Network management issues in military cognitive radio networks

Timo Bräysy
Centre for Wireless Communications
University of Oulu
Oulu, Finland
timo.braysy@oulu.fi

Stefan Couturier
Fraunhofer FKIE
Wachtberg, Germany

Niels Smit
Ministry of Defence,
Utrecht, Netherlands

Vincent Le Nir
Royal Military Academy
Brussels, Belgium

Erik Verheul
Royal Netherlands Navy
Ministry of Defence,
Den Helder, Netherlands

Boyd Buchin
Rohde & Schwarz
Munich, Germany

Jaroslaw Krygier
Military University of Technology
Warsaw, Poland

Topi Tuukkanen
Finnish Defence Research Agency
Riihimäki, Finland

***Abstract*—Cognitive Radio (CR) was designed to support flexible spectrum usage by adding spectrum sensing facilities and decision making logic to the radio devices. Cognitive Radio Network (CRN) is an extension of the CR concept to enable holistic end-to-end optimization of the network operation and services. We discuss CRN management issues in the context of military and tactical operation environments, where the key feature is the temporal nature of the network installations. Our special interest is in the wireless ad hoc network solutions. The network lifetime may extend from just hours to several days. The limited lifetime of the networks makes it both possible and necessary to define the management functionalities with respect to different mission phases. Traditional FCAPS (Fault, Configuration, Administration, Performance, and Security) functions and their required actions are therefore detailed to some level at each operational phase (before, during and after mission). We will emerge the idea that as the cognitive and autonomous technologies will be developed to operate communication networks and become trustworthy enough to be applied also in tactical context, they will most likely first be applied in the during mission phase. Of course, this phase is also the most critical in the sense that it is here that lives are at stake. To answer this critical issue, the policy management must be seen as an equally critical functionality. It is necessary to develop the interconnection between mission goals and defined policies so that the Cognitive Network Engine (CNE) determining the operational parameters of the network, in all situations provides a reliable and failsafe communication solution to be utilized.**

Keywords—cognitive radio networks; network management; military; tactical

I. INTRODUCTION

We propose a cognitive radio network architecture for military specific applications of communication networks. Our attention is on Cognitive Radio Networks (CRNs) as defined e.g. in [1]. Cognitive radio has originally been designed to support flexible spectrum usage by adding spectrum sensing facilities and decision making logic to the radio devices. Therefore, cognitive network can be understood as a network wide solution to realize the flexible spectrum use according to Primary User (PU) and Secondary User (SU) paradigm. The approach in this paper is wider since we approach the cognitive network as a method to enable holistic end-to-end optimization, not just in a sense of spectrum usage. Examples of such network wide goals are quality-of-service (QoS) of data transfer, network reliability and security. We pay attention to network wide issues and key processes that are used to manage how the network behaves and organizes itself. The network level functionalities are controlled by methods for network management, mutual trust management, network topology control, and clustering. In order to facilitate the optimization in all of these and many other functionalities over the whole networks, particular attention needs to be paid to the management issues.

Many of the relevant cognitive radios network issues have been discussed in [2], including traditional routing and data transport issues in the context of new challenges brought by cognitive features, mainly related to spectrum sensing, spectrum sharing, and mobility. In addition, network topology control, clustering, and QoS issues in CRNs were comprehensively addressed. In this article, we will concentrate on cognitive network management technologies and the related functionalities required. We limit the discussion to ad hoc type networks. Many aspects of infrastructure based cognitive networks have already been investigated in [2].

The rest of the paper is organized as follows: section II will take a look at the published variations of cognitive radio network architectures and proposed management solutions, and in section III, our approach is presented with short discussions of each of the key elements. In section IV a more thorough

[1]This research was carried on as part of NATO STO IST-140 "Cognitive Radio Networks"

analysis of cognitive network management issues is given. The conclusions are given in section V.

II. Related work

A cognitive resource manager (CRM) framework is proposed in [3] as a holistic approach to manage the CRNs as an entity with the main emphasis on global end-to-end performance optimization rather than link-level tuning. In their view, the CRNs could emerge as a result of communication between individual CRMs, which are managing the radio performance by set of reasoning methods and information. For a similar purpose, an implementation of cognitive networks is proposed to build on three layer framework. The "highest" layer sets the goals that are being implemented by the adaptive lowest layer based on the decision taking place at the cognitive middle layer. Another high level abstraction of a CRN architecture is given in [4]. Many of the key elements, such as end-to-end goals and cognition management are included, along with modular description of the other management entities in the system. Furthermore, policies are recognized as something that is partly used to drive the decision making processes.

An architecture for managing multi-parameter based cognition is proposed in [5]. The key idea is to structure the various parameters at different protocol layers in order to reduce the actual number of parameters that need to be tuned during and by the cognitive operation. By parameter structuring, it may become possible to apply critical learning methods and algorithms to larger number of parameters simultaneously, instead of the very limited single parameter applications so far reported. This will become increasingly important when parameters of all protocol layers are included in the cognitive algorithms.

In general, policies are sets of rules that allow, disallow, and prioritize parameter setting in network management. To that end, policy based management is discussed in [6], [7] and especially for cognitive networks in [8]. The terminology as well as exact roles and implementations of policy engine varies, but generally there is a need for "reasoning architecture" which sets the goals for the reasoning intelligence. The reasoning architecture proposed in [8] states that policies are set of rules that determine how the radio works. For the dynamic operating environment, changing of the policies or rules should be possible. In [8] policy architecture is separated to three components: Policy server (database), Policy engine, and Policy handling toolbox as well as defined interfaces between the components.

The Cognitive Network Management System (CNMS) for complex MANETs is introduced in [9]. Its aim is to provide automated, policy-based real time network management. Policy learning in CNMS is intrinsically distributed, and based on network performance observations for the refinement of contexts, and actions.

Also in [10], the policy-based management of radio resources is described. An overall management process is split into the autonomous components, i.e. the context acquisition, the profiles management and the policy-based management. These components constitute the inputs to the adaptation process of cognitive infrastructures. The output lies in the configuration of the behavior of the network elements. All components rely on the ongoing knowledge building.

To our understanding policies are essential elements in military context. Two examples of cognitive networking concepts in military framework are Tactical Information Technology for Assured Networks (TITAN) with its related Network Management System (NMS) that is presented in [11], and DirecNet network management, described in [12]. TITAN-NMS is an autonomous process by which the mission specific parameters are generated to policies according to which the network is maintained in the operation time. If adjustments are needed, the corrective actions are first attempted at the local level. If that is not enough, the cognitive management is performed at the higher hierarchical level of the network. The system includes also the mission-to-policy translation component as a separate element. Policies are therefore set of rules that specify which network properties are maintained in mission time and what methods are available in each mission. DirecNet is meant for Theater Area Networks (TAN) with high capacity, directional transmission and mesh/ad hoc structures with heterogeneous links. The management system of such (obviously highly complex system of systems) includes ways to manage and apply policies and how they are related to mission objectives. This particular management system is more towards providing information and interface to the system managers rather than a self-sustained autonomous management entity of the entire TAN.

A cognitive networking architecture with required functionalities and interfaces is presented in [13]. The main emphasis is still in radio resource management issues, such as spectrum sensing and adaptive access, but also other parameters and cooperation functionalities are included in the architecture. The interfaces introduced between the blocks make the architecture more generic and applicable to larger number of use cases and environments.

To allow for reusability of cognitive engines two essential interfaces are presented in [14]. The first is a Network Knowledge Representation Language (NKRL) to store and communicate information regarding network state to cognitive elements; the second a cognitive specification language (CSL) that describes the interface between policies and objectives and the cognitive engine.

In the OSI systems the network management functions are categorized to five different management areas: Fault, Configuration, Administration[2], Performance, and Security (FCAPS) [15]. Generally speaking, network management means 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. [16] provides a brief description of typical management solutions and also proposes a novel cognitive network management protocol (CNMP) especially suited for cognitive wireless ad

[2] Accounting is sometimes mentioned instead of Administration, especially for commercial networks. The latter is deemed more relevant in military context.

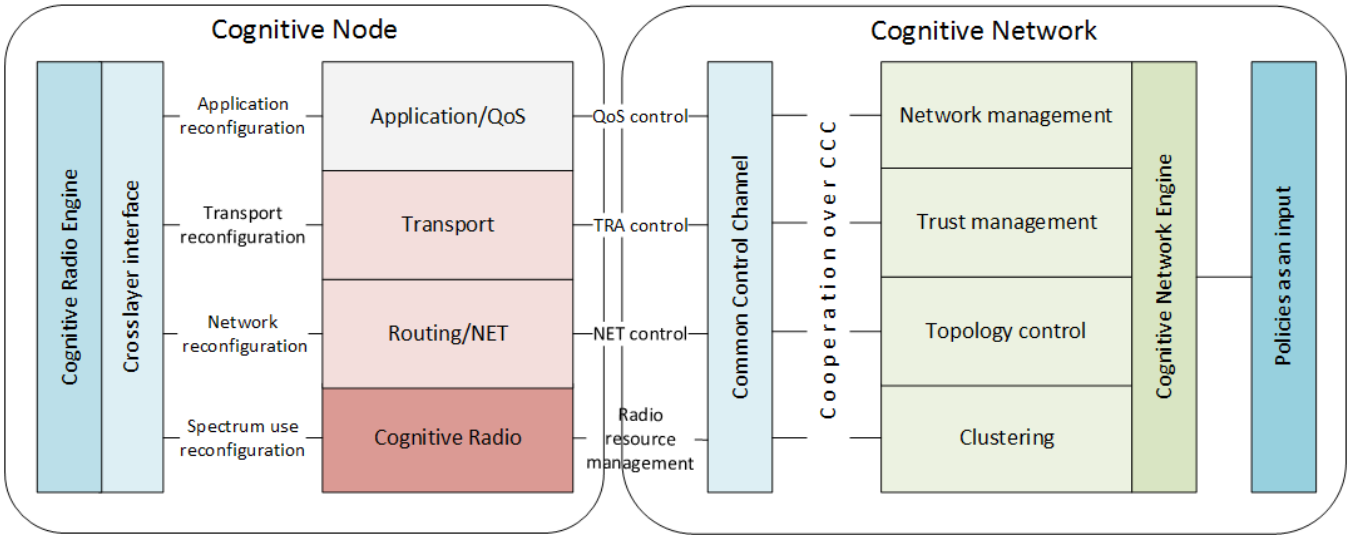

Figure 1. Essential cognitive radio networking functionalities and relations.

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.

III. ELEMENTS OF CRN ARCHITECTURE

Cognitive radio with the Cognitive Radio Engine (CRE) to handle the spectrum management capabilities is a necessary requirement in order to build cognitive radio networks. We note that in our opinion, the cognitive network is not the same as a network of cognitive radios. We introduce another abstract entity, a Cognitive Networks Engine (CNE), which manages the network wide end-to-end optimization. The cognition cycles of CRE and CNE are interlocked, and one could even say that CNE emerges as a result of *cooperating* CREs [3]. In this view, CNE is obviously distributed entity. In any case, the cognition 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 network wide phenomena.

An illustration of the cognitive network functionalities is given in Figure 1. The node centric functions and the network wide functions are separated. CRE is mentioned as an essential element in the node architecture, yet it or its algorithms are not described in this paper (see e.g. [17] for recent advancements in military context). Similarly, the application layer and related QoS issues are included in the figure but not addressed in the paper. Ultimately, the technical solution to be proposed must be applicable to any application and use case.

Based on the views reflected above as well as on our assessment, it is necessary to develop a synthesis of the roles of policies and goals and their relation to the operation of the CNE. First of all, note that from our viewpoint of military and tactical networks, we address the CRNs as ultimately temporary mission specific tools to reach the mission goals constrained by the policies in place. Each mission is managed in three phases: before, during, and after mission. Management functionalities required and utilized vary accordingly. This issue is addressed in more detail in section IV.

We place high emphasis on how policies ultimately define the limits of the network operation and management. In our view, the mission specific high level definitions as well as the overall environment characteristics are used to determine i) set of policies that specify the limits for the network operations (what is allowed, what is not allowed and priorities), ii) set of lower level operational goals for the network operation stating the desired functionality to be provided by the network and iii) set of metrics that can be used to monitor the network performance and assess possible needs for modifications. The CNE uses a specified set of algorithms to find a network parameter set that fulfills the network operational goals and stays within the limits given by policies. The CNE also uses the metrics to monitor the network operation, thus forming the familiar cognitive cycle. These relationships between policies, goals, metrics and CNE are illustrated in Figure 2.

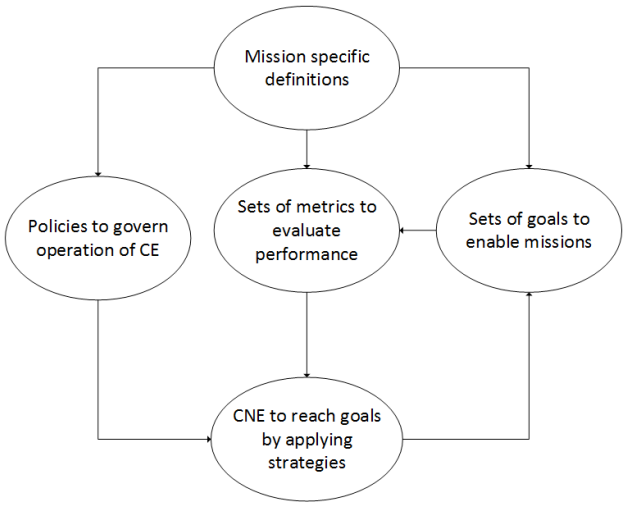

Figure 2. Relationships between policies, goals, metrics and CNE.

The key issue in the node centric view is the inclusion of a cross layer functionality to provide the cognitive engine with the required information. This makes it possible for the cognitive engine to constantly reconfigure all layers of the radio node functions. The cognitive network, on the other hand, requires the existence of a Common Control Channel (CCC) as a key element to allow cooperative control over the whole network. The radio node layers can also use the CCC to perform network wide reconfigurations of their operation parameters. This also includes that the CRE can manage, for example, the network wide frequency use. In this sense, the collection of interconnected CREs becomes a CNE.

We note that finding optimized solutions at the CNE/CRE might be computationally complex, and if most of the optimization solutions are identified as not possible by the policy reasoner (i.e. parameter values are outside the limits set by policies), lot of the computational power would be wasted – therefore a way how to include the policies in the decision making process needs to be found.

Cognitive networking is made possible by the cognitive node described above and a number of special technologies that also utilize the CCC for network wide cooperative configuration. The technologies that have been selected as most important are clustering, topology control, and trust management. Each of these technologies as well as their significance in cognitive networking is briefly discussed below.

A. Clustering

In [16] (cognitive) ad hoc network management is discussed from the perspective of hierarchical management based on clustering. The differences between centralized, infrastructure-based and distributed, ad hoc networks regarding their management are discussed in [18] and an approach for a completely distributed cognitive processing is discussed. Clustering is an important method to limit the management burden in large networks and therefore provides a tool for enhancing scalability of the network management.

B. 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. Especially in wireless ad hoc and sensor networks it is used to lay the foundations for message routing, which can save energy, and to reduce interference between nodes. With respect to CRNs, TC is important tool for network wide end-to-end optimization, besides routing and clustering.

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 neighbor discovery (ND). As in military operations the ability to communicate is essential, high QoS will be required for TC. Moreover, it must be analyzed whether centralized or distributed TC algorithms are advantageous.

C. Trust management

In our view, a trust management is an essential feature to be considered in a purely ad hoc based cognitive network architecture [19] [20]. This is due to the fact that nodes are expected to share their measured environment information and status parameters and, based on this shared information, make performance affecting decisions. Therefore, it is essential to manage the trust on node to node basis.

IV. CRN MANAGEMENT ISSUES

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 Cognitive Radio Ad Hoc Networks (CRAHNs) [18], as end user devices will become elementary active elements in the network 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 Self-Organizing Networks (SON) paradigm currently being brought into civilian cellular networks. It would even be possible that only part of the network devices are autonomously managed, while others, e.g. legacy devices, are manually managed.

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 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.
- Knowledge needs to be 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 make 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. If there is a need for a safe mode for those occasions must be investigated (e.g. tighter limits for autonomous adjustments would be effective if the network is not connected)?

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 the Table 1. Although e.g. [21] presents a range of military operations across a conflict continuum and similarly [22] depicts a more complex mosaic of military activities in a conflict, our focus in this paper is the lifecycle 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.

One should note that we have included the policy management in the table, although it is not part of FCAPS. To our understanding it is an essential managed element 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 analyzed 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. 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 1. Management functionalities with respect to mission phases.

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

V. Conclusions

We have presented an extensive view of cognitive radio network management issues in the context of military and tactical operation environments, where the key feature is the temporal nature of the network. This makes it possible to define the management functionalities with respect to different mission phases.

The traditional FCAPS functions and their required actions were therefore detailed to some level at each operational phase (before, during and after mission). Most importantly, it is necessary to raise the idea that as the cognitive and autonomous technologies are developed to operate communication networks, they become trustworthy enough to be applied in tactical context. They will most likely first be applied in the "during mission" phase, where their utilization is deemed most beneficial. Of course, that phase is also the most critical in the sense that it is there that lives are at stake.

The policy management must be seen as an equally critical functionality. It is necessary to develop the interconnection between mission goals and defined policies so that the CNE provides a reliable and failsafe communication solution to be utilized in all situations.

References

[1] R. W. Thomas, D. H. Friend, L. A. DaSilva, and A. B. MacKenzie, " Cognitive networks: Adaptation and learning to achieve end-to-end performance objectives", IEEE Communications Magazine, December 2006.

[2] S. Couturier, J. Krygier, O. I. Bentstuen, and V. Le Nir, "Challenges for network aspects of cognitive radio", 2015 International Conference on Military Communications and Information Systems (ICMCIS), 2015.

[3] P. Mähönen, M. Petrova, J. Riihijärvi, M. Wellens, "Cognitive wireless networks: Your network just became a teenager," *Proc. IEEE INFOCOM 2006*, 2006.

[4] D. Xu, Q. Zhang, Y. Liu, Y. Xu, and P. Zhang, "An architecture for cognitive radio networks with cognition, self-organization and reconfiguration capabilities," IEEE 2012.

[5] F. Gao and K. Zhang, "Enhanced multi-paramater cognitive architecture for future wireless communications", IEEE Communications Magazine, July 2015.

[6] M. Sherman, A. Comba, D. He, and HMcDonald, "A cognitive policy management framework for DoD", Proc. of IEEE MilCom, 2010.

[7] D. C. Verma, "Simplifying network administration using policy based management", IEEE Networks, Vol. 16, No. 2, pp. 20-26, Mar/Apr 2002.

[8] D. Denkovski, V. Pavlovska, V. Atanasovski, and L. Gavrilovska, "Novel policy reasoning architecture for cognitive radio environments", IEEE GlobeCom 2010.

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

[10] P. Demestichas, Ed., 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

[11] L. Kant, A. McAuley, K. Manousakis, R. Chadha, C.-J. Chiang, Y. Gottlieb, C. Graff, M. Patel, J. Bowcock, K. Moeltner, and D. Yee, "On the Application of Cognitive Network Design to MANET Network Management", IEEE MilCom 2011.

[12] J. Sonnenberg, S. A. Davidson, and M. Sherman, "The DirecNet Network Management Architecture", IEEE MilCom 2013.

[13] I. AlQerm, B. Shihada, and K. G. Shin, "CogWnet: A resource management architecture for cognitive wireless networks", Proc. of IEEE International Conference on Computer Communication and Networks (ICCCN) 2013.

[14] L. A. DaSilva, A. B. MacKenzie, C. R.da Silva Ryan, and R. W. Thomas, "Requirements of an Open Platform for Cognitive Networks Experiments", IEEE DySPAN 2008.

[15] L. Raman, "OS1 Systems and Network Management", IEEE Communications Magazine, March 1998.

[16] P. Potier and L. Qian, "Network management of cognitive radio ad hoc networks", ACM CogArt'11, October 2011.

[17] Cognitive Radio in NATO, STO Technical Report, TR-IST-077, January 2014

[18] A. Doyle, T. Forde, "The Wisdom of Crowds: Cognitive Ad Hoc Networks", in "Cognitive Networks: Towards Self-Aware Networks", 2007

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

[20] S. Parvin, S. Han, B. Tian, F. Hussain "Trust-based authentication for secure communication in cognitive radio networks". Proceedings of IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing : 589–596, 2010

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

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