architecture is further developed in Ref. [158]. The authors propose and implement an OpenFlow-based CRN. In this architecture (see Figure 4-25), the Cognitive Engine (CE) is an application at the control plane and has well-defined interfaces to radio and node resources, as well as to the applications.

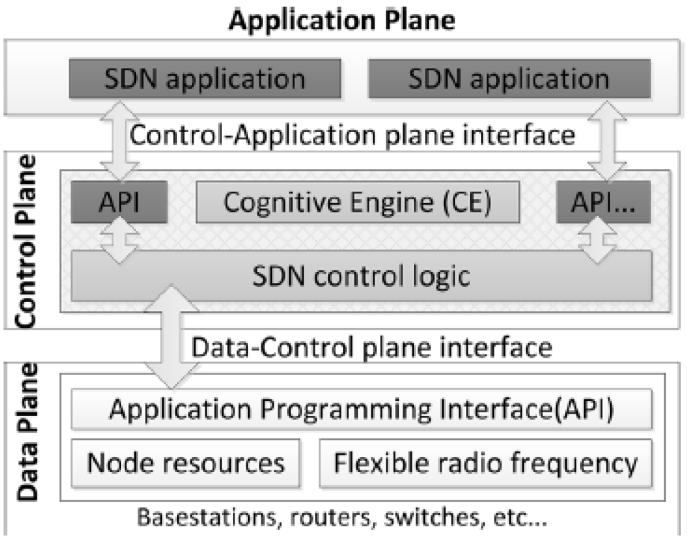



**Figure 4-25: SDN-Based CRN Architecture, by Namal *et al.* [158].**

With this architecture, implemented on modified WARP platforms, OpenFlow-enabled cognitive base stations are prototyped. CE implemented on BSs can dynamically control the use of radio resources. Furthermore, a centralized manager, an SDN controller, manages the whole infrastructure. In this particular case study, no attention is given to network level cognitive operations, only on radio resource management. Nevertheless, the architecture indicates the possibilities given by separating data and control planes; by abstracting the underlying connections with defined APIs, the control logic has more freedom in its implementation and operations.

A proposal for a network edge architecture including SDR components, SDN controller and Mobile Edge Cloud (MEC) controller, which have the intelligence to manage the whole radio, is described in Ref. [159]. Figure 4-26 shows the radio architecture, where it is evident that the MEC controller is in major role. In this architecture, MEC controls the radio layer through the SDR controller, the SDN layer through the SDN controller and, also, the application through the Application manager:

> *"…modules gather the measured information at each layer respectively, then aggregate and transfer them to the MEC controller through specified and generic interfaces. More precisely, based on received updates from waveforms, SDN and application layers, the MEC controller decides whether a radio parameter should be modified at the waveform level (i.e., adding FEC, for instance), or switching to another interface at the virtual switch via the SDN controller or even modifying the Application parameter or the service chain to adapt to the underlying conditions."* [159]

Based on this description, MEC-C is designed to control only what happens inside the radio platform.

Actually, in Ref.[159], the radio architecture, as given in Figure 4-26, only resides in the node similar to base station or access point. The user equipment does not have the same internal structure, save for the several waveforms (see Figure 4-27). Besides, the actual intelligent decision making in this PoC is not performed by any software component but by an operator. The only thing which is actually proven, is that the relevant information can be made available by the interfaces shown.

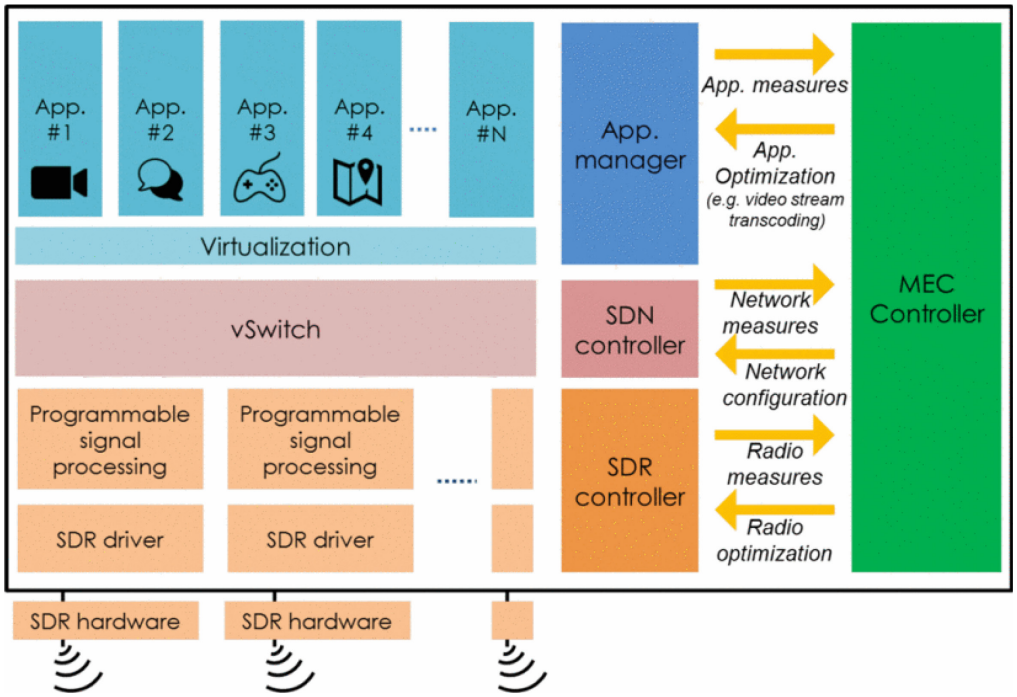



**Figure 4-26: Radio Architecture, Proposed by Phemius *et al.* 2016 [159].**

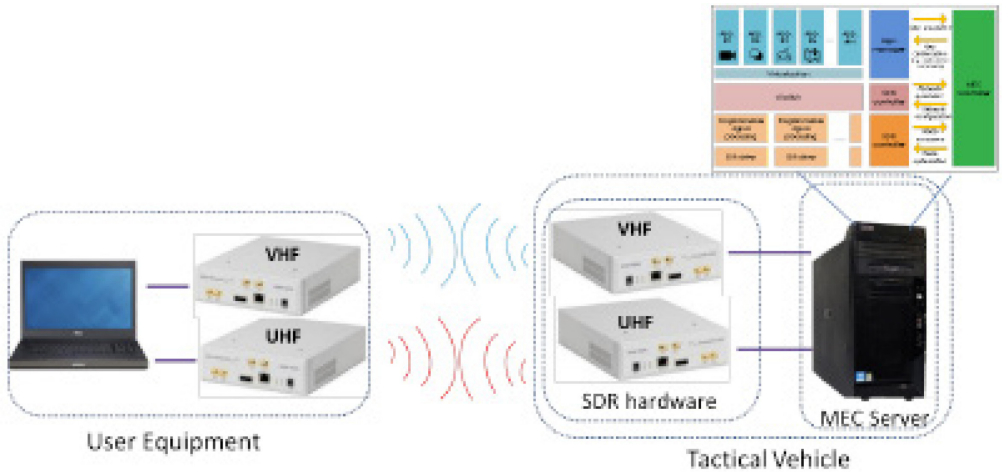



**Figure 4-27: Proof-of-Concept Arrangement [159].**

The purpose is eventually to show that the decision affecting the QoS can and should be made locally by an MEC, in this case.

### 4.8.3 Challenges and Benefits to Tactical/Military Use

In the tactical context, many connections are relying on wireless, causing congested and occasionally unreliable connections. Therefore, the SDN-like control architecture may not always be suitable or possible. In military and tactical context, the first issue is to resolve the dependency on a single point of failure, as represented by a single controlled architecture of SDN. Distributed architectures have been proposed but they are mainly suitable for datacentre type installation, due to the heavy data-sharing burden that they impose [138].

In a modern warfare, the operations typically include multiple operators, even across multiple nations. If some of the network capacity is shared between nations, the question comes up whether the SDN architecture is able to manage the resulting complexities. A similar question arises when tactical networks experience high mobility, meaning that the network infrastructure is most likely under constant change, thereby, a stable network topology cannot be guaranteed [160].

Furthermore, there are issues related to cyber security and defence. This is a particular issue within the category "single point of failure": If an attacker manages to breach the system through the controller, it would make the whole controlled network section vulnerable. Cyber security of SDN is under research.

In theory, SDN would provide benefits to the operation and management of the tactical networks. These include [160]:

- Better and more detailed, and most importantly, more agile management of data traffic. This means e.g., more agile priority rules, etc., for the case of network congestion or for times when operational requirements are changing.
- Dynamic policy control of the network, so that it (they) may better adapt to local conditions (or requirements of the mission). Note that policies are an important factor in the management of CRNs as well, and there is clearly some coherence here.
- If the traffic management by SDN controllers can indeed be extended towards tactical (wireless) edge in a reliable manner, this would bring clear benefit due to more reliable and "situation aware" network functionality.

## 4.9 OPEN COGNITIVE RADIO NETWORK SIMULATORS

CRN offers various dimensions of configurable parameters at all layers of the Open Systems Interconnection (OSI) model. At physical layer (layer 1), this includes spectrum sensing (e.g., energy detection, feature detection, sensing time), dynamic spectrum access (e.g., overlay, underlay, interweave), modulation scheme (e.g., QAM[3], OFDM, SC-FDM, DSSS, FH), forward error correction (e.g., block coding, convolutional coding, turbo coding), and other parameters (e.g., frequency, bandwidth, power). At data link layer (layer 2), this includes media access control (MAC) (e.g., CSMA, OFDMA, TDMA, Aloha), logical link control (e.g., flow control, error control, ARQ) and topology control (e.g., clustering). At network layer (layer 3), this includes network protocol (e.g., IPv4, IPv6), routing algorithms (e.g., OLSR, AODV, OSPF). High-fidelity simulation of CRN should provide the flexibility to adjust manually or autonomously these configurable parameters according to the user needs and the electromagnetic environment toward end-to-end objectives.

The CRN software framework should provide libraries of components at all layers of the OSI model (e.g., modulation schemes, protocols, routing algorithms) along with realistic channel models for simulating a high number of nodes. At the same time, the CRN software framework should provide interfaces with hardware platforms for testbed evaluation and Hardware-In-the-Loop (HIL). High-fidelity simulation means

[3] Due to the number of acronyms in this paragraph, the acronyms are not expanded. Instead, we refer the reader to the List of Acronyms.

that there is no abstraction at the level of data link layer, physical layer and that it includes realistic channel models. The CRN software framework should also provide the possibility to reuse the same code either in a testbed mode with hardware platforms (small number of nodes with real-time scheduling), in an emulation mode (HIL with real-time scheduling) or in a simulation mode with realistic channel models (high number of nodes). A list of CRN software frameworks and SDR hardware along with experiments is provided in Refs. [132], [161], and [162].

Unfortunately, there is no such software framework in the research community. Several types of open-source software frameworks can be identified for the high-fidelity simulation of CRN. On one hand, radio simulators such as GNU Radio or CogWave provide many signal processing blocks and modulation schemes for the physical layer. However, they provide only basic MAC functionalities for the data link layer and do not provide functions for upper layers. On the other hand, network simulators such as OMNeT++ and ns-3 provide libraries for the internet stack (e.g., TCP, UDP, IPv4, IPv6), wired and wireless protocols (e.g., Ethernet, PPP, IEEE 802.11, IEEE 802.16, LTE), MANET protocols, mobility, and many other protocols and components. They offer real-time schedulers for integration into testbed and virtual machine environments. Moreover, they provide fairly accurate representation of the layers above and including the data link layer. However, they abstract significantly the physical layer, the channel models and some parts of the data link layer.

In the following, we review some open-source frameworks and evaluate the layers at which they operate for high-fidelity simulation of CRN.

### 4.9.1 GNU Radio

GNU Radio [163] is an open-source software framework which provides signal processing blocks to implement software radios. The GNU Radio framework is built on a combination of Python and C++. The main signal processing blocks are written in C++ and integrated with Python using simplified wrapper and interface generator (SWIG). The GNU Radio Companion provides a graphical user interface (GUI) to connect GNU Radio blocks and to design flow graphs similar to Simulink. Many signal processing blocks are available such as filters (FIR, IIR), Fourier transforms (DFT, FFT), equalizers, modulation schemes (GMSK, PSK, QAM, OFDM), error-correcting codes (Reed-Solomon, Viterbi, turbo codes), realistic channel models (AWGN channel, fading channel, frequency-selective fading, hardware impairments), interfaces with hardware (USRP, OsmoSDR platforms). However, the GNU Radio framework provides only basic MAC functionalities (simple CSMA MAC [164]) at the data link layer and do not provide functions for upper layers. The GNU Radio framework can be interfaced with other applications by named pipes (FIFO) or virtual network interfaces at data link layer (TAP) or network layer (TUN). Most works in the literature consider to interface GNU Radio with the Click modular router software (CSMA/routing) [165] or to implement time-critical MAC functionalities (Bluetooth, IEEE 802.11) in the field programmable gate array (FPGA) of the hardware platform [166].

### 4.9.2 CogWave

CogWave [167] is an open-source software framework aiming at developing CR modulation schemes. The CogWave framework uses the Qt framework, the communications library IT++, the USRP universal hardware driver (UHD) and other libraries to enable real-time transmission between USRP devices. The CogWave framework provides many modulation schemes, such as the multi-channel DAA-OFDM, the DADS modulation scheme with a short spreading sequence, and other modulation schemes ported from the GNU Radio framework (OFDM, BPSK, QPSK, GMSK, CPFSK, etc.). Compared to the GNU Radio framework, the CogWave framework is able to reconfigure the modulation scheme during run-time (e.g., switching from DADS to multi-channel DAA-OFDM in the presence of a jammer) and allows precise timing control for burst transmissions (FDD and TDD). The CogWave framework can be interfaced with other applications by named pipes (FIFO) or virtual network interfaces at data link layer (TAP) or network layer (TUN). However, the CogWave framework does not provide functions for the data link layer and upper layers.

### 4.9.3 OMNeT++

OMNeT++ [168] is a discrete-event network simulator, which provides C++ libraries and model frameworks to support various types of networks (e.g., wireless ad hoc networks). The INET framework contains models for the wired protocols (PPP, Ethernet, etc.), wireless protocols (IEEE 802.11, IEEE 802.16, IEEE 802.15.4, etc.), routing protocols (OSPF, AODV, DYMO, DSDV, DSR, OLSR, etc.), network layer (IPv4, IPv6, ARP, etc.), transport layer (TCP, UDP, SCTP, RTP, etc.), application layer (HTTP, DHCP, Video, Voice, P2P, etc.). A CR extension to the OMNeT++ framework has been developed in [169]. The OMNeT++ framework provides strong GUI support for simulation visualization. It also supports real-time simulation by the real-time scheduler, which synchronizes the simulation time with the computer system time. Hardware interfacing is supported by a real-time socket scheduler and a raw internet socket connected to an underlying physical interface. The real-time socket scheduler waits for incoming messages from an external device and sends outgoing messages to the same device. However, the OMNeT++ framework abstracts significantly the physical layer, the channel and some parts of the data link layer.

### 4.9.4 Ns-3

Ns-3 [170] is a discrete-event network simulator which provides C++ libraries of network simulation models wrapped in Python. The ns-3 framework provides models for wired protocols (PPP, Ethernet, etc.), wireless protocols (IEEE 802.11, IEEE 802.16, LTE, etc.), routing protocols (OSPF, AODV, DSDV, OLSR, etc.), network layer (IPv4, IPv6, ARP, etc.), transport layer (TCP, UDP, etc.), application layer (HTTP, etc.). A CR extension to the ns-3 framework has been developed in Ref. [171]. This extension is based on the CR extension to the ns-2 framework [172]. Other CR extensions to the ns-2 and ns-3 framework have been developed in Refs. [173], [174], [175]. The ns-3 framework supports real-time simulation by the real-time scheduler. Hardware interfacing is supported by a raw internet socket connected to an underlying physical interface. However, the ns-3 framework abstracts significantly the physical layer and the channel.

### 4.9.5 CORE

CORE (Common Open Research Emulator) [176] is an open-source framework for emulating networks on one or more PCs. The CORE framework emulates the network layer (IPv4, IPv6, etc.), routing protocols (OSPF, etc.), transport layer (TCP, etc.) and above layers using virtual network stacks in the Linux operating system. The emulation is controlled by and easy-to-use Tcl/Tk GUI. Because the CORE framework is a live-running emulation, CORE networks can be connected in real-time to physical networks. However, the CORE framework abstracts significantly the data link layer, the physical layer and the channel.

### 4.9.6 EMANE

EMANE (Extendable Mobile Ad hoc Network Emulator) [177] is an open-source framework which provides C++ libraries of network simulation models wrapped in Python. The EMANE framework provides models for wireless protocols (IEEE 802.11abg, etc.). However, the EMANE framework abstracts significantly the channel and the physical layer, which is based on BER *vs.* SNR curves, instead of actual transmitted IQ samples. The EMANE framework does not provide interfaces with hardware devices.

### 4.9.7 Extension of Open-Source Frameworks for the High-Fidelity Simulation of Cognitive Radio Networks

This extension, shown in Figure 4-28, requires either the development of the data link layer, the physical layer and the channel into the network simulators (OMNeT++, ns-3) or the fusion of the radio simulators (GNU Radio, CogWave) into the network simulators. For the first case, some works in the literature have proposed different approaches. In Ref. [178], the authors propose an accurate representation of the physical layer of IEEE 802.11 as well realistic channel models in the ns-3 framework. In Ref. [179], the authors propose a high-fidelity simulator, including the data link layer, physical layer, and realistic channel models in

the OMNeT++ framework. However, these works do not provide interfaces with hardware devices to test in a real environment (testbed mode) or in an emulation mode for HIL. Moreover, they do not provide the flexibility to replace the data link layer and the physical layer. In Ref. [180] and Ref. [181], the authors propose a high-fidelity network emulation simulation testbed using a combination of a new framework called CREATE (Cognitive Radio nEtworking ArchiTecturE), with the CORE framework, the EMANE framework (IEEE 802.11abg) or the GNU Radio framework [182]. However, the CREATE framework is not an open-source framework and does not provide the flexibility to replace the data link layer and the physical layer.

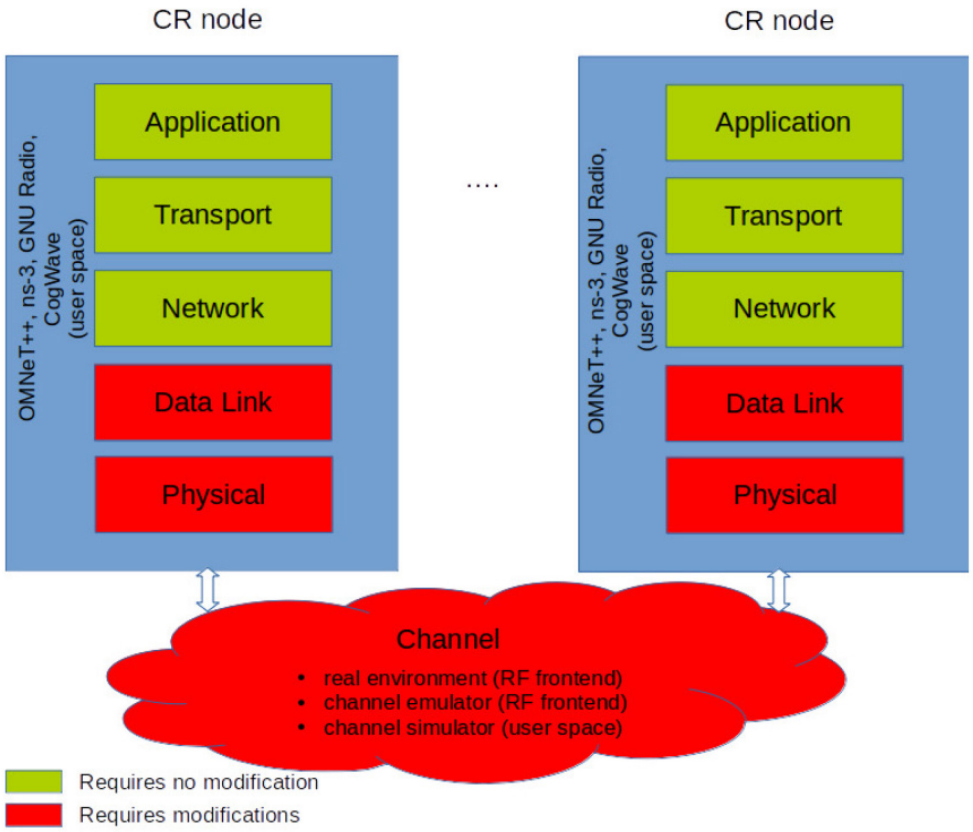



**Figure 4-28: Extensions of Open-Source Frameworks [183].**

### 4.9.8 Combinations of Open-Source Frameworks for The High-Fidelity Simulation of Cognitive Radio Networks

The combination of open-source frameworks at the network layer is given in Figure 4-29. The layers above and including the network layer are provided by the network simulators (OMNeT++, ns-3). The layers below the network layer are provided by the radio simulators (GNU Radio, CogWave). The network and radio simulators are connected by a UNIX socket, named pipe (FIFO), virtual network interface (TUN/TAP), or DLEP interface [184]. The combination at the network layer requires the development of the data link layer in radio simulators (GNU Radio, CogWave). Indeed, the GNU Radio framework provides only basic MAC functionalities (simple CSMA MAC [164]) at the data link layer. The CogWave framework does not provide functions for the data link layer.

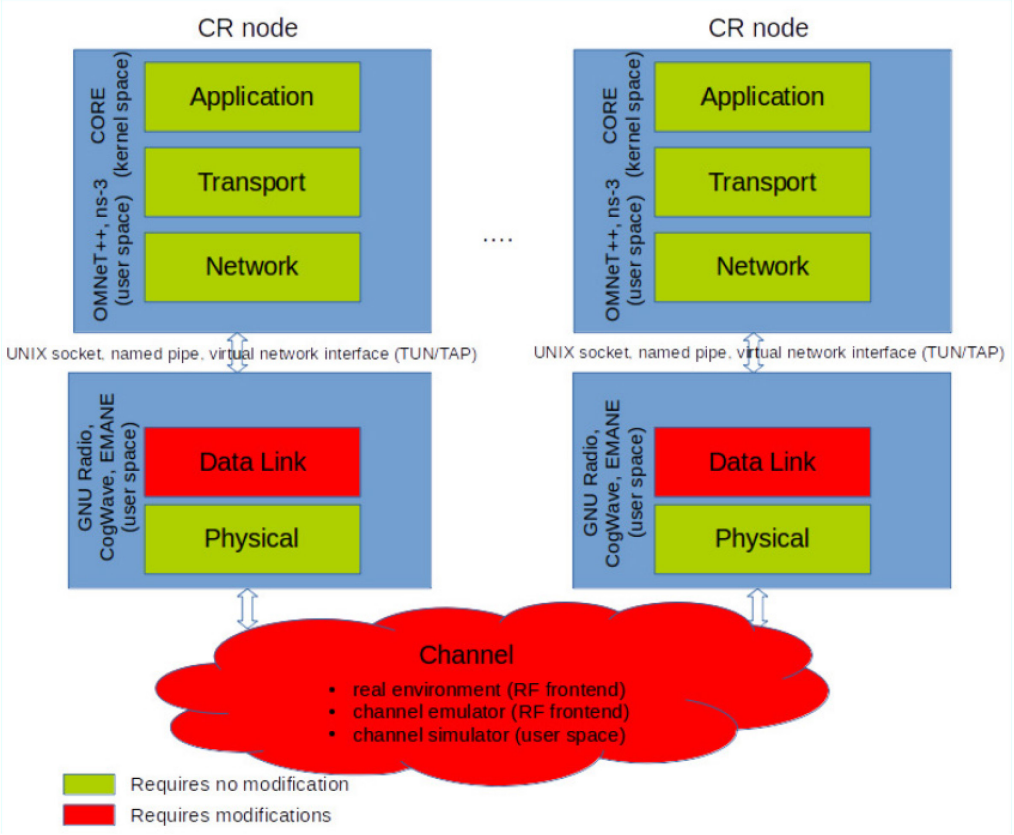



**Figure 4-29: Combination of Open-Source Frameworks for the High-Fidelity Simulation of CRN [183].**

Radio simulators (GNU Radio, CogWave) provide interfaces with hardware devices to test in a real environment or on channel emulator hardware (testbed mode). They also provide realistic channel models (AWGN channel, fading channel, frequency-selective fading, hardware impairments) for the simulation of small number of nodes. The combination at the network layer requires either the development of realistic channel models for the simulation of high number of nodes in the radio simulators (similarly to Ref. [185]), or the development of realistic channel models for the simulation of high number of nodes in the network simulators (which significantly abstract the channel). In the latter case, an interface between the radio simulator and the network simulator is necessary at the network layer and the physical layer.

The CORE framework and the EMANE framework can be combined by TUN/TAP interfaces at the network layer [186]. The CORE framework can also run in conjunction with underlying ns-3 simulated wireless networks. However, the combination of the CORE and EMANE frameworks or the combination of the CORE and ns-3 frameworks require significant work on the physical layer and the channel due to their abstraction. A possible solution is to combine the CORE and EMANE frameworks or the CORE and ns-3 frameworks with a radio simulator (GNU Radio, CogWave). Ns-3 has the advantage over OMNeT++ to internally represent packets as bit vectors in network byte order, resembling real-world packet formats [187].

The authors in Ref. [183] observed that the extension of open-source frameworks requires a major rewrite of the different frameworks. They estimated that a better solution is to combine radio simulators and network simulators at the network layer (see Figure 4-29), although this combination requires the development of the data link layer, realistic channel models and interfaces in the radio simulators. Therefore, they developed in the CogWave open-source software framework several MAC protocols (Point-to-Point-TDD, Point-to-Point-FDD, Aloha, non-persistent CSMA, 1-persistent CSMA, p-persistent CSMA, TDMA, OFDMA) for the data link

layer and realistic channel models (AWGN channel, log-distance path loss, fading channel, frequency-selective fading) for simulating a high number of nodes as well as interfaces with hardware platforms for testbed evaluation and hardware-in-the-loop (HIL). The extensions have been implemented in such a way that the same MAC protocol (data link layer) and modulation scheme (physical layer) can be used without modifications either in a testbed mode with hardware platforms (small number of nodes with real-time scheduling), in an emulation mode (HIL with real-time scheduling) or in a simulation mode with realistic channel models (high number of nodes).

In a testbed mode with a hardware platform, such as the USRP, the physical layer is connected to an UHD device class which transmit and receive IQ samples in real-time according to the USRP time clock. Another device class could be created for other hardware platforms (e.g., OsmoSDR platforms). In an emulation mode, the physical layer is connected to a virtual device class which transmits and receives IQ samples in real-time, according to the computer system time using realistic channel models.

In a simulation mode, the physical layer is connected to a simulator device which adds the IQ samples of all the transmitting nodes to all the receiving nodes at a particular time using realistic channel models in simulation time. Preliminary tests show that the new extensions in the CogWave open-source software framework allow accurate simulation, emulation, and connection with RF hardware for all the modulation schemes and MAC protocols, which have been implemented. The combination of the CogWave open-source software framework with the network simulators (OMNeT++, ns-3) allows to execute different protocols and applications (e.g., routing protocols, TCP, UDP, ping application, client-server application). However, more tests and adjustments are needed to validate the simulator device for a high number of nodes.

## 4.10 REFERENCES

[1] Fortuna, C. and Mohorcic, M., “Trends in the Development of Communication Networks: Cognitive Networks”, Computer Networks, Vol. 53, No. 9, pp. 1354-1376, 2009.

[2] Clausen, T. and Jacquet, P., “Optimized Link State Routing Protocol (OLSR)”, RFC 3626, 2003.

[3] Perkins, C., Belding-Royer, E. and Das, S., “Ad hoc On-Demand Distance Vector (AODV) Routing”, RFC 3561, 2003

[4] Liu, Y., Mi, Z., Zhang, J.-F. and Qu, X., “Improvement of ETX Metric Base on OLSR”, 2010 International Conference on Wireless Communications and Signal Processing (WCSP), Suzhou, 2010.

[5] Royer, E. and Toh, C.-K., “A Review of Current Routing Protocols for ad hoc Wireless Networks,” IEEE Pers. Commun., 1999.

[6] Hussein, O. and Saadawi, T., “Ant Routing Algorithm for Mobile ad hoc Networks (ARAMA)”, Conference Proceedings of the 2003 IEEE International Performance, Computing, and Communications Conference, 2003.

[7] Cesana, M., Cuomo, F. and Ekici, E., “Routing in Cognitive Radio Networks: Challenges and Solutions”, Challenges and solutions, ad hoc Networks, 2010.

[8] Lee, J.-J. and Lim, J., “Cognitive Routing for Multi-hop Mobile Cognitive Radio ad hoc Networks”, Journal of Communications and Networks, Vol. 16, No. 2, April 2014.

[9] Le, T., Rabsatt, V. and Gerl, M., “Cognitive Routing with the ETX Metric”, 13th Annual Mediterranean ad hoc Networking Workshop (MED-HOC-NET), 2014.

[10] Hou, L., Yeung, K. and Wong, K., "A Vision of Energy-Efficient Routing for Cognitive Radio ad hoc Networks". 6th International Symposium on Wireless and Pervasive Computing (ISWPC), 2011, IEEE. pp. 1-4.

[11] Singh, K. and Mohn, S., "Routing Protocols in Cognitive Radio ad hoc Networks: A Comprehensive Review", Journal of Network and Computer Applications 72, 2016, pp. 28-37.

[12] Rahman, M.A., Caleffi, M. and Paura, L., "Joint Path and Spectrum Diversity in Cognitive Radio ad hoc Networks". EURASIP J. Wireless. Commun. Network 2012 (1), pp. 1-9.

[13] Zhang, Y., Song, F., Deng, Z. and Li, C., "An Energy-Aware Routing for Cognitive Radio ad hoc Networks". International Conference on Information Science and Technology (ICIST), 2013. IEEE. pp. 1397-1401.

[14] Rehman, R.A. and Kim, B.S., "L2ER: Low-Latency and Energy-Based Routing Protocol for Cognitive Radio ad hoc Networks Int". J. Distrib. Sens. Netw. 2014.

[15] Kamruzzaman, S., Kim, E. and Jeong, D.G., "An Energy-Efficient QoS Routing Protocol for Cognitive Radio ad hoc Networks": 13th International Conference on Advanced Communication Technology (ICACT), 2011. IEEE. pp. 344-349.

[16] Rahman, M.A., Caleffi, M. and Paura, L., "Joint Path and Spectrum Diversity in Cognitive Radio Ad Hoc Networks". EURASIP J. Wirel. Commun. Netw. 2012 (1), pp. 1-9.

[17] Che-Aron, Z., Abdalla, A.H., Hassan, W.H., Abdullah, K., and Rahman, M.A., "E-D2CARP: A Joint Path and Spectrum Diversity-Based Routing Protocol with an Optimized Path Selection for Cognitive Radio ad hoc Networks", IEEE 2nd International Symposium on Telecommunication Technologies (ISTT), Langkawi, Malaysia, November 2014.

[18] Chao, C.-M., Fu, H.-Y. and Zhang, L.-R., "An Anypath Routing Protocol for Multi-hop Cognitive Radio *Ad hoc* Networks", 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl. Conf. on Autonomic and Trusted Computing and 2014 IEEE 14th Intl. Conf. on Scalable Computing and Communications and Associated Symposia/Workshops, 2014, pp. 127-133.

[19] Mahgoub, F.A., Elsayed, H.A. and El Ramly, S., "Performance Comparison of CAODV, SEARCH, and WCETT Routing Protocols in CRAHNs", International Conference on Systems Informatics, Modelling and Simulation (SIMS), 1-3 June 2016, Riga, Latvia.

[20] Cacciapuoti, A.S., Calcagno, C., Caleffi, M. and Paura, L., "CAODV: Routing in Mobile ad hoc Cognitive Radio Networks, Wireless Days (WD)," 2010 IFIP, Venice, Italy.

[21] Chowdhury, K.R. and Felice, M.D., "SEARCH: A Routing Protocol for Mobile Cognitive Radio ad hoc Networks", Computer Communications, Vol. 32, No. 18, 2009, pp. 1983-1997.

[22] Ruslan, R., Saian, R. and Teramizi, N.M., "Performance Analysis of AODV and WCETT Routing Protocols in Cognitive Radio Ad-Hoc Network (CRAHN)," Fifth International Conference on Intelligent Systems, Modeling and Simulation, 2 Jan 2014.

[23] Draves, R., Padhye, J., and Zill, B., "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks". In Proceedings of MOBICOM '04, New York, NY, USA, 2004, pp. 114-128.

[24] Al-Rawi, H.A.A., Yau, K.-L.A., Mohamad, H., Ramli, N. and Hashim, W., "Reinforcement Learning for Routing in Cognitive Radio *Ad hoc* Networks," Hindawi Publishing Corporation, Volume 2014, Article ID 960584.

[25] Safdar, T., Hasbulah, H.B., and Rehan, M., "Effect of Reinforcement Learning on Routing of Cognitive Radio *Ad hoc* Networks", 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC), 2015.

[26] Guan, Q., Yu, F.R., Jiang, S. and Wei, G., "Prediction-Based Topology Control and Routing in Cognitive Radio Mobile *Ad hoc* Networks", IEEE Transactions on Vehicular Technology, Vol. 59, Issue 9, November 2010, pp. 4443-4452.

[27] Jardosh, S. and Ranjan, P., "A Survey: Topology Control for Wireless Sensor Networks", Proc. of IEEE International Conference on Signal processing, Communications and Networking, Chennai, January 2008.

[28] Aziz, A.A., Sekercioglu, Y.A., Fitzpatrick, P. and Ivanovich, M., "A Survey on Distributed Topology Control Techniques for Extending the Lifetime of Battery Powered Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, Vol. 15, No. 1, 2013, pp. 121-144.

[29] Li, M., Li, Z. and Vasilakos, A.V., "A Survey on Topology Control in Wireless Sensor Networks: Taxonomy, Comparative Study, and Open Issues", Proceedings of the IEEE, Vol. 101, Issue 12, Dec. 2013, pp. 2538-2557.

[30] Wightman, P.M. and Labrador, M.A., "A3: A Topology Construction Algorithm for Wireless Sensor Networks", Proc. of IEEE Global Telecommunications Conference (GLOBECOM), 2008.

[31] Torkestani, J.A., "An Energy-Efficient Topology Construction Algorithm for Wireless Sensor Networks", Computer Networks 57, Elsevier, 2013, pp. 1714-1725.

[32] Jian-Zhao, Z., Hang-Sheng, Z. and Fu-Qiang, Y., "A Fast Neighbor Discovery Algorithm for Cognitive Radio ad hoc Networks, Proc. of 12th IEEE International Conference on Communication Technology (ICCT), Nanjing, China, November 2010.

[33] Chao, C.-M. and Hsu, C.-Y., "Supporting Fast Neighbor Discovery for Cognitive Radio Networks", Proc. of International Conference on Computational Problem-Solving (ICCP), Jiuzhai, China, 2013.

[34] Zeng, Y., Mittal, N., Venkatesan, S. and Chandrasekaran, R., "Fast Neighbor Discovery with Lightweight Termination Detection in Heterogeneous Cognitive Radio Networks", Proc. of Ninth International Symposium on Parallel and Distributed Computing, Istanbul, Turkey, July 2010.

[35] Asterjadhi, A. and Zorzi, M., "JENNA: A Jamming Evasive Network-Coding Neighbor-Discovery Algorithm for Cognitive Radio Networks", IEEE Wireless Communications, Vol. 17, Issue 4, August 2010, pp. 24-32.

[36] Chen, P.-Y., Karyotis, V., Papavassilou, S. and Chen, K.-C., "Topology Control in Multi-Channel Cognitive Radio Networks with Non-Uniform Node Arrangements", Proc. of IEEE Symposium on Computers and Communications (ISCC), Kerkyra, Greece, 2011.

[37] Santi, P., "Topology Control in Wireless *Ad hoc* and Sensor Networks", ACM Computing Surveys, Vol. 37, No. 2, June 2005, pp. 164-194,

[38] Krishnamurthy, S., Mittal, N., Chandrasekaran, R. and Venkatesan, S., "Neighbour Discovery in Multi-Receiver Cognitive Radio Networks", Proc. of International Journal of Computers and Applications, Vol. 31, No. 1, 2009, pp. 50-57.

[39] De Nardis, L., Di Benedetto, M.-G., Rakovic, V., Atanasovski, V., Gavrilovska, L., Holland, O., Aghvami, H., Tassetto, D., Bovelli, S., Stavroulaki, V., Kritikou, Y., Bantouna, A., Demestichas, P. and Romaszko, S., "Neighbour and Network Discovery in Cognitive Radio Networks: Research Activities and Results in the ACROPOLIS Network of Excellence", Proc. of 19th European Wireless Conference (EW), Guildford, United Kingdom, April 2013.

[40] Wang, F., Sun, S., Li, L., Guo, W. and Ma, Y., "Neighbor Discovery Based on Group Frequency Hopping Without Common Control Channel for Cognitive Radio *Ad hoc* Networks", Proc. of 15th IEEE International Conference on Communication Technology (ICCT), Guilin, China, November 2013.

[41] Arachchige, C.J.L., Venkatesan. S. and Mittal, N., "An Asynchronous Neighbor Discovery Algorithm for Cognitive Radio Networks", Proc. of 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), Chicago, IL, USA, October 2008.

[42] Wang, X., Sheng, M., Zhai, D., Li, J., Mao, G. and Zhang. Y., "Achieving Bi-Channel-Connectivity with Topology Control in Cognitive Radio Networks", IEEE Journal on Selected Areas in Communications, Vol. 32, Issue 11, November 2014, pp. 2163-2176.

[43] Erel, M., Özcevik, Y. and Canberk, B., "A Topology Control Mechanism for Cognitive Smallcell Networks Under Heterogeneous Traffic", 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Madrid, Spain, June 2013.

[44] Zhao, J. and Cao, G., "Robust Topology Control in Multi-Hop Cognitive Radio Networks", IEEE Transactions on Mobile Computing, Vol. 13, No. 11, November 2014, pp. 2634-2647.

[45] Van den Berg, E., Fecko, M.A., Samtani, S., Lacatus, C. and Patel, M., "Cognitive Topology Control Based on Bame Theory", Proc. of Military Communications Conference (MILCOM), San Jose, CA, USA, 2010.

[46] Peng, H., Bai, Y., Liu, X. and Yang, W., "Topology Control Approach Based on Radio Irregularity Using Game Theory for Cognitive Wireless Networks", Proc. of Computing, Communications and Applications Conference (ComComAp), Hong Kong, China, Jan. 2012.

[47] Zhang, Q., He, Q. and Zhang, P., "Topology Reconfiguration in Cognitive Radio Networks Using Ant Colony Optimization", Proc. of IEEE Vehicular Technology Conference (VTC Fall), Quebec City, QC, Canada, September 2012.

[48] Hadawale, K. and Barve, S., "Link Prediction-Based Topology Control and Adaptive Routing in Cognitive Radio Mobile *Ad hoc* Networks", IEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, December 2014.

[49] Jian-Zhao, Z., Fan, W., Fu-qiang, Y., Hang-sheng, Z. and Yu-sheng, L., "Cluster-Based Distributed Topology Management in Cognitive Radio *Ad hoc* Networks", International Conference on Computer Application and System Modeling (ICCASM), Taiyuan, China, October 2010.

[50] Chen, T., Zhang, H., Maggio, G.M. and Chlamtac, I., "Topology Management in CogMesh: A Cluster-Based Cognitive Radio Mesh Network", IEEE International Conference on Communications, Glasgow, Scotland, June 2007.

[51] Akyildiz, I.F., Lo., B.F. and Balakrishnan, R., "Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey", Physical Communication, Vol.4, No.1, March 2011, pp. 40-62.

[52] Liu, J. and Singh, S., "ATCP: TCP for Mobile *Ad hoc* Networks", IEEE J. Selected Areas of Comm., Vol. 19, No. 7, July 2001, pp. 1300-1315.

[53] Capone, A., Fratta, L. and Martignon, F., "Bandwidth Estimation Schemes for TCP Over Wireless Networks", IEEE Transactions on Mobile Computing 3 (2), 2004.

[54] Chou, C., Shankar, S., Kim, H. and Shin, K.G., "What and How Much to Gain by Spectrum Agility?", IEEE Journal on Selected Areas in Communications 25 (3), 2007.

[55] Chowdhury, K.R., Felice, M.D. and Akyildiz, I.F., "TCP CRAHN: A Transport Control Protocol for Cognitive Radio *Ad hoc* Networks", IEEE Transactions on Mobile Computing, Vol. 12, No. 4, April 2013.

[56] Al-Ali, A.K. and Chowdhury, K., "TFRC-CR: An Equation-Based Transport Protocol for Cognitive Radio Networks", 2013 International Conference on Computing, Networking and Communications (ICNC) Workshop on Computing, Networking and Communications.

[57] Information Sciences Institute, RFC 793 – Transmission Control Protocol, September 1981.

[58] Al Hanbali, A., Altman, E. and Nain, P., "A Survey of TCP over Mobile Ad hoc Networks." Research Report RR-5182, INRIA. 2004.

[59] Tsukamoto, K., Koba, S., Tsuru, M. and Oie, Y. (2015). "Cognitive Radio-Aware Transport Protocol for Mobile ad hoc Networks". IEEE Transactions on Mobile Computing, 14(2), pp. 288-301.

[60] Ya-yun, X. and Liu-lei, Z., "TCP Enhancement Technology in Cognitive Network Based on Cross-Layer Designing", Ubiquitous Wireless Broadband (ICUWB) 2016 IEEE International Conference, 2016, pp. 1-4.

[61] Slingerland, A.M.R., Pawelczak, P., Prasad, R.V., Lo, A. and Hekmat, R., "Performance of Transport Control Protocol over Dynamic Spectrum Access Links," Proc. Second IEEE International Symposium, New Frontiers in Dynamic Spectrum Access Networks (DySPAN), Apr. 2007.

[62] Dechene, D.J., El Jardali, A., Luccini, M. and Sauer, A., "A Survey of Clustering Algorithms for Wireless Sensor Networks". Computer Communications. Butterworth-Heinemann, Newton, MA USA, 2007.

[63] Abbasi, A.A. and Younis, M., "A Survey on Clustering Algorithms for Wireless Sensor Networks", Computer Communications, 30 (14-15), 2007, pp. 2826-2841.

[64] Boyinbode, O., Le, H., Mbogho, A., Takizawa, M. and Poliah, R., "A Survey on Clustering Algorithms for Wireless Sensor Networks", IEEE International Conference on Network-Based Information Systems, 2010.

[65] Agarwal, R. and Motwani, M., "Survey of Clustering Algorithms for MANET," International Journal on Computer Science and Engineering, Vol. 1 (2), 2009.

[66] Cokuslu, D. and Erciyes, K., "A Hierarchical Connected Dominating Set Based Clustering Algorithm for Mobile *ad hoc* Networks", MASCOTS '07 Proceedings of the 2007 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems.

[67] Gerla, M. and Tsai, J.T., "Multiuser, Mobile, Multimedia Radio Network," *Wireless Networks*, Vol. 1, Oct. 1995, pp. 255-65.

[68] Chiang, C.-C., Wu, H.-K., Liu, W. and Gerla, M., "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," in proceedings of IEEE SICON'97, 1997.

[69] Basu, P., Khan, N. and Little, T.D.C., "A Mobility Based Metric for Clustering in Mobile *Ad hoc* Networks," in Proceedings of *IEEE ICDCSW' 01*, Apr. 2001, pp. 413-18,

[70] Er, I. and Seah, W., "Mobility-Based D-Hop Clustering Algorithm for Mobile ad hoc Networks". *IEEE Wireless Communications and Networking Conference* Vol. 4., 2004, pp. 2359-2364.

[71] Wu, J., Dai, F., Gao, M. and Stojmenovic, I., "On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in *Ad hoc* Wireless Networks," *J. Commun. and Networks*, Vol. 4, No. 1, Mar. 2002, pp. 59-70.

[72] Younis, O. and Fahmy, S., "HEED: a Hybrid, Energy-Efficient, Distributed Clustering Approach for ad hoc Sensor Networks," in *IEEE Transactions on Mobile Computing*, Vol. 3, No. 4, Oct.–Dec. 2004, pp. 366-379.

[73] Sheu, P., and Wang, C., "A Stable Clustering Algorithm Based on Battery Power for Mobile *ad hoc* Networks". Tamkang Journal of Science and Engineering, 2006, pp. 233-242.

[74] Amis, A.D. and Prakash, R., "Load-Balancing Clusters in Wireless *ad hoc* Networks," in Proc. 3rd IEEE ASSET '00, March 2000, pp. 25-32.

[75] Li, F., Zhang, S., Wang, X., Xue, X. and Shen, H., "Vote-Based Clustering Algorithm in Mobile *ad hoc* Networks", In Proceedings of *International Conference on Networking Technologies,* 2004.

[76] Chatterjee, M., Das, S.K. and Turgut, D., "WCA: A Weighted Clustering Algorithm for Mobile *ad hoc* Networks," Cluster Computing Journal, Vol. 5, No. 2, Apr. 2002, pp. 193-204.

[77] El-Bazzal, Z., "An Efficient Management Algorithm for Clustering in Mobile ad hoc Network", In Proceedings of ACM Inter. Workshop on Performance Monitoring, Measurement, and Evaluation of Heterogeneous Wireless and Wired Networks, 2006.

[78] Dhurandher, S.K. and Singh, G.V., "Weight Based Adaptive Clustering in Wireless *ad hoc* Networks", In Proceedings of 2005 IEEE International Conference on Personal Wireless Communications, ICPWC 2005.

[79] Chatterjee, M., Das, S.K. and Turgut, D., "An On-Demand Weighted Clustering Algorithm (WCA) for *ad hoc* Networks," in Proceedings of *IEEE Globecom '00*, 2000, pp. 1697-701.

[80] Wang, Y.-X. and Bao, F.S., "An Entropy-Based Weighted Clustering Algorithm and Its optimization for *ad hoc* Networks", wimob, pp.56, *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications* (WiMob 2007), 2007.

[81] Dhurandher, S.K. and Singh, G.V., "Weight-Based Adaptive Clustering in Wireless ad hoc Networks". IEEE, 2005.

[82] Yau, K.-L.A., Ramli, N., Hashim, W. and Mohamad, H., "Clustering Algorithms for Cognitive Radio Networks: A Survey". Journal of Network and Computer Applications, 45, 2014.

[83] Liu S., Lazos, L. and Krunz, M., "Cluster-Based Control Channel Allocation in Opportunistic Cognitive Radio Networks", IEEE Transactions on Mobile Computing, Vol. 11, No. 10, October 2012.

[84] Li, D. and Gross, J., "Robust Clustering of *ad hoc* CRN Under Opportunistic Spectrum Access", IEEE ICC, 2011.

[85] Heren, M.A.C., Yilmaz, H.B. and Tugcu, T., "Energy Efficient MAC Protocol for Cluster Formation in Mobile Cooperative Spectrum Sensing," IEEE WCNC, 2015.

[86] Kozal, A.S.B., Merabti, M. and Bouhafs, F., "Energy-Efficient Multi-Hop Clustering Scheme for Cooperative Spectrum Sensing in CRNs", IEEE CCNC, 2014.

[87] Shahrasbi, B. and Rahnavard, N., "A Clustering-Based Coordinated Spectrum Sensing in Wideband Large-Scale Cognitive Radio Networks", In Proc. of Globecom 2013 – Cognitive Radio and Networks Symposium, 2013.

[88] Potier, P. and Qian, L., "Network Management of Cognitive Radio ad hoc Networks", ACM CogArt 2011, October 2011.

[89] Demestichas, P., Dimitrakopoulos, G. and Kritikou, Y. (Eds.), "Policy-Based Management of Radio Resources and Autonomic Computing in Cognitive/Reconfigurable Networks and Systems", Wireless World Research Forum, Working Group 6 White Paper, 2008.

[90] VanderHorn, N., Haan, B., Carvalho, M. and Perez, C., "Distributed Policy Learning for the Cognitive Network Management System", MILCOM, 2010.

[91] Doyle, A. and Forde, T., "The Wisdom of Crowds: Cognitive *ad hoc* Networks", in "Cognitive Networks: Towards Self-Aware Networks", 2007.

[92] Joint Publication 1, Doctrine for the Armed Forces of the United States, March 2013.

[93] Army Doctrine Publications, Operations, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33695/ADPOperationsDec10.pdf, 2010 (accessed 30.1.2017).

[94] Bao, F. and Chen, I-R., "Trust Management for the Internet of Things and Its Application to Service Composition," in IEEE WoWMoM 2012 Workshop on the Internet of Things: Smart Objects and Services, San Francisco, CA, USA, June 2012.

[95] Ruidong, L., Kato, J. and Li, J., "Future Trust Management Framework for Mobile *Ad hoc* Networks", IEEE Communications Magazine, pp. 108-114, April 2008.

[96] Buchegger, S. and Le Boudec, J., "Performance Analysis of the CONFIDANT Protocol", in Proc. of the 3rd ACM International Symposium on Mobile *ad hoc* Networking and Computing (MobiHoc), Lausanne, 2002.

[97] Yunfang, F., "Adaptive Trust Management in MANET", 2007 International Conference on Computational Intelligence and Security.

[98] Sen, J., Chowdhury, J.R. and Sengupta, I., "A Distributed Trust Mechanism for Mobile *Ad hoc* Networks", *Ad hoc* and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium, IEEE 2006.

[99] Junfeng, T., Ruizhong, D., Xiaoxue, M. and Zixian, W., "A Trust Model of P2P Network Based on Reputation and Risk", World Congress on Software Engineering, IEEE 2009.

[100] Bao, F. and Chen, I., "Dynamic Trust Management for Internet of Things Applications", Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, pp. 1-6, 2012.

[101] Han, Z., Liu, K.J.R., Sun, Y.L. and Yu, W., "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks", in Proc. INFOCOM 2006, April 2006.

[102] Chen, D., Chang, G., Sun, D., Li, J., Jia, J. and Wang, X., "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things", Computer Science and Information Systems, Vol. 8, No. 4, Oct. 2011, pp. 1207-1228.

[103] Konorski, J. and Orlikowski, R., "DST-Based Detection of Noncooperative Forwarding Behavior of MANET and WSN Nodes," in Proceedings of the 2nd Joint IFIP WMNC, Gdańsk, Poland, 2009.

[104] Mukherjee, T. and Nath, A., "Cognitive Radio Network Architecture and Security Issues: A Comprehensive Study". International Journal of Advanced Research in Computer Science and Software Engineering 5 (6), 2015.

[105] Rawat, A.S., Anand P., Chen H. and Varshney, P.K., "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks". IEEE Transactions on Signal Processing 59 (2), 2011, pp. 774-786.

[106] Chen, R., Park, J., Hou, Y. and Reed, J., "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks". IEEE Communications Magazine 46 (4), 2008, pp. 50-55.

[107] Bhattacharjee, S., Debroy, S. and Chatterjee, M., "Trust Computation Through Anomaly Monitoring in Distributed Cognitive Radio Networks". Proceedings of IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications, 2011, pp. 593-597.

[108] Chen, R., Park, J. and Bian, K., "Robust Distributed Spectrum Sensing in Cognitive Radio Networks". Proceedings of IEEE INFOCOM, 2008, pp. 31-35.

[109] Charles, C.T. and Goergen, N., "Security in Cognitive Radio Networks: Threats and Mitigation". Proc. of the 3rd International Conf. on Cognitive Radio Oriented Wireless Networks and Communications, 2008, pp. 1-8.

[110] Kaligineedi, P., Khabbazian, M. and Bhargava, V., "Secure Cooperative Sensing Techniques for Cognitive Radio Systems". Proceedings of IEEE International Conference on Communications, 2008, pp. 3406-3410.

[111] Pei, Q., Yuan, B., Li, L. and Li, H. "A Sensing and Etiquette Reputation-Based Trust Management for Centralized Cognitive Radio Networks". Neurocomputing 101, 2-13, 2013, pp. 129-138.

[112] Wang, W., Li, H., Sun, Y. and Han, Z. "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks". Proceedings of the 43rd Annual Conference on Information Sciences and Systems, 2009, pp. 130-134.

[113] Kalaiselvan, C. and Kavitha, K., "An Advanced Security Enhancements for Cognitive Radio Networks with Trust Management". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 4 (5), 2015, pp. 4816-4822.

[114] Li, J., Fen, Z., Wei, Z., Feng, Z. and Zhang, P., "Security Management Based on Trust Determination in Cognitive Radio Networks". EURASIP Journal on Advances in Signal Processing 2014, pp. 1-16.

[115] Amanowicz, M., Głowacka, J., Parobczak, K. and Krygier, J., "A Trust-Based Information Assurance Mechanism for Military Mobile Ad hoc Networks," MIKON 2014 – 20th International Conference on Microwaves, Radar, and Wireless Communications, 16–18 June, Gdańsk, Poland.

[116] Smarandache, F. and Dezert, J., "Advances and Applications of DSmT for Information Fusion, Vol.1-3," American Research Press Rehoboth, 2004, 2006, 2009.

[117] Masri, A.M., Chiasserini, C.-F., Casetti, C. and Perotti, A., "Common Control Channel Allocation in Cognitive Radio Networks through UWB Communication", Journal of Communications and Networks, Vol. 14, No. 6, December 2012.

[118] Liu, Y., Dong, L. and Marks II, R.J., "Common Control Channel Assignment in Cognitive Radio Networks Using Potential Game Theory", IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 2013.

[119] Wang, X., Zhang, X., Zhang, Q. and Tang, C., "Common Control Channel Model on MAC Protocols in Cognitive Radio Networks", International Conference on Computer Science and Network Technology (ICCSNT), Harbin, China, 2011.

[120] Mirhoseninejad, S.M., Berangi, R. and Fathy, M., "Improving Saturation Capacity Through Verification of Common Control Channel Mechanism in Cognitive Radio ad hoc Networks", 4th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, October 2014.

[121] Krishnamurthy, S., Thoppian, M., Venkatesan, S. and Prakash, R., "Control Channel-Based MAC-Layer Configuration, Routing and Situation Awareness for Cognitive Radio Networks", IEEE Military Communications Conference (MILCOM), Atlantic City, NJ, USA, 2005.

[122] Song, Y. and Xie, J., "A Distributed Broadcast Protocol in Multi-Hop Cognitive Radio *Ad hoc* Networks Without a Common Control Channel", IEEE INFOCOM, 2012, pp. 2273-2281.

[123] Zou, Y., Yao, Y.-D. and Zheng, B., "A Selective-Relay Based Cooperative Spectrum Sensing Scheme Without Dedicated Reporting Channels in Cognitive Radio Networks", IEEE Transactions on Wireless Communications, Vol. 10, No. 4, April 2011, pp. 1188-1198.

[124] Liu, S., Lazos, L. and Krunz, M., "Cluster-Based Control Channel Allocation in Opportunistic Cognitive Radio Networks", IEEE Transactions on Mobile Computing, Vol. 11, No. 10, pp. 1436-1449, October 2012.

[125] Thilina, K.M., Hossain, E. and Kim, D.I., "DCCC-MAC: A Dynamic Common Control Channel-Based MAC Protocol for Cellular Cognitive Radio Networks", IEEE Transactions on Vehicular Communications, Vol. PP, Issue 99, 2015.

[126] Lo, B.F., "A Survey of Common Control Channel Design in Cognitive Radio Networks", Elsevier Physical Communication, Volume 4, Issue 1, pp. 26-39, March 2011.

[127] Rose, L., Massin, R., Vijayandran, L., Debbah, M. and Le Martret, C., "CORASMA Program on Cognitive Radio for Tactical Networks: High Fidelity Simulator and First Results on Dynamic Frequency Allocation", Proc. of Military Communications Conference (MILCOM), San Diego, CA, USA, November 2013.

[128] Rauschen, D., Couturier, S., Adrat, M., Antweiler, M. and Elders-Boll, H., "Cooperative Spectrum Sensing for a Real-Time Cognitive Radio Demonstrator", NATO STO IST-123 RSY-029 Symposium on Cognitive Radio and Future Networks, The Hague, NLD, May 2014.

[129] NATO STO Technical Report, "Cognitive Radio in NATO II – Towards Dynamic Spectrum Management in NATO", Final Report of Task Group IST-104/RTG-050, December 2016.

[130] Koslowski, S., Elsner, J.P., Couturier, S., Keip, C. and Bettinger, O., "Distributed Localized Interference Avoidance for Dynamic Frequency Hopping ad hoc Networks", in Proc. of SDR-WInnComm-2013, Reston, VA, USA, January 2013.

[131] Sezer, S., Scott-Hayward, S., Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M. and Rao, N., "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," IEEE Communications Magazine, Vol. 51, No. 7,2013, pp. 36-43.

[132] Pawelczak., P., Pollin, S., Wilson So, H.-S., Motamedi, A., Bahai, A., Prasad, R.V. and Hekmat, R., "State of the Art in Opportunistic Spectrum Access Medium Access Control Design", 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), Singapore, Singapore, May 2008.

[133] Huang, T., Yu, F.R., Zhang, C., Liu, J., Zhang, J. and Liu, J., "A Survey on Large-scale Software Defined Networking (SDN) Testbeds: Approaches and Challenges," IEEE Communications Surveys and Tutorials, 2016.

[134] Kim, H. and Feamster, N., "Improving Network Management with Software Defined Networking," IEEE Communications Magazine, Vol. 51, No. 2, pp. 114-119, 2013.

[135] Xia, W., Wen, Y., Foh, C.H., Niyato, D. and Xie, H., "A Survey on Software-Defined Networking," IEEE Communications Surveys and Tutorials, Vol. 17, No. 1, 2015, pp. 27-51.

[136] Nguyen, V.-G., Brunstrom, A., Grinnemo, K.-J. and Taheri, J., "SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey," IEEE Communications Surveys and Tutorials, Vol. 19, No. 3, pp. 1567-1602, 2017.

[137] Vissicchio, S., Vanbever, L. and Bonaventure, O., "Opportunities and Research Challenges of Hybrid Software Defined Networks," ACM SIGCOMM Computer Communication Review, Vol. 44, No. 2, 2014, pp. 70-75.

[138] Bouet, M., Phemius, K. and Leguay, J., Distributed SDN for Mission-Critical Networks, MILCOM 2014. 2014 IEEE Military Communications Conference.

[139] Foukas, X., Patounas, G., Elmokashfi, A. and Marina, M.K., "Network Slicing in 5G: Survey and Challenges," IEEE Communications Magazine, Vol. 55, No. 5, 2017, pp. 94-100.

[140] Open Network Foundation, Wireless and Mobile Working Group, Available: https://www.opennetworking.org/images/stories/downloads/working-groups/charter-wireless-mobile.pdf, 2013.

[141] Pentikousis, K., Wang, Y. and Hu, W., "Mobileflow: Toward Software Defined Mobile Networks," Communications Magazine, IEEE, Vol. 51, No. 7, July 2013, pp. 44-53.

[142] Jin, X., Li, L.E., Vanbever, L. and Rexford, J., "SoftCell: Scalable and Flexible Cellular Core Network Architecture", in Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, ser. CoNEXT '13. NY, USA: ACM, 2013.

[143] Gudipati, A., Perry, D., Li, L.E. and Katti, S., "Softran: Software Defined Radio Access Network", in Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, ser. HotSDN '13. NY, USA: ACM, 2013.

[144] Bernardos, C., De La Oliva, A., Serrano, P., Banchs, A., Contreras, L., Jin, H. and Zuniga, J., "An Architecture for Software Defined Wireless Networking", Wireless Communications, IEEE, Vol. 21, No. 3, June 2014, pp. 52-61.

[145] Yazc, V., Kozat, U. and Oguz Sunay, M., "A New Control Plane for 5G Network Architecture with a Case Study on Unified Handoff, Mobility, and Routing Management," Communications Magazine, IEEE, Vol. 52, No. 11, Nov 2014, pp. 76-85.

[146] Meneses, F., Corujo, D., Guimaraes, C. and Aguiar, R.L., "Extending SDN to End Nodes Towards Heterogeneous Wireless Mobility", IEEE, 2015.

[147] Chaudet, C. and Haddad, Y., "Wireless Software Defined Networks: Challenges and Opportunities," 2013 IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems (COMCAS), 2013.

[148] Dely, P., Kassler, A., and Bayer, N., "OpenFlow for Wireless Mesh Networks", 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN).

[149] Rangisetti, A.K., Bhopabhai, B.H., Kumar, B.P., and Tamma, B.R., "Load Aware Hand-Offs in Software Defined Wireless LANs", IEEE WiMob, 2014.

[150] Singh, K.V.K. and Pandey, M., "Software-Defined Mobility in IP-Based Wi-Fi networks: Design Proposal and Future Directions", IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2016.

[151] Labraoui, M., Boc, M.M. and Fladenmuller, A., "Software Defined Networking-Assisted Routing in Wireless Mesh Networks", 2016 International Wireless Communications and Mobile Computing Conference (IWCMC).

[152] Labraoui, M., Chatzinakis, C., Boc, M.M. and Fladenmuller, A., "On Addressing Mobility Issues in Wireless Mesh Networks Using Software-Defined Networking", 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN).

[153] Detti, A., Pisa, C., Salsano, S. and Blefari-Melazzi, N., "Wireless Mesh Software Defined Networks (wmSDN)", 2nd International Workshop on Community Networks and Bottom-up-Broadband (CNBuB 2013).

[154] Arun, K.P., Chakraborty, A. and Manoj, B.S., "Communication Overhead of an Openflow Wireless Mesh Network", 2014 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).

[155] Sun, G., Liu, G. and Wang, Y., "SDN Architecture for Cognitive Radio Networks", 2014 1st International Workshop on Cognitive Cellular Systems (CCS), 2014.

[156] Matin, M. (Ed.), Spectrum Access and Management for Cognitive Radio Networks, Springer, 2017.

[157] Ahmad, I., Namal, S., Ylianttila, M. and Gurtov, A., "Towards Software Defined Cognitive Networking", 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), 2015.

[158] Namal, S., Ahmad, I., Saud, S., Jokinen, M. and Gurtov, A., "Implementation of OpenFlow Based Cognitive Radio Network Architecture: SDN&R", Wireless Networks 22, 2016, pp. 663-677.

[159] Phemius, K., Seddar, J., Bouet, M., Khalifé, H., and Conan, V., "Bringing SDN to the Edge of Tactical Networks", MILCOM 2016 – 2016 IEEE Military Communications Conference.

[160] Spencer, J., Worthington, O., Hancock, R. and Hepworth, E., "Towards a Tactical Software Defined Network", 2016 International Conference on Military Communications and Information Systems (ICMCIS).

[161] Pawelczak, P., Nolan, K.E., Doyle, L., Oh, S.W. and Cabric, D., "Cognitive Radio: Ten Years of Experimentation and Development," IEEE Communications Magazine, Vol. 49, No. 3, pp. 90-100, 2011.

[162] Masonta, M.T., Mzyece, M., and Mekuria, F., "A Comparative Study of Cognitive Radio Platforms," in Conference on Management of Emergent Digital EcoSystem. ACM, 2012, pp. 145-149.

[163] GNU Radio. [Online]. Available: http://www.gnuradio.org.

[164] Malsbury, J., "Modular, Open-Source Software Transceiver for PHY/MAC Research," in Second Workshop of Software Radio Implementation Forum (SRIF'2013), Hong Kong, China, Aug. 2013, pp. 31-36.

[165] Dhar, R., George, G., Malani, A. and Steenkiste, P., "Supporting Integrated MAC and PHY Software Development for the USRP SDR," in IEEE Workshop on Networking Technologies for Software Defined Radio (SDR) Networks, Reston, USA, Sep. 2006.

[166] Nychis, G., Hottelier, T., Yang, Z., Seshan, S. and Steenkiste, P., "Enabling MAC Protocol Implementations on Software-Defined Radios," in 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI'2009), Boston, USA, Apr. 2009, pp. 91-105.

[167] Le Nir, V. and Scheers, B., "CogWave: Open-source Software Framework for Cognitive Radio Waveform Design," in IST-123 Symposium on Cognitive Radio and Future Networks, The Hague, The Nederlands, May 2014. [Online]. Available: https://github.com/vlenircissrma/CogWave.

[168] OMNeT++ Network Simulation Framework. [Online]. Available: http://www.omnetpp.org.

[169] Khan, S., Kalil, M. and Mitschele-Thiel, A., "crSimulator: A Discrete Simulation Model for Cognitive Radio ad hoc Networks in OMNeT++," in 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC'2013), Dubai, United Arab Emirates, Apr. 2013. [Online]. Available: https://github.com/codesnk/crSimulator.

[170] Network Simulator ns-3. [Online]. Available: http://www.nsnam.org/

[171] Al-Ali, A. and Chowdhury, K.R., "Simulating Dynamic Spectrum Access Using ns-3 for Wireless Networks in Smart Environments," in IEEE SECON Workshop on Self-Organizing Wireless Access Networks for Smart City, Singapore, Jun. 2014. [Online]. Available: http://krc.coe.neu.edu/?q=ns3.

[172] Felice, M.D., Chowdhury, K.R., Kim, W., Kassler, A. and Bononi, L., "End-to-End Protocols for Cognitive Radio ad hoc Networks: An Evaluation Study," Performance Evaluation, Vol. 68, No. 9, pp. 859-875, 2011. [Online]. Available: https://github.com/abdulla-alali/TFRC-CR/tree/CRAHN.

[173] Zhong, J., "Development of NS-2 Based Cognitive Radio Cognitive Network Simulator," Master's thesis, Michigan Technological University, USA, 2009. [Online]. Available: http://faculty.uml.edu/Tricia_Chigan/Research/CRCN_Simulator.htm.

[174] Cognitive Radio Cognitive Network Simulator (ns3 Based). [Online]. Available: http://faculty.uml.edu/Tricia_Chigan/Research/CRCN_NS3.html.

[175] Esmaeelzadeh, V., Berangi, R., Sebt, S.M., Hosseini, E.S. and Parsinia, M., "CogNS: A Simulation Framework for Cognitive Radio Networks", Wireless Personal Communications, Vol. 72, No. 4, pp. 2849-2865, Oct. 2013.

[176] Ahrenholz, J., "CORE: A Real-Time Network Emulator," in Military Communications Conference (MILCOM'2008), San Diego, USA, Nov. 2008. [Online]. Available: http://www.nrl.navy.mil/itd/ncs/products/core.

[177] "The Extendable Mobile ad hoc Network Emulator" (EMANE). [Online]. Available: http://www.nrl.navy.mil/itd/ncs/products/emane.

[178] Papanastasiou, S., Mittag, J., Strom, E. and Hartenstein, H., "Bridging the Gap between Physical Layer Emulation and Network Simulation," in IEEE Wireless Communications and Networking Conference (WCNC'2010), Sydney, Australia, April 2010.

[179] Rose, L., Massin, R., Vijayandran, L., Debbah, M. and Le Martret, C., "CORASMA Program on Cognitive Radio for Tactical Networks: High Fidelity Simulator and First Results on Dynamic Frequency Allocation", in Military Communications Conference (MILCOM'2013), San Diego, USA, Nov. 2013.

[180] Ding, L., Sagduyu, Y.E., Yackoski, J., Azimi-Sadjadi, B., Li, R.L.J. and Melodia, T., "High Fidelity Wireless Network Evaluation for Heterogeneous Cognitive Radio Networks," in SPIE Defense, Security and Sensing Conference, Baltimore, USA, April 2012.

[181] Ding, L., Sagduyu, Y., T. Melodia, T., Li, J., Feldman, J. and Matyjas, J., "CREATE-NEST: A Distributed Cognitive Radio Network Platform with Physical Channel Awareness," in Military Communications Conference (MILCOM'2014), San Diego, USA, November 2014.

[182] Soltani, S., Sagduyu, E., Li, H., Feldman, J. and Matyjas, J., "Demonstration of Plug-and-Play Cognitive Radio Network Emulation Testbed," in IEEE Dynamic Spectrum Access Networks (Dyspan'2014), Mclean, USA, April 2014.

[183] Le Nir, V. and Scheers, B., "Evaluation of Open-Source Software Frameworks for High Fidelity Simulation of Cognitive Radio Networks", International Conference on Military Communications and Information Systems (ICMCIS'2015), Krakow, Poland, May 2015.

[184] Barz, C. and Rogge, H., "Improved Community Network Node Design Using a DLEP Based Radio-to-Router Interface", International Conference on Wireless and Mobile Computing, Networking and Communications, Barcelona, Spain, 2012.

[185] Elsner, J., Braun, M., Nagel, S., Nagaraj, K. and Jondral, F.K., "Networks In-the-Loop: Software Radio as the Enabler," in Software Defined Radio Forum Technical Conference, Washington, USA, Dec. 2009.

[186] Ahrenholz, J., "Integration of the CORE and EMANE Network Emulators," in Military Communications Conference (MILCOM'2011), Baltimore, USA, Nov. 2011.

[187] Weingaertner, E., Schmidt, F., vom Lehn, H., Heer, T. and Wehrle, K., "Slicetime: A Platform for Scalable and Accurate Network Emulation," in 8th USENIX Symposium on Networked Systems Design and Implementation (NSDI'2011), Boston, USA, Apr. 2011.

# Chapter 5 – MAJOR FINDINGS TAKEN FROM PREVIOUS CHAPTERS

The findings in this chapter are the essential findings from Chapter 4. The architecture framework in Chapter 7 will be a result of these findings.

## 5.1 GENERAL

- While CR focuses on frequency management, CRN focuses on end-to-end optimizations. Therefore, cognition is not only applied to frequency aspects, but to almost all parameters in the network. On the other hand, there may be conflicts between node objectives and network objectives, which have to be deconflicted by the cognitive engine(s).
- Interoperability with legacy radios needs to be regarded. Legacy radios with Over-the-Air (OTA) reconfiguration capabilities (e.g., SDR) may be controlled by CRN.

## 5.2 COGNITIVE ROUTING

- Routing should react on channel availability in different geographical regions of the network.
- For military CRN the combination of reactive and proactive routing protocols is needed;
  - Proactive protocols maintain the topology; and
  - Reactive protocols react on channel availability, interference appearance, channel stability.
- Cognitive routing should avoid fixed control channels. Dynamic control information exchange should be sufficient.
- Selection of optimal routes should be improved by the learning capability.
- Cognitive routing allows considering the energy availability of nodes on possible routes and thus to increase overall battery lifetime within a network.

## 5.3 COGNITIVE TOPOLOGY CONTROL

- Cognitive Topology Control should take into account frequency availability in order to identify the optimal links between all nodes. This information can also be useful for neighbour discovery, as neighbour discovery may not be limited to a single frequency.
- Topology control is closely connected with clustering and adaptive transmit power.
- The urgency to update topology information is dependent on external influences like mobility and channel availability. A possible lack of these updates (e.g., due to radio silence) must be regarded.

## 5.4 COGNITIVE DATA TRANSPORT

- There is a need for cross-layer information exchange between all layers of the stack in order to support end-to-end data transport.
- Data transport should adapt the transmission window to the information about the intermediate nodes (e.g., regarding congestion, channel unavailability, etc.).

- End nodes need to be informed about problems on the route.
- There is a need to access the external databases supporting cognitive networks.

## 5.5 COGNITIVE CLUSTERING

- Although the paradigm of ad hoc networks is inherently flat in organization, CRAHNs may in practice be deployed in a manner forming de facto subnetworks, e.g., due to geographical distribution of forces and clustering.
- Clustering should support both the military structures as well as the other technologies. Thus, the network structure should be optimized to efficiently use the available resources (spectrum, energy, etc.).

## 5.6 MANAGEMENT OF COGNITIVE RADIO NETWORKS

- Policies should be managed within the management processes.
- Frequency management needs to regard information from different layers (e.g., frequency availability from PHY, routing information from NET).
- Cognition helps automatizing the management before, during and after a mission, but still a trade-off between automatization and human control is needed.
- A management system should be able to build knowledge about the managed network.
- Pre-planning of a mission should be computer-aided (e.g., learning from previous missions or simulations).

## 5.7 TRUST MANAGEMENT IN COGNITIVE RADIO NETWORKS

- Trust management is required to allow nodes to trust in each other. It especially refers to cognitive engines, which need to exchange control information between the nodes.
- The cognitive management system should be based on direct observations of the control messages received and redirected to other nodes, but also on the level of reputation assessed and sent by trusted nodes.
- The advanced evidence theory can be used as an inference entity as a main part of the trust management system for CRN.

## 5.8 RELIABLE EXCHANGE OF CONTROL INFORMATION

- Control channel needs to carry information from different entities:
  - Clustering;
  - Networking (Routing, Topology Control);
  - CR (Sensing, Channel Change command);
  - Cognition; and
  - Trust management.
- There is a need to dynamically resize the control channel.

- The amount of control traffic limits the capacity for the user traffic.
- Control information can have different priorities and should be handled accordingly.
- In a static environment (e.g., in a basecamp), UWB control channels appear to be a promising solution due to their robustness. In a mobile environment, their range might be too small.
- There can be fixed and dynamic control channels. While fixed channels are instantaneously available but claim bandwidth even when they are not used, dynamic control channels need to be negotiated each time they are used.
- Not all entities from the protocol stack require a control channel.
- Exchange of control and user data over cluster borders may lead to some latency due to frequency changes in the gateway nodes.
- Clustering should be adapted to the required amount of control information.

## 5.9 SOFTWARE DEFINED NETWORKING TECHNOLOGY

- SDN seems to be a promising capability for wireless networks, on which research is still ongoing.
- The applicability of SDN in CRAHNs is yet to be studied.

## 5.10 OPEN COGNITIVE RADIO NETWORK SIMULATORS

- There is currently no open simulation environment available for easily setting up CRN simulations that supports multi-national collaboration in research and development.

# Chapter 6 – COGNITIVE RADIO NETWORKS IN SUPPORT OF MILITARY CAPABILITIES

In the preceding chapters, various aspects of CRNs have been surveyed with a specific view on CRAHNs. A number of proposed designs were identified. These different approaches adopt different parameters, whereby we observe the absence of generally accepted key measures of performance. In order to assess the potential impact, future military CRNS could introduce to the battlefield, we shall summarize proposed features using hypothetical capability statements:

- Military CRNs are to provide mission, circumstances and environmentally balanced reliable and trustworthy communications capability that is self-organizing, delay and disruption tolerant, as well as self-healing.
- Military CRNs (or sub-segments/clusters therein) can operate in several different operating modes simultaneously, being, themselves, the primary network exclusively using licensed (military assigned) frequencies (i.e., either implementing Dynamic Spectrum Access/Dynamic Spectrum Management paradigm or defining PUs and SUs internally within armed forces).
- Military CRNs may operate as a secondary network using unused portions of spectrum licensed to other users (i.e., the traditional notion of CRNs).
- Military CRNs may operate as an inter-networking element between other primary and secondary networks.
- Military CRNs may include CR nodes as well as non-cognitive radio nodes whose behaviour may be controlled by the network.
- A military CRN can also include non-cognitive legacy radio nodes, waveforms, or links whose behaviour is not controlled (e.g., legacy radio relay for trunking backbone).
- A military CRN may consist of handhelds, vehicular radios, as well as fixed radio nodes whose size, power consumption, heat dissipation, processing capabilities, complexity, antennas, available portions of the spectrum, and cost may vary.
- Military CRNs can control individual nodes or clusters of nodes in such operating modes as to minimize the probability of interception or detection within specific military operational circumstances. Individual nodes or clusters of nodes can be operated in modes to circumvent, counter, dodge, or evade hostile electronic warfare measures.
- Military CRNs' policies, constraints, and operating parameters can be planned and tested before implementation at an appropriate command level staff function, and they can be injected/inserted to nodes either locally or over-the-air as military circumstances dictate. The policies can be adjusted during the mission (as a result of a network operation or military conditions), and military CRNs should be ready to update them dynamically.
- A military CRN has to be aware that surrounding networks can also be equipped with cognitive features aiming at the same goal, for example, within a multi-national federated mission network. Military CRSs must foresee such multi-CRN operations to globally optimize the resources during the mission.

## 6.1 CAPABILITY

The concept of *capability* is used in different levels of planning and by different communities of interest. To support these varied needs, several capability models have been introduced. Thereby, some capability

models represent certain perspectives of capability in a specific context and may lead to misunderstandings between stakeholders engaged in planning, building, maintaining or operating the military capability [1].

To embrace the benefits of various viewpoints and to avoid pitfalls of some capability models, a Comprehensive Capability Meta-Model (CCMM) was proposed in Ref.[2] and partially tested within the CR research and development community in Ref. [3]. In this paper, we shall continue these earlier works by assessing the notion of CRNs at CCMM's level 2 (Business Model) and level 3 (System Model).

In the capability-based planning, the capability is seen as an ability or a capacity to perform a set of tasks, or an ability to achieve the desired effect [4]. This functional, or business, perspective and corresponding capability models are used to avoid potential bias to a particular capability solution and to develop solutions suitable for wide range of operations in different geographical locations [5]. To support the Capability-Based Planning process, several predefined functional capability taxonomies are defined, such as US Joint Capability Areas (JCA) [4] and NATO Bi-Strategic Commands' Capability Hierarchy [6], of which the latter shall be used in our analysis as our business model.

Besides capability-based planning, the acquisition community also uses the concept of capability, yet often viewing the concept of capability as systems. System models are typically used in the capability solution planning, building, and management. These models pay attention to all components of the capability instead of just focusing on the platforms and other technical components of capability.

## 6.2 MODELS

Continuing our adaptation to the CCMM, we shall adhere to the level 3 system model consisting of components such as doctrine, organization, training, materiel, leadership, personnel, facilities and policy, as defined in the DOTMLPFI model [7]. Because of the heterogeneity of the components in this model, these system models are also referred to as "lines of development" [1].

Within the CR research community, Ref. [8] collected and rearranged proposed technical properties and possible technical characteristics of CRs. One of these property groups, dynamic spectrum access, was tested in Ref. [9] through DOTMPLFI. The role and place of such military assessment of technical characteristics within broader military capability-based planning process were further elaborated in Ref. [3].

For our purposes, the business model and functional capability areas are best exemplified by [6]. Within NATO, the high-level military functional capability is divided into the following seven capability areas:

- Prepare (R)
- Project (D)
- Engage (E)
- Sustain (S)
- Protect (P)
- Inform (I)
- Consult, command and control (C).

These capability areas are further decomposed into one or more lower-level capability tiers.

The system model is known as DOTMLPFI. The use of the model has been described in more detail in Ref. [9], but to summarize, these lines of development are:

- A doctrine (D) is an expression of the principles by which military forces guide their actions and is a codification of how the activity is conducted.

- Organization (O) relates to the operational and non-operational organizational relationships of people.
- Training (T) is the provision of the means to practice, develop and validate, within constraints, the practical application of military doctrine to deliver a military capability.
- Materiel (M) is the provision of military platforms, systems, and weapons, expendable and non-expendable, needed to outfit/equip an individual, group or organization.
- Leadership (L) is influencing people by providing purpose, direction, and motivation while operating to accomplish the mission and improve the organization.
- Personnel (P) relates to the timely provision of sufficient, capable and motivated personnel to deliver defence outputs, both now and in the future.
- Facilities (F) relates the acquisition, development, management, and disposal of all fixed, permanent buildings and structures, land, utilities, and facility management services in support of defence capabilities.
- Interoperability (I) is the ability of armed forces and, when appropriate, forces of partner and other nations to train, exercise and operate effectively together in the execution of assigned missions and tasks.

Figure 6-1 depicts different disciplines of capability-based planning and highlights to the right the viewpoints of system and business models to be elaborated further in this article. The figure depicts different viewpoints that can be adopted by different communities of interest within the military capability development process. Viewpoints applied in this article are highlighted to the right.

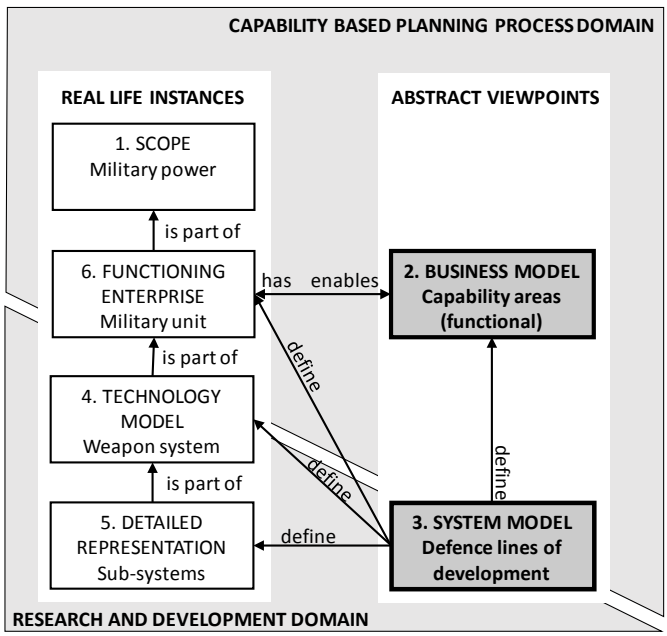



**Figure 6-1: Capability Perspectives and Viewpoints and Their Relations to Each Other (Adopted from Ref. [3]).**

These two models above provide us the framework within which to conduct our assessment of the potential of CRNs to contribute to the military capabilities. As suggested in Ref. [10], we shall consider the life-cycle of a military CRN, if needed, compressed into three phases of pre-deployment (i.e., capability planning,

procurement, and training), deployment (i.e., operations planning and implementation, monitoring, and maintenance), and post-deployment (i.e., withdrawal and cognition policies evaluation).

Furthermore, we shall consider three organizational levels of the military apparatus involved in potential development, procurement and use of the military CRNs, namely those of high-command (e.g., MoD, Joint Staff), operations command (e.g., Operations Headquarters, Combined Joint Task Force), and tactical level (e.g., brigade, battalion, company, end users).

Before commencing our analysis of the potential impact that military CRNs could contribute to military capabilities, we shall note that although this analysis concentrates on the cognitive networking layer specifically, CRNs do also need cognitive spectrum functions of lower ISO/OSI layers to achieve desired objectives. Based on the generic assessment of CRSs in Ref. [9] and Ref. [3], the cognition as a general feature is expected to:

- Lessen planning burden and shorten planning time;
- Facilitate automated configuration changes leading to adaptability;
- Improve the quality, availability, reliability, and timeliness of the information flows;
- Adopt reliable, efficient and fast dynamic spectrum access schemes appropriate for the situation at hand;
- Support improved interoperability; and
- Allow intelligent implementation of both tactical offensive and defensive electronic warfare measures, if so required.

## 6.3 ANALYSIS

Within our business model, and notably within the capability area *Prepare (R)*, we observe that automation reduces training burden on operators and shifts emphasis to the preparations needed to promulgate policies that direct and guide cognition, thus contributing to lower tier of *Force Preparation (R.1)*.

As cognition automatically implements node and network level technical “Lessons Learned” as well as local and networkwide “experimentation”, and as it facilitates maintenance and implementation of national intra- and international technical “interoperability”, we conclude that CRNs technically contribute to the tier of *Capability Development (R.2)* of the *Prepare*-capability area. The actual information exchange and communication services provided by a military CRN contribute directly to *Corporate Management and Support* tier (R.7).

CRN’s services and automated capability to adjust to the changing environmental factors support the capability area:

- *Project* and all its sub-tiers, from mounting to deployment, staging and basing.
- *Engage* and notably the tiers of Joint Manoeuvre (E.1), Joint Fires (E.2). Pending on the practical implementation of different protocols and waveforms, the CRN may support Non-kinetic Engagement, for example, by tactical self-protection jamming in conjunction with routing that supports the low probability of interception and detection (E.3).
- *Consult, Command and Control (C3)* improving all aspects and tiers within;
- *Protect* pending on the practical implementation notably within sub-tiers of security (P.1), defence against hostile action (P.2), and hazard mitigation (P.3).
- *Inform* by improving aspects and tiers of collection (I.1), processing (I.2), and dissemination (I.3).

Furthermore, within the components of our system model, the DOTMPLFI, we observe the following:

**Doctrine:** CRNs challenge armed forces in the pre-deployment phase especially by the elusive characteristics of cognition itself, which is difficult to quantify and specify for procurement by defence materiel administrations and acquisition offices. We recognize this as a potential future research topic. Within deployment phase, the perceived capability benefit from a CRN is improved availability and reliability of communications means. Besides natural and propagation challenges, CRNs may suffer from enemy kinetic and non-kinetic action, whereby, although reliable, the bandwidth requirements cannot always be met. Thus, a CRN is expected to inform users of bandwidth restraints. Doctrinally, this improved reliability could, in time, lead to modifications in regular reporting mechanisms across multiple military hierarchy layers, i.e., moving from regular reporting to continuous online status monitoring, leading to improved information sharing and improved situation awareness. Such changes in Standard Operating Procedures (SOP) can be foreseen, may be desirable, but are not mandatory nor forced by the adoption of CRNs. If CRNs employ artificial intelligence techniques – such as reinforcement learning or genetic programming – deployment time, post-deployment data collection, analysis, and policy updates need to take place and should be reflected in doctrine and SOPs.

**Organization:** The detailed knowledge and understanding of particulars of networking functions within a CRN should be automated and cognitive, thus lessening the burden on individual end users. However, a CRN will need appropriately configured policies to function correctly. Thereby, we foresee that functions of Signals Corps members shift at least one echelon higher than today to support the planning, preparation (pre-deployment), and surveillance (deployment) of the network instead of operating nodes themselves.

**Training:** Drawing again from the notion that CRNs in conjunction with cognitive spectrum management should make radio communications easier to use and more reliable for end users, we find it therefore reasonable to expect that training requirements of end users should decrease. Since there are a large number of end users, this should bring savings. The enhanced user experience together with improved reliability and increased availability may lead to secondary effects on behaviour, reporting procedures, and military operational applications. However, since planning and preparations of policies become essential, the training load on those planners and network supervisors will increase moderately. As these planners and supervisors are expected to be members of Signals Corps, it is to be expected that such training can be conducted by modifications to their already existing curricula.

**Materiel:** As already postulated, a military CRN could consist of CR nodes either in end-user mode or as intermediate nodes within the network, implying a potential solution space that facilitates different device configurations from lightweight, power-constrained handhelds to a powerful multi-antenna vehicle-mounted version. By the CR being an extension to the contemporary Software Defined Radio paradigm, most of the functionalities are expected to reside with the software, supported by databases containing measurement data as well as policies by which cognition is to be driven. A CRN can also be mostly software based. However, the network layer functionality would need network management functions that are expected to be operated at least one hierarchical layer above to the majority of end users. Conceptually, a CRN may include non-cognitive radio nodes if the network control function may set configuration parameters to those nodes. This can be achieved by minor modifications to the already existing base of contemporary SDRs but may not apply to legacy combat net radios. Although CRNs are expected to perform well in various contingencies with their own policy data and measurements, updates to policies may need to be inserted into the system from time to time. Can major policy changes be conducted over the air? Can they be implemented and enforced during active military operations? These questions, among others, need to be properly addressed before major acquisitions. Most importantly, the notion of cognition remains vague and under-specified within a military context,

implying that military procurement agencies or materiel administrations are unable to place contracts or to start procurement for short- to mid-term future. This is a subject for future studies.

**Leadership:** As already alluded to, the CRNs, and more broadly CRSs, may have an impact on the regular reporting procedures. More importantly, the notion of reliable and available communications facilitates improved timely information sharing, which leads to improved situation awareness and may facilitate self-synchronization among military units. Self-synchronization, however, is dependent on commander's leadership style and the competencies of his subordinates and is, therefore, one possible outcome of the deployment of CRNs, not precluding other leadership approaches should the commander choose otherwise [11]. Thereby we conclude that CRNs significantly contribute to the military C2 processes.

**Personnel:** The introduction of CRNs within the command and control structures may have a minor impact on the number of communications specialists and Signals Corps personnel needed especially in the lower end of the echelon as the ease of use allows regulars to operate CRs with minimal training. However, pre-deployment planning and preparation of the policies CRNs need for proper functioning may need more thorough and in-depth training, but as such functions are expected to be located higher in the echelon, numbers of such planners may be manageable, especially if combined with the role of network monitoring and supervision during the deployment.

**Facilities:** Memory and computational capacity needed to implement cognition are already available in high-end commercial handheld devices. Thereby, deployment of CRNs is not expected to give rise to any new space, weight, power, or heat requirements that advanced contemporary military radio systems would not already present. However, the network supervision and management, as well as planning and preparation of policies need software aided functionalities that may include some simulation capabilities to test policies before loading them to the network and devices. Such capabilities could precede the actual system development and procurement as the depicted planning, preparation, and simulation environment could also be used as a mechanism and a method for the overall CRN development activity itself[1].

**Interoperability:** Communications interoperability was one of the initial drivers for the first software-defined radio applications in the military domain, and programs, such as ESSOR, are just about to prove the notion. Thereby we conclude that interoperability itself would not necessarily be the primary driver for the adoption of CRNs, although noting that in a CRN, individual nodes may be, for example, SDR based, and as such a CRN could facilitate and support interoperability.

## 6.4 CONCLUSIONS

In this chapter, we explicitly concentrated on the military application of the CRNs. A notional military CRN was subjected to military capability development viewpoint, using capability areas as a business model and lines of development as a system model. We found that cognitive routing in military CRNs should choose a path minimizing interference to others, should be forward-looking in respect to link-availability, and mitigate occurrences of rerouting to improve throughput and to decrease delay. Topology control is a combination of processes to construct and maintain topology, which is performed on link information provided by lower layers beneath ISO/OSI-networking layer. In military CRNs, topology control mechanisms ensure good network energy efficiency, reduce energy consumption and rerouting, improve overall performance by minimizing delays, and maintain the connectivity of the CRN.

However, a multitude of metrics and measures of performance were identified with sometimes conflicting observations regarding their applicability, e.g., regarding the metrics' scalability. Thereby, we suggest that fundamental capacity benefits of the CRNs remain a fundamental research topic. We observed that CRNs

[1] IST-124 on Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency final report documents the use of cloud-based emulation environments in support of multi-national research and development.

challenge defence materiel administrations and acquisition offices because the notion of cognition itself remains unclear and undefined.

One benefit foreseen by the implementation of military CRNs is improved reliability and availability that, through improved information sharing and improved situation awareness, may lead, but would not force so, to the adoption of mission command and military unit self-synchronization. Based on the generic description of CRN, cognition is expected to ease planning burden, to shorten pre-deployment time, and to facilitate automated configuration changes. These together:

- Lead to adaptability;
- Improve the quality, availability, reliability, and timeliness of the information flows;
- Adopt reliable, efficient and fast dynamic spectrum access schemes appropriate for the situation at hand;
- Support improved interoperability; and
- Allow intelligent implementation of both tactical offensive and defensive electronic warfare measures, if required.

Large-scale adoption of CRNs is expected to shift functions of members of Signals Corps to higher echelon levels to support the planning, preparation (pre-deployment) and surveillance (deployment) of the network instead of operating devices and nodes themselves. CRNs are expected to perform well in various situations based on their own policies, data, and measurements. However, the question whether such policies could and should be adjusted or changed during operation should be addressed in future research. The requirement of computer-aided planning, preparation, and simulation environment was recognized, and development of such an environment could serve as a test and development platform for a broader combined CRS and CRN development activity.

This chapter adopted a two-pronged approach to articulate potential benefits CRN technology could deliver, namely by the use of a business model (capability hierarchy) and a system model (lines of development). However, future CRNs may be based on a variety of design concepts, architectural approaches, and several protocol implementations, thus leading to a certain level of ambiguity in our conceptual analysis. This cannot be avoided until the international R&D community starts to implement these different CRN building blocks for further scrutiny, e.g., through collaborative efforts suggested in the previous paragraph.

## 6.5 REFERENCES

[1] Anteroinen, J., “Integration of Existing Military Capability Models into the Comprehensive Capability Meta-Model,” in Systems Conference (SysCon), 2012 IEEE International, 2012, pp. 1-7.

[2] Anteroinen, J., “Enhancing the development of Military Capabilities by a Systems Approach,” Finnish National Defence University, 2013.

[3] Koivisto, J. and Tuukkanen, T., “Comprehensive Capability Meta Model tested by a Cognitive Radio,” in IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 2017, pp. 731-737.

[4] US DoD, “Directive: Capability Portfolio Management, Change 1,” 7045.20, 2017.

[5] “NATO Defence Planning Process,” 2017. [Online]. Available: www.nato.int/cps/en/natolive/topics_49202.htm. [Accessed: 04-2017].

[6] NATO, "Bi-SC Capability Hierarchy," SH/PLANS/JCAP/FCP/15-310118, 2015.

[7] ACT, "What is Transformation? An Introduction to the Allied Command Transformation", 2015. [Online]. Available: http://www.ieee.es.

[8] Tuukkanen, T. and Anteroinen, J., "Initial Assessment of Proposed Cognitive Radio Features from a Military Perspective," 18th International Command and Control Research and Technology Symposium, Alexandria, VA, USA, 2013.

[9] Tuukkanen, T. and Anteroinen, J., "Framework to Develop Military Operational Understanding of Cognitive Radio", in International Conference on Military Communications and Information Systems (ICMCIS), Krakow, Poland, 2015, pp. 1-9.

[10] Bräysy, T., Tuukkanen, T., Couturier, S., Verheul, E., Smit, N., Buchin, B., Le Nir, V. and Krygier, J. "Network Management Issues in Military Cognitive Radio Networks," in International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017.

[11] Vassiliou, M. and Alberts, D., "C2 Failures: A Taxonomy and Analysis," in 18th International Command and Control Research and Technology Symposium, Alexandria, VA, 2013.

# Chapter 7 – COGNITIVE RADIO NETWORK SYSTEM ARCHITECTURE FRAMEWORK

In this chapter, we propose a system architecture framework for a CRN. This architecture framework is a result of the investigations conducted in the previous chapters. Even though these investigations were focused on the network layer, they clearly pointed out the requirement for cross-layer capability in a CRN. Therefore, this chapter starts with a closer look at cross-layer aspects and, based on this, yields a proposal for an architecture framework.

## 7.1 CROSS-LAYER ASPECTS

The traditional protocol stack consists of isolated layers whose tasks are defined explicitly and which provide only services to adjacent layers. This has the advantage of simplicity and modularity in the design, which facilitates the standardization process. However, this creates some problems, such as inefficiencies and a decrease in capacity.

For example, the use of the TCP in wireless systems using the traditional protocol stack with isolated layers is inefficient, as TCP has been designed for wireline systems assuming that congestion is solely due to problems on the transport layer. However, in wireless systems, congestion can be due to problems on the lower layers, and no information can be gathered from these lower layers using the traditional protocol stack. A solution to this problem is cross-layer information exchange.

According to Ref. [1], cross-layer design can be defined as “Any kind of innovation on the traditional structure that blurs, changes, or even removes the boundaries between layers”. There are numerous cross-layer designs in the literature. Cross-layer allows information to flow upward/backward through the OSI layers. Cross-layer designs in the scope of cognitive networks are surveyed in Ref. [2].

### 7.1.1 An Example of a Cross-Layer Design for a Cognitive Radio Networks Node

A cross-layer model for a CRN node is presented in Ref. [1] and in Figure 7-1, in which a cognitive engine interacts with the different layers of a protocol stack, taking into account information from sensors and building knowledge from/to memory.

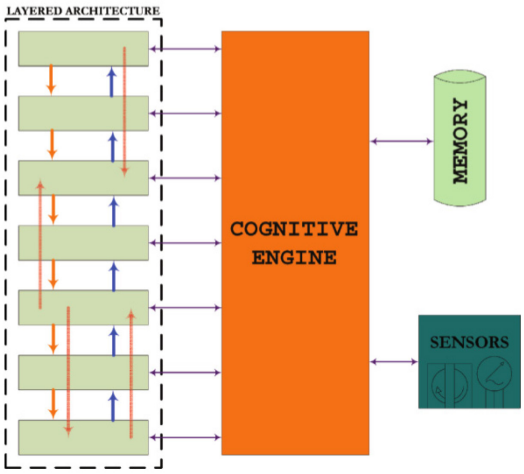



**Figure 7-1: A Model of a CRN Node with Cross-Layer Connections and Cross-Layer Information Exchange Through the Cognitive Engine [1].**

Within the cross-layer architecture, control information can be exchanged between arbitrary layers of the protocol stack. For example, link information can be passed to the network layer, which can be used to select more stable or higher capacity routes. Information from the network layer might drive the cognitive engine to choose a different frequency. These examples show that there are two ways of interaction between layers, one option is to send directly from one layer to the other, and the other option is to send information from one layer to the cognitive engine, whose decision might have an influence on the other layer.

A list of parameters that could be relevant for optimization through the cognitive engine is given in Ref. [1] and Figure 7-2, below.

| Layer | Parameters |
|---|---|
| **RF** | Antenna powers |
| | Dynamic range |
| | Pre-distortion parameter |
| | Pre-equalization parameter |
| **Physical layer** | Transmit power |
| | Digital modulation order |
| | Carrier frequency |
| | Operation bandwidth |
| | Processing gain |
| | Duty cycle |
| | Waveform |
| | Pulse shaping filter type |
| | FFT size (for OFDM) |
| | Cyclic prefix size (for OFDM) |
| **Data link layer** | Channel coding rate |
| | Channel coding type |
| | Packet size |
| | Packet type |
| | Data rate |
| | Interleaving depth |
| | Channel/Slot allocation |
| | Carrier allocation (in multi-carrier systems) |
| | MAC scheduling algorithm |
| | Handover (Handoff) |
| | Number of slots |
| **Network** | Routing algorithm/metric |
| | Clustering parameters |
| | Network scheduling algorithm |
| **Transport** | Congestion control parameters |
| | Rate control parameters |
| **Upper** | Communication modes (simplex, duplex, etc.) |
| | Source coding |
| | Encryption |
| | Service personalization |

**Figure 7-2: Adaptation Parameters for Cross-Layer Architecture [1].**

### 7.1.2 Examples of Cross-Layer Information Exchange

Every layer can profit from information from any other layer, as long as there are metrics or knobs in this layer. We list a few examples of cross-layer information exchange that were pointed out in the previous sections as beneficial:

- OLSRv2 uses link information to improve the routing. Information on multiple channels or frequencies could also be used to improve the routing of OLSRv2.
- Topology control gets information from the link layer on different frequencies and the used transmission power.

- The hierarchy of a military network needs to be taken into account in routing, topology control, and clustering. Potential sources of information are policies and applications.
- New connection management and congestion control mechanism, which take into account spectrum sensing, spectrum changes, route failure, and mobility prediction, are required for the transport layer.
- Clustering itself is a link layer issue but has influence on the network layer. Information from the physical layer (power, frequencies) and from the network layer (throughput, etc.) is to be taken into account.
- The control channel exchanges information from different layers (sensing information from the physical layer, routing information from the network layers, reliability information from trust management).

### 7.1.3 Example Metrics and Configuration Parameters for Cognitive Radio Networks

In the CRN research, the cross-layer mechanism is intended to make information from different OSI layers available to the nodes network layer. When information must be shared between different nodes, a common control channel is required.

These two mechanisms will bring cognition into the nodes' network layer and into the network itself. The network can then use this information to optimize the end-to-end connectivity in the network. To get an idea of some practical improvements that cognition can bring, a list of parameters is given with the possible benefits for the network's end-to-end connectivity. This list is just a limited example and intended to give a better understanding of the benefits that CRNs can bring.

#### 7.1.3.1 Battery Power

When the battery power of a certain node is low, the network can discourage other nodes to use this node as a relay node in case other relays are available. This will enhance the lifetime of the battery of the node and gives the network more endurance.

#### 7.1.3.2 Transmit Power

Battery lifetime can be enhanced when transmit power can be reduced in case of sufficiently strong signal strength. Increasing transmit power will improve bad quality links in the network.

#### 7.1.3.3 Radio Frequency

Clustering can be achieved by assigning different frequencies to different clusters. This way, the use of frequencies can be an instrument for network management.

#### 7.1.3.4 Spectrum Occupancy

For network management, it is useful to know the spectrum occupancy in the area of all network nodes to choose the best frequency for network optimization rather than point-to-point optimization.

#### 7.1.3.5 Congestion

Especially in radio traffic, congestion usually has a different reason than in wired networks. In radio networks congestion is usually related to a degraded radio link, while in wired networks the amount of traffic from the application or transport layer is the cause. The solution in radio networks is therefore different from the solution in wired networks; more retries instead of backing off. Congestion information can help the CRN to deal with congestion in the most optimal way.

#### 7.1.3.6 Position Information

Position information can help with topology control. It can be used in combination with the transmit power parameter.

#### 7.1.3.7 Topology Update Frequency and Topology Convergence Time

The control traffic can become a substantial part of the overall traffic when the topology update frequency is high. Moreover, all nodes must have a common view of the network topology. A trade-off must be found between the topology update frequency, the control traffic and the topology convergence time. In the case of congestion, a different topology can be adopted based on a different radio frequency.

#### 7.1.3.8 Dynamic Control Information Overhead

The management of CRN increases the amount of control information to be shared between the nodes (battery power, transmit power, radio frequency, etc.). The control information must be kept to a low percentage in comparison to the overall traffic. Depending on the required update frequencies of the different control information and the load of the traffic, dynamic control information allows to exchange most of the information between nodes when the traffic load is low and to have a low percentage of the control information when the traffic load is high.

#### 7.1.3.9 Sensing Time

Sensing time is very important to improve bandwidth utilization of CRNs. It allows to identify the presence of primary users or jammers and to vacate the band, if necessary.

#### 7.1.3.10 Channel Availability

Channel availability is a key parameter for an effective design of channel selection strategies, as well as routing metrics in CRNs. The availability of a channel dynamically varies in time due to the changes of the users' relative positions.

#### 7.1.3.11 End-to-End Throughput/Delay/Energy Consumption

End-to-end throughput is the ratio of packets received by the destination to the packets sent by the source. End-to-end delay is the sum of time taken from the source to the destination for a packet to reach. End-to-end energy consumption is the amount of energy necessary to convey the packets from the source to the destination. The optimization of end-to-end throughput/delay/energy consumption of CRN has many impacts on the network layer (routing, topology control, etc.).

#### 7.1.3.12 Route Recovery Time

The route recovery time can be a critical factor affecting the network performance. Adequate routing algorithms should be chosen to restore the route as fast as possible using for instance a different radio frequency.

#### 7.1.3.13 Channel Handoff Time

Mechanisms to reduce the channel handoff time should be taken into account in the networking protocols. For instance, pre-configured radio frequencies can be made available to all radios, in case of jamming, to switch to another channel instead of using a multiple channel rendezvous protocol.

## 7.2 ARCHITECTURE FRAMEWORK PROPOSAL

This section presents different CRN architectures found in literature (Sections 7.2.1 to 7.2.6) and, from these, develop a proposal for an architecture framework (Section 7.2.7), that provides the functionality required by military mobile ad hoc CRN. Elements of the architectures from literature that are used for the proposal are highlighted.

### 7.2.1 Typical Structure of a Military Mobile Tactical Network

Military mobile tactical networks typically feature a hierarchical setup. Figure 7-3 depicts such a setup.

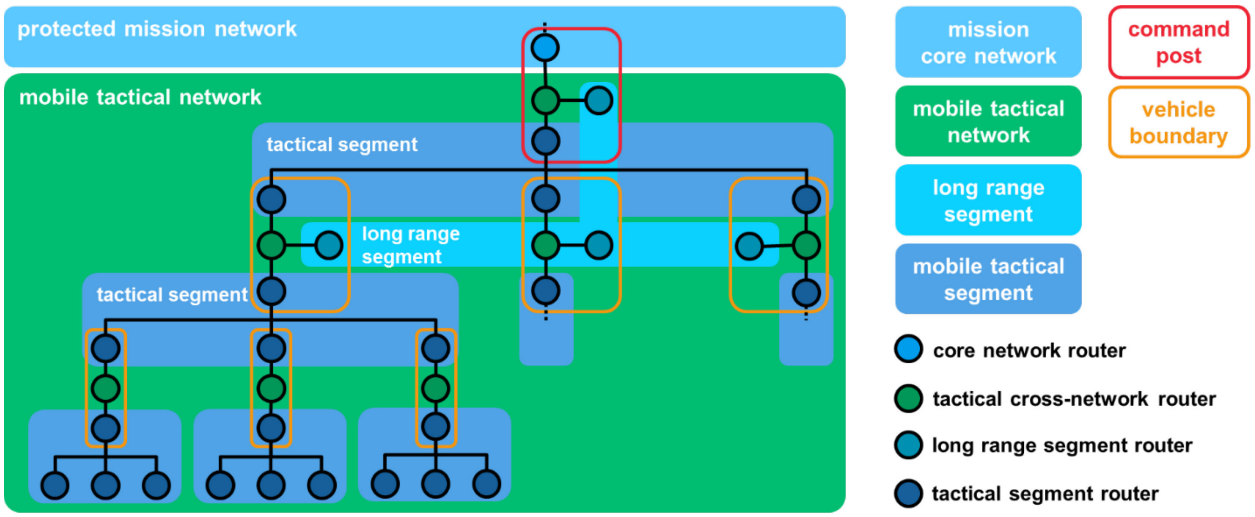



**Figure 7-3: Typical Structure of a Military Mobile Tactical Network.**

In the more complex nodes, a tactical router is typically used to connect the heterogeneous communications subsystems. Figure 7-4 depicts such a setup.

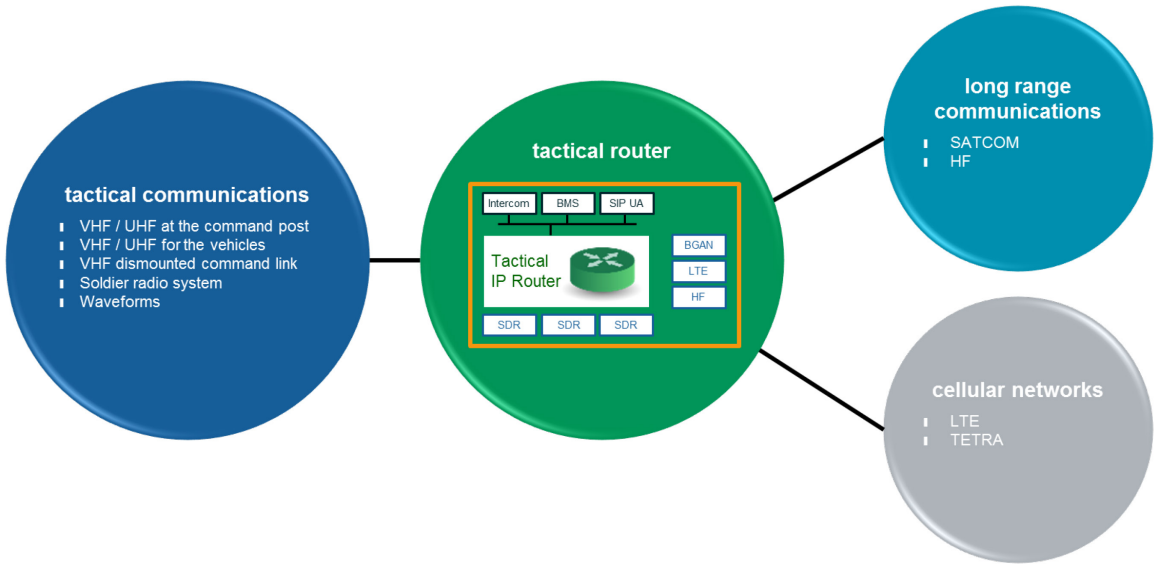



**Figure 7-4: Typical Building Blocks of a Military Mobile Communication System.**

### 7.2.2 The Cognitive Cycle in Cognitive Networks

Ref. [3] introduces an interlocked unilateral and multilateral cognitive processing (see Figure 7-5).

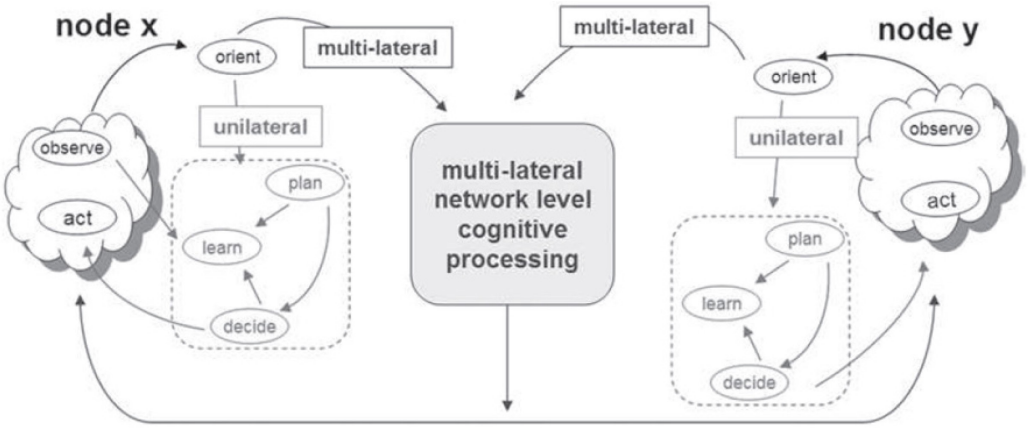



**Figure 7-5: Multilateral Cognition in a Network.**

The underlying idea is that for a CR "the cognition cycle is a state machine that shows the stages in the cognitive process for a cognitive radio […]. In network terms, the cognition cycle tends to model the process that occurs at a node and thus does not fully capture the network elements of the process. To frame the operation for a cognitive network, therefore, the cognition cycle needs to be expanded." It should be expanded to include all network elements in the process. The key point is the fact that two distinct levels of processing exist that can be denoted as node-level cognitive processing and network-level cognitive processing.

This concept is well suited for both cellular networks as well as ad hoc networks. Cellular networks are based on infrastructure and the existence of a reliable control channels. Thus, they allow for centralized cognitive processing. Ad hoc networks are based on the concept of processing network decisions on node-level – albeit ad hoc nodes feature less self-awareness in comparison to CRN nodes. Figure 7-6 compares the consequences of applying the concept to a cellular network, as depicted on the left, and an ad hoc network, as depicted on the right.

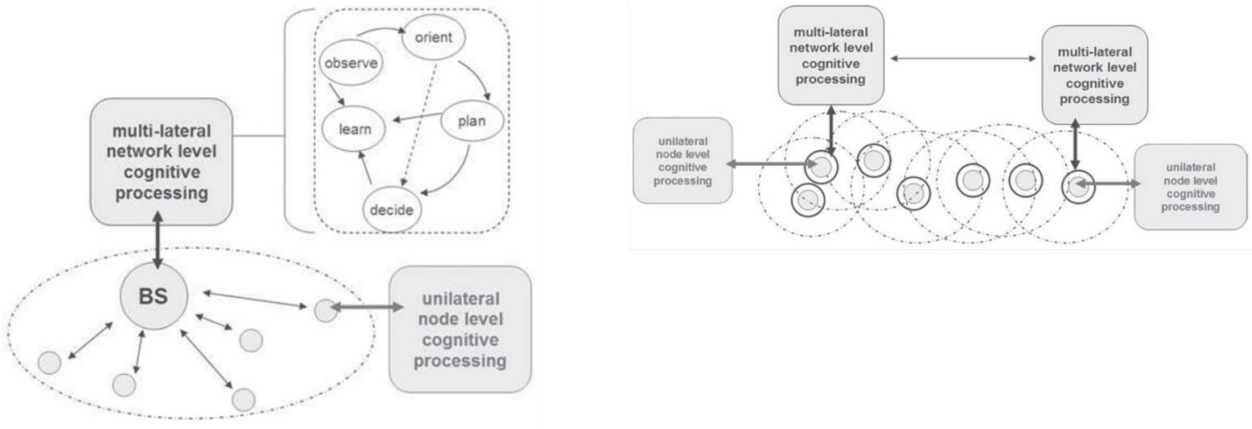



**Figure 7-6: Structural Implications of the Network's Organization.**

### 7.2.3 Cognition in a Military Mobile Tactical Network

Military mobile tactical networks regularly cannot be based on infrastructure and consequently have to network in an ad hoc manner without being able to employ a reliable control channel (see Figure 7-7).

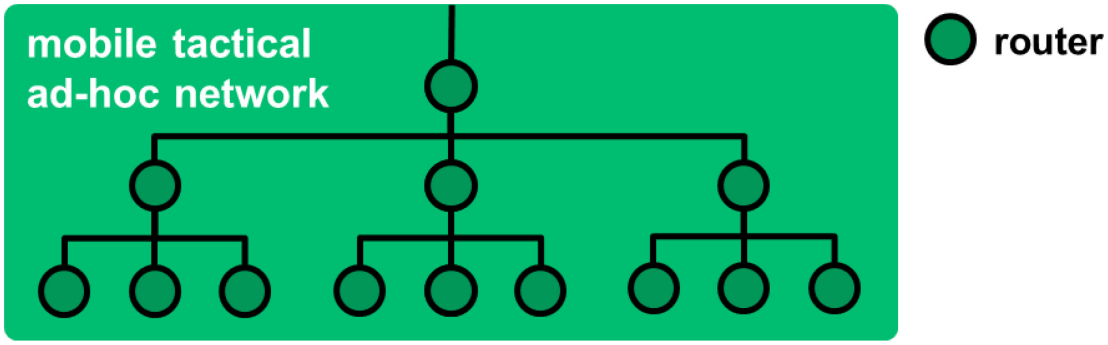



**Figure 7-7: Structure of a Military Mobile Tactical Network.**

Thus, when the concept of unilateral and multilateral cognitive processing is applied to military mobile tactical networks (see Figure 7-8), the cognitive processing will reside on node level, i.e., be decentralized, and the exchange of knowledge between the nodes will be performed in an ad hoc manner.

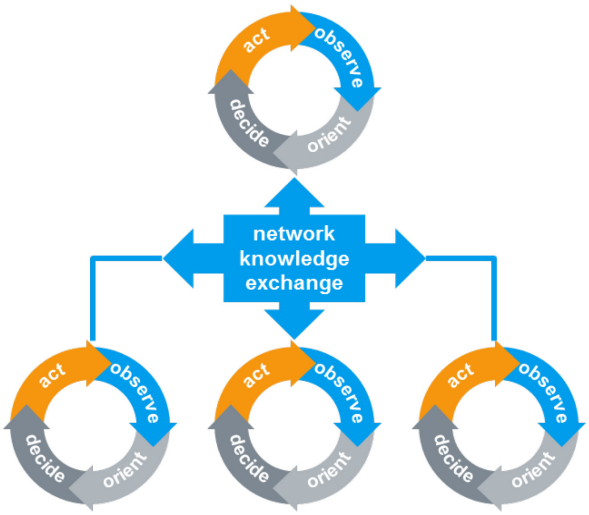



**Figure 7-8: Knowledge Exchange in a Military Mobile Tactical Network.**

### 7.2.4 Interfaces Between Cognitive Elements and End-to-End Objectives

Cognitive networks require the ability to share knowledge and interpret end-to-end objectives. Ref. [4] presents the concept of domain specific languages to facilitate this task (see Figure 7-9).

The underlying idea is that beyond the physical requirements to sense the RF environment and arbitrate access to shared spectrum, cognitive networks require the ability to share knowledge and interpret end-to-end objectives. These two functions are accomplished via two interfaces:

- An interface to the other cognitive elements in the network; and
- An interface to the sources of the network's end-to-end objectives.

These interfaces require languages to pass messages between the cognitive elements and these entities – messages from other cognitive elements and messages from applications, users and processes requiring end-to-end support.

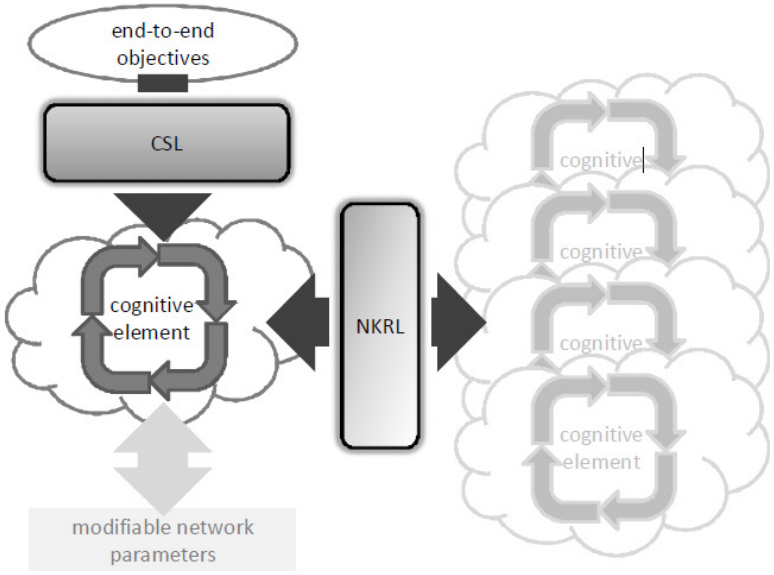



**Figure 7-9: Interfaces Between the Various Cognitive Elements and the End-to-End Objectives.**

The concept is that two languages should be used to communicate and represent information at each interface:

- The Network Knowledge Representation Language (NKRL) stores and communicates knowledge between cognitive elements; and
- The Cognitive Specification Language (CSL) bridges the interface between the end-to-end goals and the cognitive elements.

This concept was integrated into the proposed architectural framework.

### 7.2.5 Cognitive Resource Manager Framework as a Reference for Developed APIs

Ref. [5] presents a generic interface architecture to support cognitive resource management in wireless networks (see Figure 7-10).

The underlying idea is that of a Cognitive Resource Manager (CRM) that is a relatively small unit and acts like a microkernel type of operating system for CRs. It is responsible for coordinating the information exchange between functional modules through well-defined interfaces.

The concept is that information collected through the generic interfaces is used for optimization and modelling. The “toolbox” and library modules comprise a variety of optimization and modelling mechanisms and functional algorithms. Different end-to-end and local optimization processes are executed independently in a coordinated fashion, and final decision making is performed under the CRM framework.

The architecture framework proposed in this document is heavily based on this cognitive resource manager framework.

### 7.2.6 Essential Cognitive Radio Networking Functionalities and Relations

Ref. [6] presents an architecture proposal from a network management viewpoint, depicted in Figure 7-10.

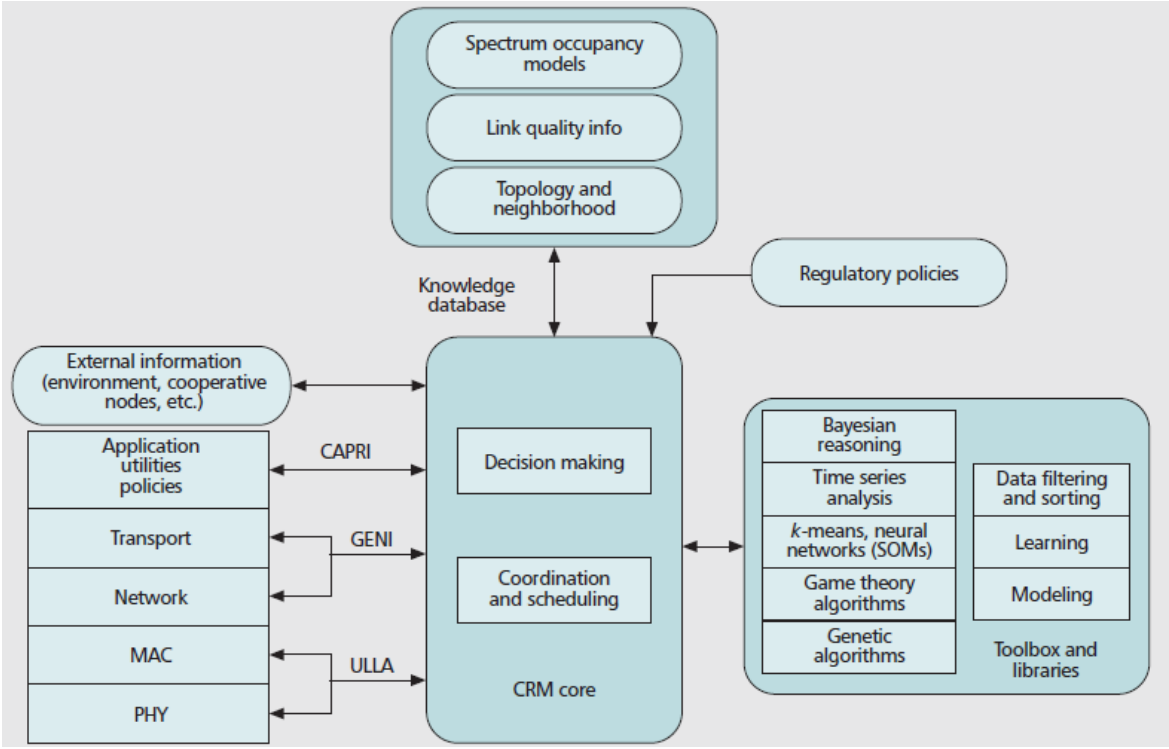



**Figure 7-10: Cognitive Resource Manager Framework as a Reference for Developed APIs.**

The underlying idea is that the CR has a Cognitive Radio Engine (CRE) to handle the spectrum management capabilities and a Cognitive Network Engine (CNE) to manage the networkwide end-to-end optimization. The cognitive cycles of CRE and CNE are interlocked, and one could even say that CNE emerges as a result of cooperating CREs. In this view, CNE is obviously a distributed entity. In any case, the cognitive cycles of CRE and CNE operate at different speeds, since CRE manages fast changing link-level parameters, while CNE is concerned with more slowly varying networkwide phenomena.

The concept is that the node centric functions and the networkwide functions can be viewed as separate functional entities and can be realized by separate cognitive engines.

The proposed architectural framework has the flexibility to support this approach.

### 7.2.7 Proposed Architecture

Figure 7-11 displays the architecture framework proposal for a CRN node.

The proposal is a high-level description of the required modules and their interfaces. The interfaces are taken from the literature. The Cognitive Specification Language (CSL) specifies an interface between the end-to-end objectives and the cognitive elements, the Network Knowledge Representation Language (NKRL) describes the storing of knowledge and facilitates communication between the cognitive elements. The Cross-Layer Interface (CLI) enables monitoring and configuration of the local node, and the toolbox and library modules provide optimisation and modelling mechanisms and functional algorithms.

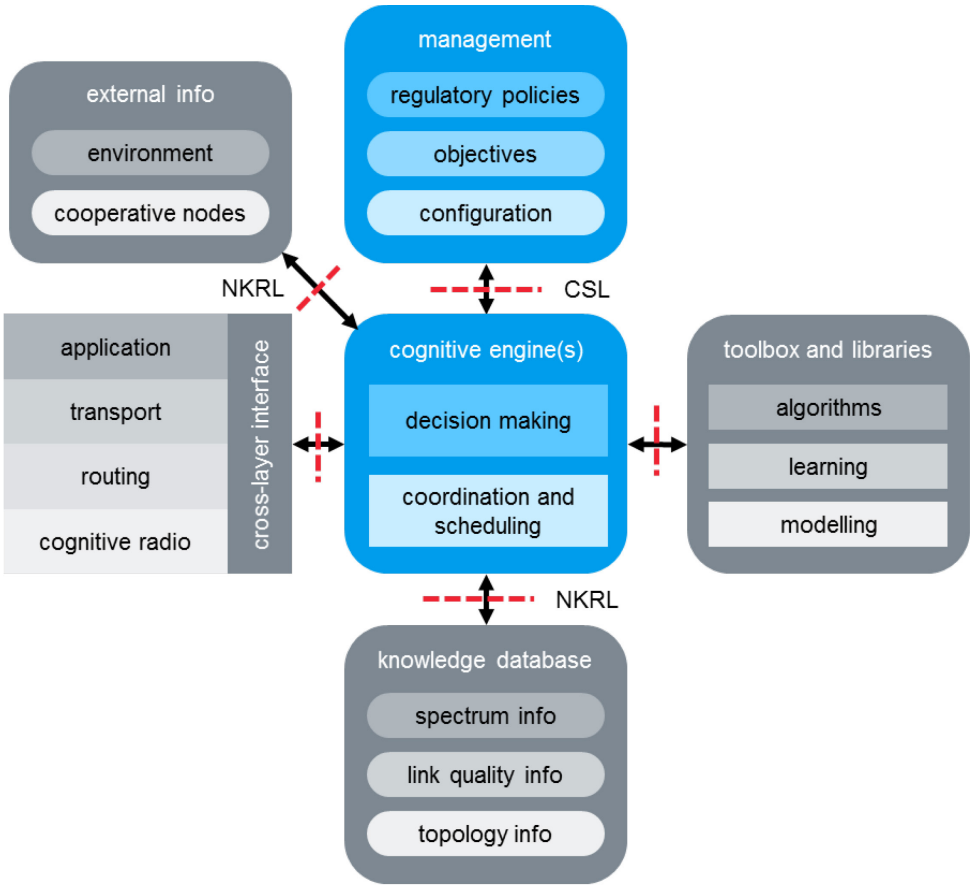



**Figure 7-11: Architecture Framework Proposal for a CRN Node.**

## 7.3 REFERENCES

[1] Arslan, H., "Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems", Springer, 2007.

[2] Mansoor, N., Islam, A.K.M., Zareei, M., Baharun, S., Wakabayashi, T. and Komaki, S., "Cognitive Radio Ad-Hoc Network Architectures – A Survey", Wireless Personal Communications, 2014.

[3] Doyle, L. and Forde, T., "The Wisdom of Crowds: Cognitive ad hoc Networks", in "Cognitive Networks: Towards Self-Aware Networks", John Wiley & Sons, 2007.

[4] DaSilva, L.A., MacKenzie, A.B., Da Silva, C.R.C.M. and Thomas, R.W., "Requirements of an Open Platform for Cognitive Networks Experiments", 2009.

[5] Sooriyabandara, M., Farnham, T., Mahonen, P., Petrova, M., Riihijarvi, J. and Wang, Z., "Generic Interface Architecture Supporting Cognitive Resource Management in Future Wireless Networks", IEEE Communications Magazine, Vol. 49, Issue 9, September 2011.

[6] Bräysy, T., Tuukkanen, T., Couturier, S., Verheul, E., Smit, N., Buchin, B., Le Nir, V. and Krygier, J., "Network Management Issues in Military Cognitive Radio Networks", 2017.

# Chapter 8 – CONCLUSIONS AND RECOMMENDATIONS

CRNs are expected to become the next step in the evolution of radio networks, as their autonomous adaptation capability promises robust, reliable, and efficient communications while requiring less management efforts than today's radio networks. As these properties appear advantageous also for tactical networks in national and multi-national operations, this RTG was tasked to investigate the usage of CRN technology in NATO environment.

While challenges for the usage of CRNs in the military domain had already been addressed in the preceding ET, "Network Aspects of Cognitive Radio" (IST-ET-074), also the results of other NATO RTGs working on similar topics have been followed, namely, "Cognitive Radio in NATO" (IST-077) and "Cognitive Radio in NATO II" (IST-104). In addition to them, the progress of the group on "Heterogeneous Tactical Networks" (IST-124) has been observed.

## 8.1 CONCLUSIONS

In this report, we have identified the requirements and further challenges on how to bring cognition into radio networks. Scenarios and vignettes have been developed that establish whether CR and CRN techniques do outperform legacy systems and offer new solutions to existing communication problems. Based on that, current networking technologies have been analysed regarding their support for military CRNs. That included identifying advantages when using cognition as well as regarding the military requirements for tactical networks. Based on that, solutions for the networking technologies have been explored, and an architecture framework on CRN has been proposed. Moreover, potential impact of the deployment of CRN technologies to military capabilities has been assessed.

According to our understanding, CRNs attempt to achieve end-to-end optimization in multi-hop communications. Cognition can influence not only the spectrum access, but all parameters of the network and its nodes. This requires cross-layer information exchange. Decisions taken by the cognitive engine(s) may need to deconflict between node and network objectives.

Decisions taken in CRN may furthermore need to regard the interoperability to legacy devices. Dependent on their capabilities, e.g., the possibility for over-the-air reconfiguration, they may be controlled by CRN.

Routing should be able to react on information regarding frequency availability and energy availability at each node of the network. Especially for military network this requires a combination of proactive and reactive routing protocols for being able to make use of the advantages of both approaches.

Also, TC should take into account the frequency availability in order to identify the optimal links between all nodes. As the frequency availability, as well as other important information (e.g., the distance to neighbouring nodes), changes over time and, due to mobility, it is important to adequately update topology information. A possible lack of these updates (e.g., due to radio silence) must be regarded.

Data transport should be able to react on problems on the route. Therefore, there is a need for the end nodes to be informed about e.g., congestion or frequency unavailability on intermediate nodes. In order to collect all relevant information about this at a node, cross-layer information exchange is required. Based on these capabilities, an enhanced TCP named "M-TCP-CE" is proposed.

Clustering should support both the military structures as well as the requirements of other technologies, such as TC. Thus, the network structure should be optimized to efficiently use the available resources (spectrum, energy, etc.).

Management should be supported by cognition, as it helps automatizing the management before, during and after a mission. Nevertheless, still a trade-off between automatization and human control is needed. Traditional management approaches need to be enhanced for managing policies. In addition to that, frequency management becomes more important, as it needs to include information from different layers.

Military networks should support trust management. Trust management is required to allow nodes to trust in each other. It especially refers to cognitive engines, which need to exchange control information between the nodes. A trust management system named "TUBE" is proposed, which observes control messages received and redirected to other nodes and assesses the level of their reputation.

The control channel should be dynamically resized to the current needs of the network, because highly varying information from several different technologies must be transmitted quickly. As dynamism requires negotiation between nodes, which introduces a delay to the transmission, a trade-off between dynamic and delay needs to be found. The coverage of a control channel is related to the applied clustering, as described in Section 4.7.2.3.

SDN concepts seem promising and warrant further scrutiny for application in CRAHNs.

The advantages of military CRN compared to legacy networks should be validated via network simulations, but there is currently no open simulation environment available for easily setting up CRN simulations.

The support of CRN for military capabilities has been analysed. For that, the DOTMLPFI system model has been applied. As CRN are still in an early stage of development, the analysis found some ambiguities, but nevertheless expects several improved capabilities due to the application of cognition.

Cross-layer information exchange has been recognized as a pillar of the analysed CRN technologies. Several examples for this have been described; a full list of exchange interfaces needs to be developed as part of a full CRN architecture. A framework for such architecture has been proposed, which already introduces the functional blocks of a CRN and the interfaces between them.

## 8.2 RECOMMENDATIONS

Operational deployments of CRN do not yet exist today. Even though the research in this group has taken their development a step further, it will not be possible to start building CRN now. This means that further research is required to increase the Technology Readiness Level (TRL). This group has considered CRNs to remain at low TRL. In order to increase the TRL, the group has identified the following recommendations.

One important finding was that the behaviour of systems that are highly adaptive will have to be constrained by policies. Appropriate policies need to be developed and tested in preparation for the introduction of CR technologies into the marketplace by industry. Therefore, it is recommended that NATO (spectrum managers and the subsequent RTG) consider appropriate coalition policies for dynamic spectrum access. Considering the enhanced cognitive capabilities of CRN, policies may not only concern spectrum access but all parts of the radio. Such policies are currently being investigated in the NATO group on "Electromagnetic Environment Situational Awareness" (IST-146). Consequently, it is recommended to consider the results of this group in the further research and development of CRN technology.

For the introduction of CRN in the military domain, there is a need to be aware of any additional vulnerability issues that are opened up. Some of these vulnerabilities have been identified in this report, but have not been analysed intensively and therefore require further investigations. Consequently, we recommend that vulnerabilities and security issues for military CRN are addressed in appropriate entities, and that the results are taken into account by system designers.

In order to take the next step towards the realization of the enhancements identified in this group, we recommend setting up an RTG on the development of an architecture for a cognitive tactical radio system. This architecture could be based on the architecture framework described in this report. The development will require the group to work on the description of the global goals, the decomposition of the system, the definition of interfaces, the detailed description of the functional blocks and their goals, and the application of cognitive sciences in a military system (artificial intelligence, machine learning …).

A further step will be the validation of the findings. A promising approach for this is the setup of a demonstrator for military CRN based on a network simulation, which will require a huge amount of efforts. Therefore, we recommend exploring validation approaches and strategies for all further steps in the realization of CRN technologies (policies, architecture, etc.). Successfully validated findings should furthermore be considered when creating a STANAG on CRN technologies.

For making use of all advantageous introduced by CRN, concepts for the usage of CRN in NATO need to be developed. We recommend mandating respective authorities with the creation of such concepts.

# Annex A – PRESENTATIONS AND PUBLICATIONS

Couturier, S., Bräysy, T., Buchin, B., Krygier, J., Le Nir, V., Smit, N., Tuukkanen, T., and Verheul, E. "Cognitive Radio Networks – Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management", Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio (WInnComm-Europe), Paris, France, October 2016.

Bräysy, T., Couturier, S., Smit, N., Le Nir, V., Tuukkanen, T., Verheul, E., Buchin, B., and Krygier, J. "Network Management Issues in Military Cognitive Radio Networks", International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, May 2017.

Couturier, S., Bräysy, T., Buchin, B., Krygier, J., Le Nir, V., Smit, N., Tuukkanen, T., and Verheul, E., "End-to-End Optimization for Tactical Cognitive Radios", International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, May 2018.

Tuukkanen, T., Bräysy, T., Buchin, B., Couturier, S., Krygier, J., Le Nir, V. , Smit, N., and Verheul, E. "Assessment of Cognitive Radio Networks through Military Capability Development Viewpoint", International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, May 2018.

# REPORT DOCUMENTATION PAGE

| 1. Recipient's Reference | 2. Originator's References | 3. Further Reference | 4. Security Classification of Document |
|---|---|---|---|
| | STO-TR-IST-140<br>AC/323(IST-140)TP/874 | ISBN<br>978-92-837-2198-7 | PUBLIC RELEASE |

**5. Originator**

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

**6. Title**

Cognitive Radio Networks: Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management

**7. Presented at/Sponsored by**

Final Report of IST-140.

| 8. Author(s)/Editor(s) | 9. Date |
|---|---|
| Multiple | October 2019 |
| **10. Author's/Editor's Address** | **11. Pages** |
| Multiple | 146 |

**12. Distribution Statement**

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

**13. Keywords/Descriptors**

Clustering
Cognitive radio networks
Control channel
Data transport
Network management
Routing
Topology control
Trust management

**14. Abstract**

One of the most important aspects in today's military missions and operations is information superiority. Gathered information shall be available at the right place at the right time in all situations. For its distribution, communication networks are used. Consequently, there is a requirement for adaptability of such networks to all possible situations, which may lead to a certain complexity. Despite this complexity, they shall be robust, efficient, and easy to handle.

The Cognitive Radio Network concept is a promising solution for this, as such networks can monitor their internal states as well as external influences, like changes in the spectral environment, and to react on them autonomously. In this report, networking technologies, such as routing, topology control, data transport, and network management, are analysed regarding their potential for supporting end-to-end optimization, and solutions for cognitive enhancements are proposed. These enhancements are specifically tailored to the needs of tactical communications. Based on the findings, a new architecture framework for Cognitive Radio Networks is proposed, which can be seen as a starting point for the standardisation and development of cognitive tactical radio systems.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

**DIFFUSION DES PUBLICATIONS**
**STO NON CLASSIFIEES**

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

## CENTRES DE DIFFUSION NATIONAUX

**ALLEMAGNE**
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

**BELGIQUE**
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

**BULGARIE**
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

**CANADA**
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

**DANEMARK**
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

**ESPAGNE**
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

**ESTONIE**
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

**ETATS-UNIS**
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

**FRANCE**
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

**GRECE (Correspondant)**
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

**HONGRIE**
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

**ITALIE**
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

**LUXEMBOURG**
*Voir* Belgique

**NORVEGE**
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

**PAYS-BAS**
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

**POLOGNE**
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

**PORTUGAL**
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

**REPUBLIQUE TCHEQUE**
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

**ROUMANIE**
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

**ROYAUME-UNI**
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

**SLOVAQUIE**
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

**SLOVENIE**
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

**TURQUIE**
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

## AGENCES DE VENTE

**The British Library Document Supply Centre**
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

**Canada Institute for Scientific and Technical Information (CISTI)**
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

**DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS**

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

## NATIONAL DISTRIBUTION CENTRES

**BELGIUM**
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

**BULGARIA**
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

**CANADA**
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

**CZECH REPUBLIC**
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

**DENMARK**
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

**ESTONIA**
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

**FRANCE**
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

**GERMANY**
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

**GREECE (Point of Contact)**
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

**HUNGARY**
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

**ITALY**
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

**LUXEMBOURG**
*See* Belgium

**NETHERLANDS**
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

**NORWAY**
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

**POLAND**
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

**PORTUGAL**
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

**ROMANIA**
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

**SLOVAKIA**
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

**SLOVENIA**
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

**SPAIN**
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

**TURKEY**
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

**UNITED KINGDOM**
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

**UNITED STATES**
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

## SALES AGENCIES

**The British Library Document Supply Centre**
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

**Canada Institute for Scientific and Technical Information (CISTI)**
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2198-7