

## Technical Evaluation Report

**Dr. Malcolm R. Vant**  
Ottawa, Ontario K2A2L7  
Canada

### ***ABSTRACT***

*The STO-IST-123/RSY-029 symposium on Cognitive Radios and Future Networks was held in The Hague, the Netherlands May 12-13, 2014. It addressed several key topics in the development and use of CRs (Cognitive Radios) and future military networks. CR and Future Networks in combination are envisaged as providing the underpinnings for the next generation radio communications networks of the NATO and Partner nations, and should enable them to share information efficiently and robustly over networks composed of heterogeneous devices, many with bandwidth-limited channels. CRs are built on Software Defined Radio technology, which enables them through clever internal programming to sense their environment and autonomously change their parameters to maximize various measures of Quality of Service, such as throughput and priority message handling. A key example of this behaviour is the automatic sensing of the current radio spectrum occupancy by the CR and its ability to select and change to unoccupied frequency bands. This behaviour shows great promise for making more efficient use of congested frequency bands through sharing of frequencies on a priority or non-interfering basis. During the Symposium, several key messages came through:*

- The military CR problem space is different that the civilian one. It deals with networks of networks having very different capabilities, from fibre optic to combat net radios. This is not the civil problem of handling non-interfering users in spectrum freed by UHF TV, although some work may be transferable.*
- Security has to be considered carefully. Cyber-attacks through internet entry points on the equipment and software, backdoor vulnerabilities, as well as intelligent jammer EW attacks on the physical layer, are big potential problems.*
- Need to look at CR network system solutions as a whole, not as individual parts, so as to properly assess feasibility and vulnerabilities. Solutions in one layer may open up vulnerabilities or problems in another.*
- Context of various types (mission, network, social, hierarchical) is important as an input to the CR radio and network management policy (in a technical sense) both for optimization of performance (routing, sensing) and effectiveness (delivery delay).*
- Need as many targeted field trials and as much realistic system level testing as feasible. Don't believe the simplified theoretical models.*

### **1.0 INTRODUCTION**

The STO-IST-123/RSY-029 symposium on Cognitive Radios and Future Networks was held in The Hague, the Netherlands May 12-13, 2014. It addressed several key topics in the development and use of CRs (Cognitive Radios) and future military networks. CR and Future Networks in combination are envisaged as providing the underpinnings for the next generation radio communications networks of the NATO and Partner nations, and should enable them to share information efficiently and robustly over networks composed of heterogeneous devices, many with bandwidth-limited channels. Cognitive Radios are built on SDR (Software Defined Radio technology), which enables them through clever internal programming to sense their environment and autonomously change their parameters to maximize various measures of QoS (Quality of Service), such as throughput and priority message handling. A key example of this behaviour is

the automatic sensing of the current radio spectrum occupancy by the CR and its ability to select and change to unoccupied frequency bands. This behaviour shows great promise for making more efficient use of congested frequency bands through sharing of frequencies on a priority or non-interfering basis. Given this background, the goal of the symposium was to discuss the particular problems, challenges and solutions involved in applying CRs and Future Networks to military networks. The expected audience for the symposium was broad: developers, users, operators, and decision makers.

With these issues in mind, the symposium technical program committee asked for papers on the following topics:

- CR strategies and related decision making processes for network coexistence
- Cross-layer strategies across the different functional layers up to the system management layer
- Dynamic Frequency Management
- Information sharing (policies, databases, ...)
- Security issues in implementing CR
- Implementation issues
- Coordination standards and protocols
- Cooperative and distributed spectrum sensing
- Waveform design and modulation for interference mitigation in CR
- Aggregate interference and coexistence issues
- Cognitive medium access control, interference management, handoff and routing protocols
- Cognitive intelligent techniques
- Distributed adaptation and optimization methods for cognitive radio networks
- Regulatory policies and their interactions with communications and networking
- Cognitive radio test-beds, simulation tools, and hardware prototypes
- Network aspects of cognitive radio
- Content-centric networking
- Software-defined networking
- Inter-domain Multicast and Unicast Routing in Tactical Networks
- QoS and Resource Management in Tactical Networks
- Mission Aware Networking
- Network aspects of IP security solutions
- Internet of Military Things
- SATCOM on the Move

From the abstracts received, 22 papers were selected for presentation at the meeting, plus an additional 7 poster presentations and demonstrations were chosen for viewing during an extended break. In addition, two keynote addresses and three invited papers were given. The papers were organized in the following sessions: Spectrum Sensing, Dynamic Spectrum Access, Posters and Demonstrations, Test and Evaluation, Development Environments, International Programs on Coalition Networks, When Cognitive Radio meets Future Networks, and Cross-Layer Aspects of Tactical Networks.

## **2.0 VIEWS AND OBSERVATIONS**

### **2.1 General**

The venue for the symposium was very good; no major issues were raised by the participants. Overall, the event was well organized and ran smoothly.

The event had 90 registrants, which is a bit higher than the past two IST events which had 75 and 78 registrants; the actual number that attended at some time during the symposium was 80. The uptick in registrations is encouraging given the current travel restrictions in most nations. Prior to the last few years, events had averaged over 100 registrants and some have been as high as 150. Papers were presented by participants from 13 nations and at least two NATO and multinational organizations, which represented a very good cross-section across the nations. Turnout from the U.S. was especially good - there were 11 speakers, which is a record for IST for an event not held in the U.S.

Unfortunately only 12 completed surveys were returned from the 80 attendees, which made it difficult to get reliable statistics on the audience's impression of the symposium. On the question of the "Overall Assessment of the Event", the average score in the surveys was between "excellent" and "very good" with 3 votes given to "excellent", 7 to "very good", and 2 to "good". For "Overall Value to My Organization" the score was again high with an average of 81-90.

Overall, the quality of the papers was very good. At least 80% of the papers presented substantial results. The surveys indicated the majority of the presentations were well organized and effective. The organizing committee is commended for the work they did in attracting very relevant and well-presented papers and a wide range of participants.

### **2.2 Grouping of Papers**

The symposium papers were organized as three main groups:

- Spectrum Sensing
- Dynamic Spectrum Access
- 
- Cognitive Radios meets Future Networks
- Cross-Layer Aspects of Tactical Networks
- International Programs on Coalition Networks
- 
- Test and Evaluation
- Development Environments
- Posters and Demonstrations

Two Keynotes and three Invited Presentations reinforced the exploration of the themes.

### **2.3 Keynotes**

The first keynote presentation was given by Dr. Richard Linderman from AFRL (Air Force Research Lab). He provided a thought provoking presentation covering four main topics: software-defined RF, software-defined networks, mission awareness, and realistic emulation and testing. He urged the group to not just think about SDR (Software Defined Radio), but about the further possibilities of software-defined RF where

communications, radar, ESM (Electronic Support Measures), and ECM (Electronic Control Measures) could be combined. CR networks already include some aspect of this in that they can sense their environment, which could provide a modest ESM capability. The group was encouraged to think about moving information, not data bits, on networks. Our sensors and associated communications easily have the capability of overwhelming the limited communications spectrum if we persist in moving data and not information. He emphasized the importance of mission awareness as context in network optimization, and finally he underlined that we need to be able to do large scale emulations and realistic field tests to understand the complex behaviour of systems. This keynote did a good job in encouraging attendees to think outside their specific box and look at some of these bigger trends. In particular, the messages on context and the need for realistic large scale testing were very appropriate for this symposium.

Mr. Michael Street from NCI Agency gave the second keynote in which he described where the NATO community has been in terms of operations, standards development and interoperability, and also how missions and their demands on the networks have evolved. He left us with the following points:

- Future Ops will rely strongly on information and mobility;
- Interoperability and effective spectrum exploitation are crucial;
- Waveform designs to address these challenges are being realised; but
- Implementation and deployment of these new developments remain as challenges.

## 2.4 Invited Speakers:

Mr. Holtzer from TNO, NLD gave the first Invited Paper entitled “Interoperability in Heterogeneous Environments”, which discussed current directions in Network Development and the role that CRs will play. He urged us to consider carefully how CRs are connected and embrace civilian technologies where they make sense, but do it wisely. Heterogeneous networks, composed of many types of radios, present a major challenge for interoperability.

For the second Invited Paper, Philippe Margot from the OCCAR (Organisation conjointe de cooperation en matière d'armement) EA (Executive Administration), and Christian Serra from A4EESOR (Alliance for ESSOR) provided an update on the ESSOR (European Secure Software Defined Radio) High Data Rate Waveform development.

Invited Paper 3, entitled “Advancing the State of the Art in Applying Network Science to C2”, was presented by Tim Grant who is associated with the Netherlands Defence Academy. His presentation discussed the field of Network Science in the broad sense of networks – not just the ones with electrons. His remarks provided food for thought when examining how context affects the optimization of RF networks.

## 2.5 Summary of Papers

### 2.5.1 Spectrum Sensing

The first grouping of sessions covered Sessions 1 and 2 and consisted of eight papers that dealt with various aspects of spectrum sensing such as: security, adaptation algorithms for optimizing the use of the spectrum and avoiding interference, optimization of routing choices, and laboratory experiments to test theory against practice. Several of the papers made use of various sorts of contextual information to aid their optimization tasks, such as the state of neighbouring links, or throughput measurements. This theme of context comes through in many of other sessions as well.

Paper 1 described a proposed method for enhancing security in CR MANETs (Mobile Ad-Hoc Networks) employing (DSS) distributed spectrum sensing. It was the only presented paper specifically addressing security issues, although another paper in the poster session also covered CR vulnerabilities extensively. The

paper described an approach, based on consensus weighting carried out at each node, for countering a SSDF (Spectral Sensing Data Falsification) attack, in which false spectral information is provided to the network. The weighting is done by using a trust measure for each node as a weighting factor on that node's contribution to the consensus calculation. The paper only presents the results for one scenario, so the method is a work in progress, however much discussion was provoked by it. Questions were asked about the performance with multiple malicious nodes, the use of trust versus authentication, and possible attack strategies to react to the consensus weighting. It was also questioned how the approach deals with a number of causes of variations, for example: propagation differences, fading, and the geolocation of nodes. With the exception of authentication, most of these issues are the subject of further work. It was clarified that trust would not replace authentication, but would be used in addition to it.

Paper 2 presented a thorough literature survey of the use of evolutionary game theory to improve cooperative spectrum sensing in CR networks. In using cooperative sensing to determine the available frequencies, users face a tradeoff between not contributing to the sensing and having more time for data transmission, or contributing to the common good, but having less time for their own transmission. EG (Evolutionary Game) Theory has been applied to this problem in the literature with some success. The authors point out that several challenges remain in the field. So far there is no consideration of the cooperation overhead, just the cooperation gain. Recovery strategies are required for when there is a deviation from the desired behaviour. Also, distributed learning algorithms are needed to aid convergence to a stable equilibrium. The paper was an interesting survey of the subject, but it did not specifically address the military issues of CR. Several of the questions posed by the audience probed the applicability to military environments, such as dealing with rapidly changing situations, or the case of some nodes being better placed geographically than others to contribute to the sensing problem. These issues were not yet addressed and would require further study by simulation and testing.

Paper 3 presented results of laboratory experiments in signal analysis for cooperative spectrum sensing. The laboratory setup consisted of USRP (Universal Software Radio Peripheral) platforms and a GNU software defined radio environment, with two wireless microphones used to simulate licensed users in the frequency band. The motivation was to explore the discrepancy between the theoretical and experimentally measured gains from cooperative sensing, and to attempt to find ways to improve the sensing performance. From the results presented, they appeared to be very early in their study and very little new analysis was actually demonstrated. Suggestions were made that several types of contextual information, such as knowledge of licensed users, and temporal and positional correlation could aid the sensing process, but this was not yet proven.

Paper 4 showed the results of a demonstration of a real-time cooperative spectrum sensing algorithm in a laboratory environment. The concept consisted of nodes that work cooperatively to sense the environment and then locally compute where interference is present. The idea is to avoid having to use a potentially vulnerable master coordinating channel. Each node senses a much wider spectral band than it uses, marks the margins of the largest free spectral zone it finds, and then collectively shares this information with the other nodes using bits in the data packet. A designated super node decides what channel to occupy next if the present channel becomes noisy. The process was demonstrated successfully in the laboratory for the simple case of two USRP nodes with one interfering signal injected directly into one USRP. There is a finite delay in making the switch, which can be an issue if the next chosen channel becomes occupied prior to, or during, a frequency switch. A question was posed as to what happens when the system encounters a fast frequency-hopper. At present, the design is only meant to address non-malicious interferers and therefore cannot handle such threats. The research has not yet fully made the transition to a military context, although it potentially solves the issue of avoiding a coordination channel.

Paper 5 from FFI, Norway received the best paper award. The paper described novel analytical work with the results backed up by simulation. The authors summarized their work in using P2P (Peer to Peer) protocols for discovery of nodes on mobile networks, reviewed the challenges of using this technique in a

military context, and discussed a new RA (Resource Allocation) algorithm for use in dynamic spectrum assignment. The combination of geo-location from P2P self-discovery and the RA algorithm is claimed to have several advantages: potentially better interference protection than sensing-based systems; it avoids the need to have dedicated infrastructure in the form of spectrum databases; and it avoids the need for dedicated spectrum coordination channels (although it runs on a backbone). It has good scalability, as shown by simulation, and should be robust in that failures are local, not global. However, it requires an internet-like backbone connection, and cannot be used with legacy radios. More importantly, it would require strong authentication and encryption for it to be trusted in a military context. If the issue with authentication can be solved, the technique could be promising for use with the next generation of military SDRs, provided that the necessary supporting standards can be agreed upon and adopted by manufacturers.

Paper 6 examined a tactical network consisting of a primary user and a group of secondary users, but where the primary user was not the owner of the network, only a priority user. In the network, data has to flow among the various users, primary and secondary, to reach its destination. Situations of non-cooperation and cognitive cooperation were analyzed, and it was shown for the cases considered that cooperation improved the stable throughput rate flow for all users. Channel state information was used by the cognitive algorithm in the user nodes to monitor and optimize data flow. Through the use of cognition the secondary users cooperate with the primary user by queuing traffic for the primary user when the channel is busy and then passing on the queued data when the channel becomes free. Although the analytical results look promising, the method still requires simulation and testing to validate it.

Paper 7 described a software defined radio test platform optimized for cross-layer co-operation, and which allowed easy implementation of routing and MAC (Media Access Controller) algorithms. Central to the concept is a centralized register plane that provides a mechanism for sharing cross-layer information. A technique called ROSA (Routing and Spectrum Allocation Algorithm), which senses the noise plus interference at each frequency sub-band at each node, was used to calculate a path of least resistance through the network physical and frequency space. The method looked promising, but it was very early in the assessment of the technique.

Paper 8 described a method for empowering HF radios with a degree of cognitive ability to improve channel allocation and throughput. The motivation of the work is to improve the speed at which links can be automatically established. Instead of using a single manually allocated frequency to do the ALE (Automatic Link Establishment) among the channels, a wideband technique is proposed in which the receivers can listen simultaneously over a broad HF band and make a rapid decision as to what frequencies to use. The method is claimed to provide several advantages over current techniques: better estimation of the ionosphere conditions, more rapid operation, an ability to anticipate the failure of a link before it actually fails, and better quality of service management. This work is still in its early stages and is still being tested in the laboratory.

### **2.5.2 CRs and Future Networks**

The next main grouping of sessions combined Sessions 6, 7 and 8, which included Papers 13 to 22. This grouping covered various future networking issues. Several of the papers (13, 14, 15) discussed the issues involved in introducing CRs into tactical networks, such as aiding the routing optimization using context information from various sources. In some respects, these papers are also closely related to Papers 5, 6, and 7 in Session 2. Another pair of papers in this grouping (18, 19) discussed the practical results of a major field trial involving interoperability of coalition networks, and the changes that needed to be made, both to protocols and software defined tactical radios, to overcome the difficulties encountered in the trial. Finally, the remaining papers (16, 17) discussed international standards and their evolution, both at the tactical and enterprise network level. The overlapping in content among the papers in the different sessions is an indication of how the problems encountered in military CR and Future Networks need to be addressed by a systems approach.

Paper 13 (no written paper available) described an analysis method, based on stochastic geometry, that was used to determine the potential interference experienced by a CR network operating near a network of PUs (Primary Users). The objective was to help establish the correct policy for the controller of the DSA (Dynamic Spectrum Access) process of the CR network to use to ensure the various radios can co-exist. It was shown by analysis that there can be sensing gain or loss for the CRs depending on the situation. For example, a DSA equipped CR network operating near a single PU benefits since it can use some of that PU's spectrum when it is vacant, whereas a single DSA node near a PU network loses, since it is overwhelmed by the demands on spectrum by the PUs. No experimental results were given, only a theoretical analysis, so this work has to be considered exploratory still.

Paper 14 considered self-optimization in future hybrid networks. The networks are hybrid in the sense that their elements have a wide range of transport capabilities, different policies, and different rates of mobility. At issue is how to use a potentially huge set of parameters to tune a complex time-varying network so as to achieve a performance objective, such as optimum routing. In dealing with such a large potential parameter set, there needs to be some consideration of the tradeoff between the overhead in obtaining and using the information in those parameters and the usefulness of the information to network performance optimization. The paper concentrated on the theoretical investigation of the value of partial information about the state of the network links to the routing optimization process. Despite the fact that much work remains to be done, and other parameters besides routing need to be considered, the approach outlined seems promising. There are some similarities to the conclusions in Paper 20, which also found depth-first sampling to be the best compromise in hybrid networks where some nodes were low bandwidth.

Paper 15 summarized the results of the 4th Joint Interactive Content Understanding Forum held on 25 March 2014 at the Naval Research Laboratory, Washington DC, USA. The main theme of this forum was the role of content understanding in cyber security. According to the authors, content understanding can provide two very important inputs to cyber security situation awareness and decision making: context and intent. Their contention was that there is a lot of work in both cyber security and content understanding, but very little on the convergence of the two. This presents an opportunity. Although the paper was not focused directly on the issue of the network layer of cognitive radios or future military networks, it provided relevant background for thinking about the role of context in decision making at the network level.

Paper 16 provided an update on the long-running series of TACOMS projects. The most recent of which were TACOMS Post-2000, and TACOMS Phases 1 and 2. The projects' objectives were to provide standards that would lead to interoperability of the modernized tactical radio networks of the NATO nations. TACOMS Post-2000, which was primarily industry driven, resulted in a new set of standards that proved to be rather cumbersome to use. TACOMS Ph1 produced a STANAG (NATO Standard) suite for Integrated Data & Voice for tactical networks, however it did not clearly separate the information and network layers, so that services ended up interacting between layers in a tangled fashion. The objective in TACOMS Ph2 is to move to a true service-oriented architecture with clear separation of the two layers. This presentation gave a useful benchmark as to the status of the evolving Tactical Radio Network standards - not yet at CR stage but clearly preparing for SDR.

Paper 17 describes how the cost-effective, inter-carrier ETNA (Ethernet Transport Network Architecture) approach to SDNs (Software Defined Networks) might be combined with the security features of PCN (Protected Core Networking). The combination could be attractive to NATO for use in the FMN (Federated Mission Network). The ETNA study, which was commissioned by European telecommunications companies, focused on manageability and integrity of SDNs. ETNA describes how to provide SDN-based Intra-Domain services and an inter-carrier interface for Carrier Ethernet platforms. In addition, and perhaps more importantly, it provides a streamlined method to rapidly roll out QoS oriented communications services on a very large scale, which should be of interest to NATO for the FMN. In the paper, the principles elucidated by the IST activities on PCN (IST-069, -103) are shown to have had direct impact on the thinking in the SDN field. ETNA incorporates many of the principles outlined in the PCN work, but uses a different

management structure than envisioned by PCN. As indicated in the paper, PCN clearly separates user and network domains and views the network solely as a means to deliver a service with a given QoS; whereas ETNA-based SDN assigns network activities to the right execution platforms and locations. The authors believe that it should be possible to add PCN as a layer on top of the ETNA infrastructure, and in doing so provide PCN specific functions. The paper provided food for thought and possible new directions for IST work.

Paper 18 related lessons learned from the CoNSIS (Coalition Networks for Secure Information Sharing) field trial. CoNSIS is a multinational project aimed at improving the secure sharing among nations of information and services in tactical networks, while using, to the largest extent possible, commercial standards and technologies, and incorporating the PCN principles. At the end of Ph 1 a major field trial took place with a coalition peace-making operation as its theme. Many lessons learned and recommendations, important to the eventual success of CoNSIS, were drawn from this trial. For example, multicast, which is important for interoperability, is not easy to implement since there are no common multicast protocols for communication between commercial routers and military radios. It did appear that commercial web services standards could be leveraged for use in this coalition network, but work needs to be done to develop multinational standards. Considerably more work, both theoretical and experimental, needs to be done on the issues of interoperable common security approaches. The paper provides many more detailed recommendations at the link and radio level that are useful for the further development of SDR and CR tactical radios.

Similarly to Paper 18, Paper 19 also discussed results from the CoNSIS project, but looked specifically at how to apply civil standards to solve the problem of router to radio interaction raised during the trials. In particular, the OLSR (Optimized link State Routing) v2 and DLEP (Dynamic Link Exchange Protocol) protocols both of which have been specifically designed for MANETs and include extensibility as one of the major design goals, are considered in detail. Their extensibility allows them to be modified to handle the coalition network interoperability challenge. Since there is already a draft modification to handle multi-topology routing and heterogeneous link characteristics for OLSR v2, the authors suggest building on this and adding their own extensions to solve some of the other problems with the routing at the radio level, noted in Paper 18. They believe that these modifications will not affect backward compatibility in OLSR v2, which is important if proprietary solutions are to be avoided. In the question period, there was a concern expressed about the overhead involved in using OLSR, but the authors contended that it is not a burden given the way they are using it. Both Papers 18 and 19 illustrate the value of incorporating realistic field trials in the development of SDR and CR. Many insights were gained through the trials that would not have been obvious in a lab environment.

Paper 20 deals with the problem of providing resilient routing with a good QoS over heterogeneous coalition networks. In particular, they are concerned with the overhead burden that some radio networks, built with civilian protocols and routing concepts, can place on narrow-band tactical radios. They propose a new protocol able to provide efficient inter-domain connectivity in a radio environment, as well as support for differentiated QoS and local network policy enforcement. As an example of the problem faced, a low-bandwidth radio network of one nation might be sandwiched between two higher capacity networks of other nations and be expected to pass a lot of data or signaling information associated with routing and network management. The authors propose a reactive, depth-first search MANET routing protocol, where the search can be steered based on network policy, and required QoS. In this way, policy can prevent signaling over low capacity links where possible. Hints to guide the search for the optimum route can be provided from various sources such as a database of the cross-layer topology, local traffic history and previous searches. Using simulation, the protocol has been tested for acceptable delays and overheads, but without any QoS routing or policy enforcement restrictions. More work remains to be done, but the approach of using various types of context to guide routing in heterogeneous networks is an intriguing one.

Paper 21 continues the theme of using context to aid routing, but takes it a step further and proposes using information from application layers to aid the routing process in mobile tactical networks. Starting with the



observation that most MANET routing protocols don't deal well with rapid changes in topology, they propose routing protocols that do not make use of a global knowledge of the topology. Instead, the protocols use locally derived local social metrics for the network that provide information on the centrality of the nodes (e.g. a squad leader's radio), and how they are organized in the local community (e.g. all members of the same squad). These metrics could be based on a prior knowledge about the network or be derived locally by analysis of the neighbourhood radio contacts and traffic metadata analysis. The authors go further and propose using socio-cognitive information derived from other layers, such as indicators of the local social hierarchy of the users of the nodes. In a simulation, three social metric protocols outperformed the OSPF (Open Shortest Path First) protocol in reducing data delay and increasing data delivery ratio. The paper generated a fair amount of discussion as to how easy it would be to implement and possible pitfalls that might occur when using it, such as: everyone thinking they are the same priority; the neighbourhood being homogeneous; or routing loops being created. These are all issues to be investigated in further work.

Paper 22 (not presented) dealt with the problem of efficient routing for flexible airborne networks. The authors propose the use of OLSR v2 (Optimized Link State Routing) protocol as a possible solution for routing among airborne nodes. Three cases were considered: a temporary break in a part of the network from the rest of it; dealing with EMCON (Emissions Control) mandated radio silence in a particular direction; and choosing the best route in the face of interference or jamming. The suggested solutions were tested in an OpNet modeling environment, but have not been subject to testing with real equipment.

### **2.5.3 Development Environments and Test and Evaluation**

The remaining four papers were grouped under Development Environments and Test and Evaluation, although Papers 9 and 12 could easily have fit in the second grouping under 2.4.2 above.

Paper 9 described work whose objective was to improve the performance of the link adaptation or creation in CRs dealing with multipath. A cognitive engine consisting of a genetic algorithm was fed "chromosomes" consisting of measurements of link parameters of a SDR. Through the evolution process in the algorithm, the best possible links were found. A simple demonstration was done using multipath created when SDR signals were transmitted among railway vehicles in a train yard. The method requires tweaking of the algorithm (heuristics) to work in a given situation and appears to still be at the proof of concept stage.

Paper 10 described ongoing work to set up a test facility for evaluation of SDRs for the Italian Navy. Descriptions of the equipment purchased and plans for the facility were presented.

Paper 11 presented an open-sourced software framework called CogWave for use in CR waveform design. The framework was demonstrated with two waveforms: DADS (Delay and Add Direct Sequence) and DAA-OFDM (Detection And Avoid - Orthogonal Frequency Division Multiplex). DADS is a low complexity waveform that allows high throughput on the SDRs when there is no interference on the channel. The system senses the throughput and switches to the more complex, multi-channel DAA waveform when the throughput drops due to interference, such as jamming or channel congestion. Frequency-hopping is possible over a wide frequency range for both waveform types. The results of a simple lab experiment using the two waveforms and a simple CW jammer were shown. The implication was that there is a plan to use the framework to develop and test further candidate waveforms for CRs.

Paper 12 summarized work performed under the CELTIC SPECTRA project on developing more robust military communication networks using CRs and commercial standards. The objective of their work was to validate the suitability of SPECTRA in a military context through demonstrations in military scenarios. The system consists of a CRRM (Cognitive Radio Resource Manager) connected over a backbone to Base Stations, which in turn are connected to mobile UEs (User Elements). The paper was thin on detail on how the system performed. During the question period, the issue of the vulnerability of the centralized CRRM was raised. It would be an attractive single-point-of-failure for a foe to exploit. It was recognized by the

presenters that the CRRM needed protecting, but few details were given as to how this would be done. Suggestions were made that redundancy of key components would help, as well as the use of strong authentication of UEs to the Base Stations. It would be interesting to see an actual vulnerability assessment of the system, as well as performance results under stressed conditions.

#### **2.5.4 Posters and Demonstrations**

The poster session consisted of three demonstrations and four posters. Providing an opportunity for demonstrations was a welcome addition to the symposium, in that the demonstrations helped ground the discussions in reality.

The first demonstration (P1) was of a large software package called CORASMA from Thales France. The motivation was to be able to model CR networks in enough detail to bring their TRL (Technology Readiness Level) from 2-3 (feasibility) to 5 (technology demonstration). The model was very detailed and included a physical model. Data are sampled as I,Q samples and then processed using the algorithms to be tested.

The second demonstration (P2) described a software toolkit called CNEDAT (Cognitive Network Engineering Design Analytic Toolkit) for the design of heterogeneous tactical CR MANETs. The demonstration focused on dynamic frequency assignment using SDRs, and the cognitive radio protocols that are used to adapt the CR performance. In particular, the spectrum assignment, routing and topology control modules were demonstrated.

The third demonstration (P3) was of a more modest laboratory system consisting of two USRP platforms and a GNU software radio running on a PC. The motivation was to be able to develop and test various waveforms that would reduce interference.

Poster P4 outlined work being done on developing DMR (Digital Mobile Radio) technology on a SDR platform. The idea was to be able to control unmanned devices over WiFi in Search and Rescue operations and to control the WiFi parameters using cognitive methods. The experimentation was done on USRP platforms. So far they have demonstrated the concept and passed messages over the DMR link. They are also currently developing a miniaturized DMR link that can be used in smaller unmanned devices.

The Polish Roadmap to the adoption of Tactical Level CR was described in P5. A detailed description was given of the policy framework and project structure that has as its goal the eventual introduction of CRs into the Polish military. Some experimental results on dynamic spectrum access techniques and general findings from the CORASMA software were also described.

Poster P6 described work on a black box model incorporating a GA (Genetic Algorithm) that is meant to be able to adapt wireless link performance to a given situation. To start the process rolling, some understanding of the context of the problem is required and a tweaking of initial conditions. The GA essentially uses a selected set of parameters (genes on a chromosome), which in this case describe the channel, and adapts them using "evolution" to provide an optimum solution for a given criteria being examined, e.g. throughput. The work appeared to be in its early stages.

Poster P7, which provided a survey on the vulnerabilities of centralized CR infrastructures, was very interesting. The material was also available as a PowerPoint handout. The CR infrastructure was shown to be vulnerable on multiple levels, from wireless intruders (packet in packet, man in the middle, remote management), to network exploitation of servers, to backdoors left in equipment by vendors. It is unfortunate that the security aspects of CR networks did not get more attention at the symposium, given that developers need to be aware of how their solutions to one problem may open the door to another.

## 2.6 Positive Examples of Outreach in Symposium

A good example of outreach by the symposium organizers to the broad CR stakeholder community was shown by the attendance at the meeting of researchers from the following groups:

- Industry attended in significant numbers and presented updates on ongoing standards development, as well as demos
- NCI Agency – acted as host
- Paper from ESSOR team in OCCAR
- Community of NATO R&D researchers
- Some academia working on defence problems

In addition, the organizers of the symposium arranged for demonstrations of simulation software for designing CRs to be provided during the poster session break.

A further positive observation on the symposium is that it could have been co-opted by the civil community and academia working on civil CR issues, chiefly focused on sharing unassigned newly freed-up spectrum. It was not and the topics and papers concentrated by and large on the military problem.

## 2.7 Some Further Observations on Outreach

One shortcoming in the outreach of the symposium was the lack of users from the CNAD (Committee of National Armaments Directors) and NATO C3 (Command, Control and Coordination) communities. These are the engineers who design and operate the networks. They could have provided more insight into the requirements from their point of view and also commented on what they think would help, and what would hinder their efforts. It would also be informative for them to see what is envisaged for the future networks.

## 2.8 One Further Observation

Work on PCN (Protected Core Networking), based on an idea from the NCI Agency, but developed by IST Panel Task Groups under activities IST-069 and -103, has been highly successful as noted in this symposium. During his keynote address, Dr. Street noted verbally that NCI Agency estimated that participation in these task groups saved them \$200k directly, and he estimated that there has been influence on not only the Afghan Mission Network, but also on the \$50M Federated Mission Network procurement. Paper 18 noted the use of PCN concepts, and Paper 19 provided further detail on how the PCN concept can be leveraged further. If it is not already too late to do so, the work on Protected Core Networking work should be considered for an achievement award. It has clearly had a significant military impact.

## 3.0 KEY MESSAGES

In analyzing the content of the papers, as outlined above, and taking into account the discussions at the event, several key messages emerged from the symposium. The following list provides a quick summary for the reader:

- The military CR problem space is different that the civilian one. It deals with networks of networks having very different capabilities, from fibre optic to combat net radios. This is not the civil problem of handling non-interfering users in spectrum freed by UHF TV, although some work may be transferable.
- Security has to be considered carefully. Cyber-attacks through internet entry points on the equipment and software, backdoor vulnerabilities, as well as intelligent jammer EW attacks on the physical layer, are big potential problems.

- Need to look at CR network system solutions as a whole, not as individual parts, so as to properly assess feasibility and vulnerabilities. Solutions in one layer may open up vulnerabilities or problems in another.
- Context of various types (mission, network, social, hierarchical) is important as an input to the CR radio and network management policy (in technical sense) both for optimization of performance (routing, sensing) and effectiveness (delivery delay).
- Need as many targeted field trials and as much realistic system level testing as feasible. Don't believe the simplified theoretical models.

#### **4.0 CONCLUSIONS AND RECOMMENDATIONS**

The symposium succeeded very well in focusing on the military issues of CRs and Future Networks, although the use of commercial technologies and protocols was embraced where possible to leverage work that has been done and to save costs. It became clear from the discussion that the introduction of CRs into military use is still many years away and many problems remain to be solved, such as: the development of robust and viable optimization strategies, consideration of vulnerabilities, a demonstrated ability to operate in stressed environments, and agreement on standards for the various aspects of the system.

It was clear from the symposium that more work is required to consider vulnerabilities in various approaches to implementation of CRs in a military tactical environment. Several times during presentations questions relating to unresolved vulnerabilities arose. It will be important, for the issue of security, as well as because of the sheer complexity of the systems and their interaction with their surroundings, that careful evaluations of systems be done under realistic stressing conditions.

As noted in the key messages above, the use of context of various sorts to optimize performance was very much a theme in the symposium and will be important in searching for adaptation strategies for sensing and routing that are robust and implementable.

If it is not already too late to do so, the work on Protected Core Networking, which was the subject of two IST Panel Task Groups, IST-069 and 103, should be considered for an achievement award. It has clearly had a significant military impact as mentioned in the symposium.

The symposium accomplished its objectives of exposing the military-specific challenges involved in using cognitive radios, and the problems that have to be considered and solved prior to adopting this technology. The event also successfully engaged a cross-section of the academic, industrial and defence community. Overall, the level of discussion was high, probed the issues well, and avoided repeating work applicable to CRs that could be found in other non-military, professional conferences. In terms of new activities, the Research Study Group IST-104/RTG-50 Cognitive Radio in NATO II, which met immediately after this symposium, is well placed to consider them in their research program.