End-to-End Optimization for Tactical Cognitive Radio Networks

Stefan Couturier
Fraunhofer FKIE
Wachtberg, Germany
stefan.couturier@fkie.fraunhofer.de

Timo Bräysy
University of Oulu
Oulu, Finland
timo.braysy@oulu.fi

Boyd Buchin
Rohde & Schwarz
Munich, Germany
boyd.buchin@rohde-schwarz.com

Jaroslaw Krygier
Military University of Technology
Warsaw, Poland
jaroslaw.krygier@wat.edu.pl

Vincent Le Nir
Royal Military Academy
Brussels, Belgium
vincent.lenir@rma.ac.be

Niels Smit
Ministry of Defence
Utrecht, Netherlands
ns.smit@mindef.nl

Topi Tuukkanen
Information Technology Division
Finnish Defence Research Agency
Riihimäki, Finland
topi.tuukkanen@mil.fi

Erik Verheul
Royal Netherlands Navy
Ministry of Defence
Den Helder, Netherlands
e.verheul@mindef.nl

***Abstract*—Cognitive Radios are able to dynamically use free spectrum in their vicinity, avoiding interference and congestion and thus providing robust communication links. Cognitive Radio Networks go one step further, as they do not only consider the link to the next node but focus on end-to-end optimization. Dynamic adaptations of the whole protocol stack are required, especially on the network layer. This paper analyzes networking technologies regarding their support for end-to-end optimization in tactical environments and proposes enhancements. Based on the findings, an architecture framework for Cognitive Radio Networks is proposed.**

Keywords—Cognitive Radio Networks; routing; Topology Control; data transport; clustering; network management; trust management; control channel

I. INTRODUCTION

Communication is one of the most important capabilities in military operations. Information must be available at the right place at the right time, and this is strived for by using reliable communication networks. However, in mobile radio networks – especially military ones – there are many causes for disturbances that lead to the delay or even loss of messages. Such disturbances occur due to external influences, like interference or shadowing, but also due to internal problems, like congestion or malicious nodes.

Cognitive Radio Network (CRN) technology [1] is a promising approach to mitigate the detrimental effects of these disturbances, as it has the capability to sense both the environment of a node and its inner states. Based on this it can adapt the protocols used to attain optimal end-to-end performance. It differs from Cognitive Radio (CR) technology in the sense that cognition in a CR is mainly focused on the lower layers of the protocol stack, while in a CRN cognition is also applied to the higher layers. This requires for CRN that the status – or the metrics – of the elements of each layer can be read and that their configuration parameters can be set dynamically.

In order to support end-to-end optimization, CRN technology allows the metrics of an element on one layer to influence the configuration parameters of elements in another layer. E.g. a broken link detected on the medium access layer may lead to changes in the routing on the network layer. Thus, the architecture has to allow for cross-layer optimization. In addition, an organizing entity is required to take the decisions based on the metrics of all elements and to set the configuration parameters according to the decisions. This entity is usually referred to as the cognitive engine [1].

The number and types of metrics and configuration parameters are dependent on the protocols used in the elements. Unfortunately, many of the existing protocols were not designed for tactical CRN and therefore restrict the end-to-end optimization. E.g. the well-known data transport protocols Transport Control Protocol (TCP) and User Datagram Protocol (UDP) were originally designed for wired networks [2], and the well-known routing protocol Optimized Link State Routing (OLSR) does not specifically support radio silence [3].

This paper looks at several elements and protocols related to networking. The state of the art is analyzed as well as possible enhancements for a better support of end-to-end optimization in CRN. Another focus is on the usability for tactical operations. Communications in tactical operations do not only suffer from spectrum scarcity and hostile attacks; also the heterogeneity of networks (fixed, deployable, mobile and

This paper is based on NATO IST Panel activity IST-140 "Cognitive Radio Networks – Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management".

dismounted elements), multinational interoperability and coexistence with friendly and neutral networks is a challenge. The outcomes of the investigations described in this paper are therefore proposals for technology enhancements in tactical CRN, which should advance the autonomous adaptation capability of networks as a next step to cope with these challenges.

In section II the selected technologies are introduced. Section III analyzes them and proposes enhancements. The resulting architecture framework is presented in section IV. Section V concludes our findings.

II. SELECTED TECHNOLOGIES

In [4] we present essential CRN functionalities and their relations. While [4] focuses on the management of these functionalities, in this paper we analyze the related technologies and propose technical enhancements for them in support of end-to-end optimization.

One of the most important technologies concerning end-to-end optimization is *routing*, as the route of a message may have significant influence on the latencies introduced due to hop count, congestion, or link quality. Routing is closely related to *Topology Control* (TC), as the routes are determined based on information gathered by this technology; consequently, also TC needs to be analyzed regarding enhancement for tactical CRNs.

A current approach of organizing larger number of network nodes into subgroups is *clustering*. The network is divided into smaller subnetworks (so-called clusters), each using another transmission channel than its neighbors in order to avoid interference. A message passing through several clusters may suffer from latency introduced at the cluster borders. Therefore, clustering must be taken into account when conducting end-to-end optimization.

On link level, messages are controlled via specific transport layer protocols. These *data transport* protocols handle features like delivery order, flow control, or data checksum. Also their influence on end-to-end optimization is analyzed in section III.

A further important feature of CRNs compared to legacy networks is the automatization of the management. As mentioned above, *network management* has already been handled in [4], but here we want to look at the influence of Software Defined Networking (SDN) technology on CRN management and to present an enhanced view on *trust management*.

All those technologies have in common that they need to exchange control information. In order to separate control information from user data, it is transmitted in a so-called *control channel* (also called *common control channel*, CCC). If the transmitted control information is delayed, also user data will suffer from latency. Therefore, also this topic is handled in the next section.

III. ANALYSIS AND PROPOSITION

End-to-end optimization implies a holistic CRN approach that requires re-thinking the targets of existing protocols. In the following subsections, challenges for military CRN are identified, and solutions or recommendations are proposed.

A. Routing

Classical 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 either based on proactive protocols like OLSR or reactive protocols like Ad hoc On-demand Distance Vector (AODV) with some modifications to adjust them to a specific wireless environment. Some proposals exist that are tailored to specific types of CRNs (for example [14][15][16]). They often do not meet the military requirements for reliable path (or multiple paths) selection and effective reaction on information from cognitive entities (route reconfiguration due to dynamically changed spectrum access or spectrum assignment policies). Many Mobile Ad Hoc Network (MANET) routing protocols are based on shortest path metric calculation, but that approach is not always sufficient for Cognitive Radio Ad Hoc Networks (CRAHNs), which are CRN specifically designed for ad hoc purposes. The very popular Expected Transmission Count (ETX) metric can react on link quality, but its accuracy is dependent on the current traffic exchanged over a particular link. Thus, some other metrics are proposed for non-military CRAHNs, i.e. Directional Airtime (DAT, as specified in [17]), hop count, end-to-end delay, energy, bandwidth, route stability, link and path quality, and cumulative metrics (as described in [18]). In addition, the CRAHN routing protocols should consider incumbent spectrum user activity and identified multichannel communication [19].

Following [18], we compare a set of representative protocols proposed for CRAHNs in Table 1.

TABLE I. CRAHN ROUTING PROTOCOL COMPARISON

Protocol	Metric	Type	CCC	Pros	Cons
Energy-aware routing protocol [20]	Energy weight of the link	Reactive or proac-tive	Yes	Avoids network partition	Not good for large network
Low latency and energy based routing protocol [21]	End-to-end re-sidual energy and delay	Reactive	No	Low latency	Does not take incumbent activity into account
Energy-efficient routing protocol [22]	Sleep and wake-up time	Reactive	No	Data flow coordina-tion	Multipath scheme not considered
Delay and energy-based spectrum aware reactive routing [23]	Delay and path energy	Reactive	No	Minimizes signaling overhead. Multipath transmis-sion	No efficient route maintenance mechanism
Enhanced dual diversity cognitive ad hoc routing protocol [24]	Path delay	Reactive	No	Fast route recovery. Reduces interference from incumbents	High number of control messages
Anypath routing	Link availa-	Reactive	No	Reacts on incumbent	Higher transmission

protocol for multihop [25]	bility			activity without spectrum sensing. Reduces interference to incumbents	delay

All of the above-listed routing protocols are standard MANET protocols (mostly reactive) with extended metric calculation that consider specific CRN behavior. Of course, they can support tactical CRAHNs, but with a small efficiency.

One of the most interesting solutions regarding routing mechanisms for CRAHNs (and particularly for tactical CRAHNs) is based on the artificial intelligence learning method known as reinforcement learning, presented in [26] and [27]. Authors of [26] introduced Cognitive Radio Q-routing (CRQ routing), based on the Q-learning method as described in [28]. CRQ-routing is a spectrum-aware scheme that finds least-cost routes in CRAHNs considering the dynamicity and unpredictability of the channel availability and channel quality. The CRQ-routing considers both the incumbent's and the CRAHN's network performance by minimizing CRAHN's interference to incumbents along a route without significantly jeopardizing CRAHN's network-wide performance. The CRQ-routing enables a CRAHN to observe its local operating environment regularly and subsequently to learn an action selection policy through exploring various routes, and finally to choose routes with enhanced network performance (depending on definition: lower CRAHN's interference to incumbents, lower CRAHN's end-to-end delay, lower CRAHNs packet loss rate, and higher CRAHNS throughput). The solution can be named cognitive, since it relies on the cognitive cycle.

The Q-learning method allows for constant learning based on observing the environment (i.e. incumbent activity, interference …), updating the so-called Q-function, changing the system state (i.e. change channel, route …) to maximize the Q-function, and then reiterating the cognitive cycle by observing the environment again. If the indicated changes decrease the Q-function value, another strategy will be tried (i.e. another channel or route is selected …). Continuous observation of the CRAHN's reactions on the changes leads to a system state that maximizes the Q-function and thus also the network performance. The Q-learning-based routing mechanisms require cross-layer interactions to observe the network status and to enforce a change of the system (network) state (traffic routes). The Q-learning modules are reinforced by the information coming both from the applications and the bottom layers. Assuming the clustering network architecture, the cluster-heads play an important role to collect a network wide knowledge that supports so-called Q-Learning Self-Organizing (QLS) mechanisms.

Application of the artificial intelligence techniques in the CRAHNs produces interesting 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. Nevertheless, the military CRAHNs should consider similar techniques in the tactical domain. An additional effort is still needed to propose solutions and to perform the required research on the application of artificial intelligence to military CRAHNs.

B. Topology Control

TC is a technique that is used to model the network as a graph in order to reduce the cost of distributed algorithms. The edges of the graph represent the connectivity. These graphs lay the foundation for routing. Therefore, TC directly influences end-to-end optimization.

Especially in wireless ad hoc and sensor networks TC is furthermore used to determine the required transmitting power and to reduce interference between nodes. In homogeneous TC approaches all nodes use the same transmit power, while in the non-homogeneous case they may have different transmitting ranges.

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).

For both topology construction and topology maintenance, information must be exchanged in order to create and update the topology graph. This information may include the identification of a network node or its position. Especially in military networks, such information may be classified. Therefore, TC must be adequately protected or be able to apply security measures for handling this information.

Exchange of updated information is required when there are significant changes in the topology, e.g. due to node movement. In addition to that, communication failures may be an indicator for the need to update topology information. Therefore, it is recommended to not only regularly transmit updates but to also observe the status of the network for changes, which may indicate the need for immediate updates.

Regular updates, which imply the frequent transmission of control messages, may furthermore be undesirable in military operations, as any emission can be detected and located by hostile forces. But the lack of updates, either due to radio silence or due to resource unavailability (e.g. caused by jamming) may lead to outdated or wrong topology information and thus to a degradation of user traffic performance. When resources are available again, there is a high need to communicate. It must be made sure that the network is not flooded with TC updates at this moment unless necessary.

While TC usually checks the availability of a link based on a fixed given frequency, TC for CRN must regard all available frequencies on that link. The selection of one of these frequencies for transmission must be in line with the given restrictions, like policies and clustering. Nevertheless, for ND frequencies cannot be negotiated. Either there is a fixed frequency, which in case of interference will impede discovery, or the frequency may change, which in average will delay discovery, as several frequency changes may be necessary until a node is discovered. Consequently, the more frequencies are possible for ND, the longer the ND process will take at an

average. Therefore, there must be a trade-off between agility and discovery time.

C. Clustering

Clustering is closely related to the more general TC. By clustering a large distributed network (such as tactical MANET), many essential networking functions, including routing and control signaling, are affected crucially. Clustering can reduce the amount of control traffic in the network, e.g. by limiting the number of nodes that participate in flooding messages on the topology. By selecting appropriate clustering objectives for the military CRAHNs, the networks can also be optimized with respect to energy use, load balancing, stability, and many other parameters.

The clustering process consists of cluster formation and cluster maintenance. Part of the cluster formation process is the selection of a cluster head (CH) for each cluster. This obviously has crucial implications on the topology. The optimization objective set for cluster formation and maintenance affects how and by which principle the CH's are selected. One optimization objective is to support the typical military traffic patterns, e.g. group communication [29].

D. Data transport

CRNs require efficient end-to-end data transport control algorithms. Standard TCP or UDP are not designed for wireless networks. Some modifications proposed in literature can be used in typical ad hoc networks [30], 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 in order to match the capabilities of the channel and of the destination nodes. It was designed for typical wide area fixed networks, where congestion mainly results from intermediate node overloading.

Furthermore, CRNs provide new challenges in data transmission control. Data segments can be lost or delayed due to spectrum mobility (handoff) and ongoing spectrum sensing. TCP will react on such situations by decreasing the transmission window. Nodes could inform the source that this is a transitory state caused by the cognitive entities. Moreover, intermediate nodes that are particularly engaged in the cognitive procedures should buffer the traffic. In CRNs large bandwidth variations can occur in some segments of the network due to volatile activity of licensed users in these segments. Thus, these network segments can radically increase or decrease their throughput. TCP cannot adapt its transmission rate to such rapid changes in an efficient way, especially in the case of high Round Trip Times (RTT).

Considering the specific requirements of tactical CRAHNs, cognitive transport protocols have to be equipped with mechanisms that allow the identification of intentional interruptions of data transmission in intermediate nodes. The interruptions can be caused by an ongoing sensing procedure, channel handoff, an ongoing link quality measurement, intermediate node mobility prediction, congestion, buffer overflow, and route failure notification.

Fig. 1 presents a sample multi-hop CRAHN, where it would be beneficial for the packet transmission between a source (CR1-S) and a destination (CR6-D) node to be controlled by a cognitive process that uses information provided by the other nodes. Unfortunately, most of the sources of the information are in the path between the CR1-S and CR6-D. The links between the node pairs can use different channels (c1, c2 ...), which can be switched by at least one node in the path. Switching the channels can lead to a route change between CR1-S and CR6-D. The source and the destination nodes should learn and build knowledge of the conditions of the transmission. Based on this, they have to decide on the sizes of the transmission or advertised windows, selective acknowledgment, and on other transmission parameters.

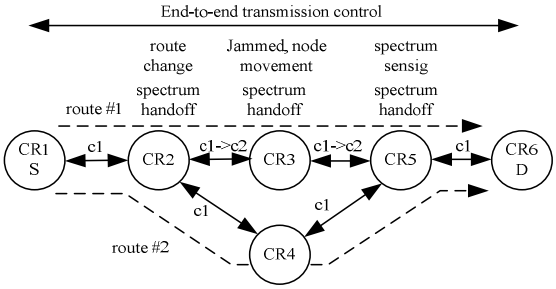

Fig. 1. End-to-end transmission control in a CRAHN.

On the other hand, the military CRAHNs operate under the umbrella of the set of policies imposing rules and limitations on traffic handling, quality of service (priorities, preemptions, and time characteristics), and security. This is another source of information that the source and destination nodes can use during transmission control. Moreover, military network nodes can often gather information from outside the CRAHN (i.e. using multi-interface radios/gateways).

After the analysis of current transmission control solutions, many required features can be found in TCP-CRAHN proposed by [31], TCP CoBA proposed in [32] and some TCP improvements in [33].

Following the literature descriptions, the end-to-end transmission control state diagram is proposed for source and destination nodes of the tactical CRAHN, which is shown in Fig. 2. This diagram is an enhancement of the original TCP. The main features compared to the original TCP are the reactions on sensing events in the intermediate nodes ("Sensing (3)"), the capability for channel handoff ("Channel handoff (4)"), the availability of policy sources ("Policy change (5)"), the capability to inform the routing about route failures ("Route failure (6)"), the availability of an external database ("DB query (7)"), and the capability to consider the application requests ("APPL req (8)" – Application Request Notifications (ARN) and Application Request Enforcements (ARE)) for e.g. bandwidth.

State #1 is responsible for collecting the initial parameters of the transmission path. It is based on the 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. The TCP SYNchronization (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. This information can be used by the NET queuing rules, by the routing, and by the MAC/PHY cognitive engines to support channel management in a part of the network where current transmission is handled (for example, the selection of stable channels with high data rate waveforms or slow channels with low probability of signal interception).

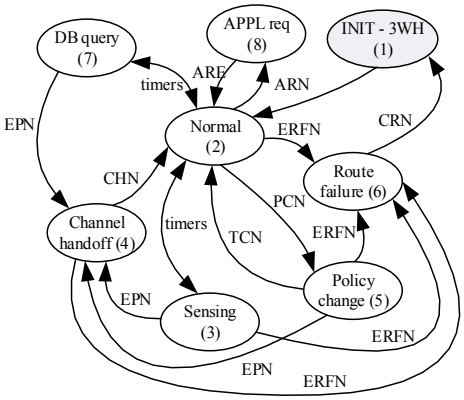

Fig. 2. Transmission control state diagram for the tactical CRAHNs.

After completion of the collection of the initial parameters, the transmission control mechanism moves to the "Normal" state (state #2) where TCP functions are performed.

The source and destination nodes will change to the "Sensing" state (state #3) when the intermediate nodes start the sensing procedure. Initially, it is assumed that sensing procedures performed at the MAC/PHY layers require breaking the transmission. If other sensing methods are identified to influence the transmission control (depending on military waveform solutions), they should be considered in the "Sensing" state. Transmission breaks typically lead to an 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 to stop the transmission before the sensing events and recreate it later with the same Congestion WiNDow (CWND) size. If the waveforms can adjust the sensing time, a source node can send a request to the intermediate nodes to reduce this time, depending on the application's requirement. One of the methods used to regulate the sensing time and used to increase transmission efficiency can be found in [31], but it should be verified according to the sensing method used in specific military waveforms.

While being in the sensing state, the end nodes can receive the information (in CCC) about channel handoff (Explicit Pause Notification (EPN)), which enforces moving to "Channel handoff" state (state #4). The EPN can be generated by each intermediate node. Source and destination nodes have to suspend transmission, pending the new links are ready. From [31] and [34] we can learn that standard TCP cannot effectively track the changes of an available bandwidth in a path between source and destination. Such a situation can be especially noticeable in tactical CRAHNs, where the accessible channels can be jammed, subject to interference, or 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. For example, the highest priority streams would require the most stable channels in the path. 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. The indicator of channel stability can be the channel accessibility rate. If a new channel is selected, the intermediate node must inform the end nodes on the new channel's (link) characteristics (available bandwidth, link quality, channel stability), which can be used to set up an appropriate CWND size, timeouts, and Maximum Segment Sizes (MSS). The intermediate node should send the Channel Handoff Notification (CHN) message. The transmission control mechanism reactivates an updated CWND (considering 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 reestablished 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.

E. Network management

CRN management was thoroughly addressed in [4]. The key finding is that the different mission phases should be separately addressed in the management functions. Due to the temporal nature of the military networks, configuration of a network is performed before the mission, monitoring as well as real-time management takes place during the mission, and finally collected information is analyzed after the mission. This is fundamentally different from civilian fixed and stable network setups.

In [4] a potentially important new approach to network management was not addressed, namely that of SDN. In the SDN approach, all management and network operations are performed by a *SDN controller*, implemented as a software component in a regular Central Processing Unit (CPU) platform. There are some studies, e.g. [10] and [11], anticipating the arrival of SDN technology also to the military tactical networks. Furthermore, some proposals for merging the SDN and CRN architectures have been made [12], [13]. In case this trend continues in military tactical networks, this will undoubtedly affect network management.

F. Trust management

The trust management problem in ad hoc networks has been intensively investigated in the past years, but CRAHNs impose new threats. In [35] the authors point out that trust management mechanisms are required to identify the malicious network nodes and to monitor the signaling traffic in the CCC. Most solutions for CRNs are devoted to detecting nodes transferring false sensing information. The literature presents some attacks using fake sensing information. Examples are Byzantine attack [36] or Spectrum Sensing Data Falsification attack [37]. The authors of [38] propose a trust assessment model for CRs, where a level of trust to other nodes is calculated based on direct observation of the node (signaling generated by this node) and based on reputation concerning a given node, identified and sent by other nodes. The direct observation leads to Bayesian analysis, and the reputation system is based on Dempster-Shafer theory [39]. The trusted nodes are considered in route selection.

Assuming that the main elements of the tactical CRs are cognitive engines that require mutual communications, effective trust management systems have to be applied in the CRAHNs. The nodes exchanging the signaling messages, which are required to build the knowledge about the spectral environment (i.e. cooperative sensing-based) or to support dynamic spectrum access and management (i.e. cognitive routing, TC), must trust other nodes. If the cognitive engine of the authenticated node would try to send false information (i.e. about sensing results), the rest of the network will completely collapse. Thus, in military CRNs, especially in tactical CRAHNs, it is proposed to take into account a solution similar to the TrUst-Based situation awarEness system (TUBE) [40].

The TUBE system performs three major functions: collection of information about the network environment, trust evaluation and classification of the nodes, and suggesting reactions to identified threats to ensure communication security. It is composed of the following modules: information acquisition, inference, recommendations, classification, and reaction. The heart of the system is the inference module, which is responsible for the evaluation of the nodes based on the results of direct observations and recommendations. However, recommendations can be biased or outdated, so they must be verified before using them 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 behavior can be triggered by different events. Moreover, the input data can be unreliable, incomplete and/or conflicted, so TUBE uses inference and classification processes proposed in [41]. This allows defining a set of primary and secondary hypotheses on the node behavior that improves the quality of potential threat detection. In case of direct evaluation based on performed actions, TUBE considers the following set of hypotheses: cooperating, uncertain cooperating, egoistic, suspect egoistic, honest, uncertain honest, liar, and suspect liar. The verification of those hypotheses leads to the neighboring node classification. Nodes 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 the classification can significantly contribute to the situation assessment of the CRAHN environment and should be used by the reaction module to provide an appropriate action, which can reduce the impact of the detected threats.

G. Control channel

Control information required by the technologies presented in subsections III-A to F will in most cases not be transmitted periodically but on demand. Consequently, the data volume may vary heavily. In order to avoid control channel *saturation* at load peaks, which would lead to message latency, the capacity must be sufficient.

However, a static control channel with high capacity, i.e. large bandwidth, will constrain resources for user data. On the other hand, a dynamic control channel, which can be adapted to the capacity needs, must be negotiated for each transmission and is thus only available with a delay. Therefore, a mixture of these approaches is recommended. E.g. in [6] a proposal to divide the control channel into several sub-channels, which can be dynamically allocated for a transmission, is described.

While a purely dynamic control channel usually connects two radio nodes, a static control channel may be used by all nodes of a network. For large networks, this may lead to network-internal interference or inefficiency. Therefore, larger networks are often split up into smaller subnetworks, e.g. via clustering (see section III-C). The nodes reached by the same control channel determine its *coverage*, which is equivalent to the cluster size in a clustered network. The disadvantage of network splitting is that messages crossing cluster borders suffer from additional latency. Therefore, the control channel coverage should be adapted to the data flow, i.e. heavily used routes should contain few cluster border crossings.

Delay of control messages may have an impact on the network. While a late hello message should not harm TC unduly, a delayed channel change message in a CRAHN may lead to exclusion of nodes from the network. Therefore, the messages must be prioritized accordingly. In addition, the support for cluster- and network-wide unicast, broadcast, and multicast control messaging may allow for systematic distribution of control information.

A further important aspect for the control channel is *robustness*, especially in tactical CRNs. That includes robustness against deliberate interference from incumbent spectrum users or hostile jammers, but also unintentional interference. A static control channel used by the whole network would be a single point of failure. Therefore, the authors of [7] propose using spread spectrum techniques, dynamic control channel allocation, and the use of jamming-resilient key distribution techniques for protecting vulnerable information (e.g. location). Moreover, trust management (see section III-F) should be used to ensure the correctness of the exchanged control information.

A control channel approach for military CRN must take into account the described aspects regarding robustness, message delay, coverage, saturation, dynamicity, and security.

IV. Architecture Framework

Based on the findings from the previous section, a new architecture framework for CRN is proposed. Fig. 3 gives an overview of its components and interfaces. The central element of the architecture framework is the decision making entity that consists of one or more cognitive engines. The entity is also responsible for the coordination and scheduling of parameter changes within the CRN. The decision making is supported by a set of toolboxes and libraries [8].

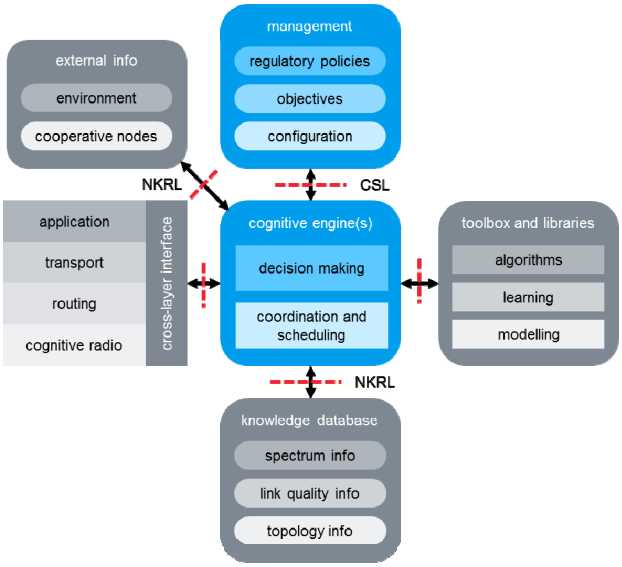

Fig. 3. CRN architecture framework proposal.

The cognitive engines have access to the protocol stack via a cross-layer interface. For management tasks (see section III-E) concerning policies, objectives, and the CRN configuration, the framework uses the Cognitive Specification Language (CSL) as defined in [1]. External information on the environment and cooperating nodes is stored in a knowledge database. Knowledge on these aspects is described, stored and exchanged via the so-called Network Knowledge Representation Language (NKRL), also defined in [1].

A central aspect of the framework is the concept of unilateral and multilateral cognitive processing, as proposed in [9]. Based on this, the cognitive processing resides on node level, i.e. it is decentralized, and the exchange of knowledge between the nodes is performed in an ad hoc manner.

In addition to the components and interfaces, which are depicted in Fig. 3, also the structure of the network was considered when developing the architecture framework. Consequently, the architecture supports clustering (see section III-C) and is well suited to support the typical structures of military mobile tactical networks.

V. Conclusion

In this paper, networking technologies in CRNs have been analyzed regarding their support for end-to-end optimization. As there is a focus on military CRN, typical military traffic patterns and security aspects, which go beyond civilian radio networks, have been considered.

The analysis has shown that existing network paradigms for fixed and civilian networks do not necessarily fit military tactical radio networks and may actually be counter-productive. Routing should use artificial intelligence or machine learning techniques to optimize route selection based on the cognitive cycle. For TC, the choice between multiple frequencies on a single link needs to be considered, as well as specific military aspects, like classification of position information or lack of updates due to radio silence.

Based on information from the cognitive engine, from the network management, and from other layers, an enhancement regarding TCP for a more efficient data transport has been 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 CRN.

Network management had been discussed in an earlier publication; in this paper we have shown that SDN may support CRAHN management, but that will need further research. 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 neighboring nodes, but also on a strong reputation system.

The control channel needs to deal with heavily varying data volumes; therefore, it should be adaptable to the current traffic. Finally, a new architecture framework for CRN has been proposed.

References

[1] R. W. Thomas, L. A. DaSilva, “Cognitive Networks”, in: Bruce A. Fette (ed.), “Cognitive Radio Technology”, Second Edition, Academic Press, 2009.

[2] J. Liu and S. Singh, “ATCP: TCP for Mobile Ad Hoc Networks”, IEEE Journal on Selected Areas of Communications, vol. 19, no. 7, pp. 1300-1315, July 2001.

[3] A. P. Janani, M. Sakthivel, and K. Baskaran, “A competitive performance analysis of reactive and proactive routing protocols of MANET under short time communication scenario”, International Journal of Wireless and Mobile Computing (IJWMC), Vol. 6, No. 3, pp. 253-260, 2013.

[4] T. Bräysy, S. Couturier, N. Smit, V. Le Nir, T. Tuukkanen, E. Verheul, B. Buchin, and J. Krygier, “Network management issues in military cognitive radio networks”, Int. Conf. on Military Communications and Information Systems (ICMCIS), Oulu, FIN, May 2017.

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

[6] S. M. Mirhoseninejad, R. Berangi, and M. Fathy, “Improving saturation capacity through verification of common control channel mechanism in cognitive radio ad-hoc networks”, 4th International eConference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, October 2014.

[7] B. F. Lo, “A survey of common control channel design in cognitive radio networks”, Elsevier Physical Communication, Volume 4, Issue 1, pp. 26-39, March 2011.

[8] M. Sooriyabandara, T. Farnham, P. Mahonen, M. Petrova, J. Riihijarvi, Z. Wang, “Generic Interface Architecture Supporting Cognitive Resource Management in Future Wireless Networks”, IEEE Communications Magazine, Vol. 49, Issue 9, September 2011.

[9] L. Doyle and T. Forde, “The Wisdom of Crowds: Cognitive Ad Hoc Networks”, in Q. H. Mahmoud, “Cognitive Networks: Towards Self-Aware Networks”, John Wiley & Sons, pp. 203-221, 2007.

[10] K. Phemius, J. Seddar, M. Bouet, H. Khalifé, and V. Conan, “Bringing SDN to the Edge of Tactical Networks”, Proc. of IEEE Milcom 2016.

[11] J. Spencer, O. Worthington, R. Hancock, and E. Hepworth., “Towards a tactical software defined network”, Proc. of ICMCIS 2016.

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

[13] S. Namal, I. Ahmad, S. Saud, M. Jokinen, and A. Gurtov, “Implementation of OpenFlow based cognitive radio network architecture: SDN&R”, Wireless Networks (2016), 22: 663-677.

[14] M. Cesana, F. Cuomo, E. Ekici, “Routing in cognitive radio networks: Challenges and solutions”, Challenges and solutions, Ad Hoc Networks, 2010.

[15] J.-J. Lee and J. Lim, “Cognitive Routing for Multi-hop Mobile Cognitive Radio Ad Hoc Networks”, Journal of Communications and Networks, vol. 16, no. 2, April 2014.

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

[17] H. Rogge, E. Baccelli, “Directional Airtime Metric Based on Packet Sequence Numbers for Optimized Link State Routing Version 2 (OLSRv2)”, RFC 7779, April 2016.

[18] K. Singh, S. Mohn, “Routing protocols in cognitive radio ad-hoc networks: A comprehensive review”, Journal of Network and Computer Applications 72 (2016) 28–37.

[19] L. Hou, K. Yeung, K. Wong, “A vision of energy-efficient routing for cognitive radio adhoc networks”, 6th International Symposium on Wireless and Pervasive Computing (ISWPC), 2011. IEEE. p. 1–4.

[20] Y. Zhang, F. Song, Z. Deng, C. Li, “An energy aware routing for cognitive radio ad hoc networks”, Int. Conf. on Information Science and Technology (ICIST), 2013. IEEE. pp. 1397–1401.

[21] R.A. Rehman, B.S. Kim, “L2ER: Low-latency and energy-based routing protocol for cognitive radio ad hoc networks”, Int. J.Distrib. Sens. Netw. 2014.

[22] S. Kamruzzaman, E. Kim, D.G. Jeong, “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.

[23] M.A. Rahman, M. Caleffi, L. Paura, “Joint path and spectrum diversity in cognitive radio ad-hoc networks”, EURASIP J. Wirel. Commun. Netw. 2012(1), 1–9.

[24] Z. Che-aron, A. Abdalla, W Hassan, K Abdullah, M. Rahman, “E-D2CRAP: A joint path and spectrum diversity based routing protocol with an optimized path selection for cognitive radio ad hoc networks”, 2nd International Symposium on Telecommunication Technologies (ISTT), 2014 IEEE, pp.39–44.

[25] C. Chih-Min, F. Hsiang-Yuan, Z. Li-Ren, “An Anypath Routing Protocol for Multi-hop Cognitive Radio Ad Hoc Networks”, IEEE 11th Intl Conf on Ubiquitous Intelligence & Computing, 2014, pp. 127-133.

[26] A.A.H. Al-Rawi, A.Y. Kok-Lim, M. Hafizal, R. Nordin, H. Wahidah, “Reinforcement Learning for Routing in Cognitive Radio Ad Hoc Networks, Hindawi Publishing Corporation”, Volume 2014, Article ID 960584.

[27] T. Safdar, H.B. Hasbulah, M. Rehan, “Effect of Reinforcement Learning on Routing of Cognitive Radio Ad-Hoc Networks”, 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC), 2015.

[28] E. Even-Dar, Y. Mansour, “Learning Rates for Q-learning”, Journal of Machine Learning Research 5 (2003) 1-25.

[29] R. Massin, C. J. Le Martret, P. Ciblat, “A Coalition Formation Game for Distributed Node Clustering in Mobile Ad Hoc Networks,” in IEEE Transactions on Wireless Communications, vol. 16, no. 6, pp. 3940-3952, June 2017.

[30] J. Liu, S. Singh, “ATCP: TCP for Mobile Ad Hoc Networks”, IEEE J. Selected Areas of Comm., vol. 19, no. 7, pp. 1300-1315, July 2001.

[31] K. R. Chowdhury, M. D. Felice, I.F. Akyildiz, “TCP CRAHN: A Transport Control Protocol for Cognitive Radio Ad Hoc Networks”, IEEE Transactions on Mobile Computing, vol. 12, no. 4, April 2013.

[32] K. Tsukamoto, S. Koba, M. Tsuru, Y. Oie, “Cognitive radio-aware transport protocol for mobile ad hoc networks”, IEEE Transactions on Mobile Computing, 14(2), 2015, pp. 288-301.

[33] X. Ya-yun, Z. Liu-lei, "TCP enhancement technology in cognitive network based on cross-layer designing", IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), pp. 1-4, 2016.

[34] A.M.R. Slingerland, P. Pawelczak, R.V. Prasad, A. Lo, and R. Hekmat, “Performance of Transport Control Protocol over Dynamic Spectrum Access Links,” Proc. Second IEEE Int’l Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN), Apr. 2007.

[35] 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.

[36] A.S. Rawat, P. Anand, H. Chen, P.K. Varshney, “Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks”, IEEE Transactions on Signal Processing 59 (2): 774–786, 2011.

[37] R. Chen, J. Park, Y. Hou, J. Reed, “Toward secure distributed spectrum sensing in cognitive radio networks”. IEEE Commununications Magazine 46 (4): 50–55, 2008.

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

[39] G. Shafer, “A Mathematical Theory of Evidence”, Princeton University Press, 1976.

[40] M. Amanowicz, J. Głowacka, K. Parobczak, J. Krygier, “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.

[41] F. Smarandache and J. Dezert, “Advances and Applications of DSmT for Information Fusion, vol.1 - 3,” American Research Press Rehoboth, 2004, 2006, 2009.