Cognitive Radio and Networks in coalition deployments through the dual use of IEEE 802.11h

Lorenza Giupponi, José Nuñez, Iñaki Pascual, Josep Mangues

Outline

• Introduction to the project
• Scenarios and vignettes
• Routing protocol model
• Implementation Details
• Testbed setup
• Conclusions
Introduction

• Interest from the Spanish Ministry of Defense to investigate cognitive radio and networking paradigms.

• The project started in 2016.

• The project funds us during 2 years.

• The objectives of the project are aligned with NATO RTG IST140 (previous IST 077).
Motivation

• In military environments
  • The different nations rely on a fixed frequency assignment.
  • The fixed frequency assignment in many cases is not efficient and not operative.
• Coalition deployments:
  • Platoons from different nations operate in the same band often without interoperational capabilities.
  • Are characterized by a high variability of the theatre of operations
• A dynamic management of frequencies may be very useful.
• This has already been proven via simulation studies in IST077.
Requirements from the client

• Dual use of civil technology.
• If possible, rely on COTS (Commercial off-the shelf) products.
• Experimental approach
• Study of both cognitive radio and cognitive networking solutions.
• Particular interest in cognitive routing solutions and effective distributions of information.
• Not interested in more traditional routing solutions based on routing tables, due to
  • difficulty to maintain these tables in very dynamic tactical environments
  • need to avoid as much as possible exchange of control information
• Assessment of scalability
Methodology

• We take advantage of COTS, like IEEE 802.11 h to coexist in 5 GHz bandwidth between WiFi and radar technology.
• IEEE 802.11h includes
  • Dynamic frequency selection
  • Transmission power control
• We build a IEEE802.11ac wireless multi-hop testbed where we exploit those functionalities at two levels of cognition:
  • cognitive radio
  • cognitive networking, load aware routing.
Methodology

- ns-3 emulation capabilities are exploited for rapid prototyping
- The same code will be used in simulations and in the testbed.
- This enables cross-validation of simulated and experimental scenarios, hence offering the best of both worlds:
  - Model validation for the simulator based on experimental evaluations
  - Scalability assessment of the scheme in the simulator once models have been validated.
Technical problems we aim to solve

- **Problem 1**: Configuration of the cognitive ad-hoc network and distribution of the control information.

- **Problem 2**: Intra-platoon interference control by means of transmission power control.

- **Problema 3**: Detection of transmissions coming from other foreign platoons and consequent channel re-selection (inter-platoon interference control).

- **Problema 4**: Routing algorithm for a cognitive network.

- **Problema 5**: Scalability.
Outline

• Introduction to the project
• **Scenarios and vignettes**
• The Protocol Model
• Implementation Details
• Testbed setup
• Conclusions
Simulation methodologies and vignettes in IST077

- Scenarios based on the vignettes defined in IST-077 group.
- Prevention of an aid convoy attack.
- NATO troops are involved in peacekeeping operations.
- They only can operate in case of self-defense.
- NGOs provide food and medical equipments through aid convoys.
- A group of rebels has been recently attacking the zone.
- A coalition deployment supervises the route of the humanitarian convoy from a distance.
- The objective of the tactical vignette is to prevent the hijack of such an humanitarian convoy.
Preventing the hijack of an aid convoy vignette
Vignette IST 077

- Cloud 1: Company BEL
  - Platoon 1 and platoon 2 BEL
  - Voice/data
- Cloud 2: Platoon 1 BEL
  - Voice/data
- Cloud 3: Pelotón 2 BEL
  - Voice/data
- Cloud 4: Company FR
  - Platoon FR
  - Voice/data
- Cloud 5:
  - Platoon GE
  - Voice/data
- Cloud 6:
  - Convoy
- Cloud 7
  - Rebels
Possible frequency conflicts that we aim to reproduce and deal with

- Clouds 3, 4 and 5 operate in the same frequency channel in uncoordinated fashion.

- The rebels try to attack the frequency of operation of clouds 3, 4 and 5.

- The helicopter of cloud 4 has a counter-RCIED (Radio Controlled Improvised Explosive Device) which affects the frequency of operation of clouds 3 and 5.
Outline

- Introduction to the project
- Scenarios and vignettes
- Routing protocol model
- Implementation Details
- Testbed setup
- Conclusions
Cognitive networking

• We need cognitive routing approach which:
  • reduces to the minimum the control information exchange
  • takes decisions based on local information
  • quickly adapts to dynamic tactical environments

• We propose backpressure (BP) routing approach due to:
  • scalability,
  • low overhead,
  • maximization of resource usage in high mobility and dynamic wireless contexts,
  • low requirements in terms of state stored at nodes.
Cognitive networking

- **Neighbour Discovery**: BP does it, each node maintains neighbour tables.

- **Route dissemination**: BP does not need it, and this reduces significantly the overhead.

- **Route calculation**: BP does it, but at packet level.

- **Route recovery/maintainence**: not needed it.
The Backpressure idea

Shortest Path Routing

Backpressure Routing

• Minimize a drift-plus-penalty function
  • Lyapunov drift $\Delta(t) = L(t+1) - L(t)$
    • $L(t)$ function that measures network congestion
  • Penalty $p(t)$ quantifies the cost of performing routing decisions satisfying $\Delta(t)$ minimization
  • Control Parameter $V$ allows for appropriate trade-off between backlog reduction and penalty minimization
Distributed Max-Weight Policy

The weight of a link \((i,j)\) with a data packet to transmit to reach \(d\) is calculated as follows:

\[
    w_{ij} = \Delta Q_{ij} - Vp(i, j, d)
\]

Distributed Max-Weight Policy

Minimize over-the-air resources
get closer to the destination

select less congested nodes

Strong Stability

\((x_{\text{dest}}, y_{\text{dest}})\)

destination

\((x_1, y_1)\)

\((x_2, y_2)\)

\((x_3, y_3)\)

\((x_4, y_4)\)
V Parameter Illustration

**Distributed Weight computation:**

\[ w_{ij} = \Delta Q_{ij} - Vp(i, j, d) \]

backpressure reach destination

What is the role of the V parameter in practice?
Backpressure offers robustness under heterogeneous wireless link rates choosing higher rate links over low-rate links.

Backpressure shows lower latencies since 1) longer paths only used under congestion 2) lower queuing latencies.
Outline

• Introduction to the project
• Scenarios and vignettes
• The Protocol Model
• Implementation Details
• Testbed setup
• Conclusions
From simulation to rapid prototyping

• Protocol Implemented in Ns-3 simulator
  • Ns-3 is a quite accurate network simulator but still a simulator

• Ns-3 asset: Emulation Mode
  • You do not need to make double effort to test your schemes in simulations and in testbeds.
  • It allows the ns-3 simulator to send ns-3 packets to real physical devices, and to receive real (and ns-3) packets from physical devices.
  • The protocol requires to manage data queues to take routing decisions and there are various implementation issues.
Ns-3 emulation mode

- Physical Nodes have one ns-3 process running
  - routing intelligence
- It allows executing ns-3 IP stack over physical devices implementing L2 functionalities
- ns-3 provides the interface with the real physical device
  - RAW sockets
  - to generate/receive/send packets from/to the real device
  - real devices on PROMISCUOUS mode
Ns-3 Emulation: Characteristics

• ns-3 emulation is based on MAC spoofing
  • FdNetDevice avoids this way conflicts between virtual ns-3 IP stack (virtual MAC address) and real IP stack (real MAC address)
• SOCKET RAW captures all Ethernet packets
  • FdNetDevice sends to ns-3 stack the packets that have the specified ns-3 MAC address
  • Packets generated with ns-3 are sent with a source, and destination MAC addresses different than the real physical MAC address
  • Packets with the real source and destination MAC address are sent to the real node stack
Outline

• Introduction to the project
• Scenarios and vignettes
• Routing protocol model
• Implementation Details
• Testbed setup
• Conclusions
Testbed setup

- The testbed consists of 15 nodes emulating soldiers of platoons.
- Each node accounts with 2 IEEE802.11ac cards for control and data communications, intra- and inter-platoon.
  - chipset Atheros AR10XX
- An Agilent signal generator is used to generate jamming and other kind of co-channel signals.
- Nodes have installed Linux/GNU (Ubuntu 14.04 Desktop 64 bits).
- Network Time Protocol for node synchronization
Testbed setup

- Driver and firmware of the cards is ath10k
- We substitute the original firmware with the one provided by Candela Technologies
  - It allows “ad-hoc” mode, which is fundamental to allow every node in the platoon network to be able to talk to all the other nodes
  - It allows for channels of 20 MHz, and also of 40 and 80 MHz.
  - It allows direct access to firmware source code.
  - With commands `iw` or `iwconfig`, we can easily change the channel, the bandwidth, the transmission power.
Testbed setup

- TPC: We have tested that transmission power can be properly changed, by measuring the received power in a receiving node.
- To activate DFS and TCP functionalities we need:
  - IEEE 802.11d: it is an amendment approved in 2001 to 802.11, which allows clients to automatically configure themselves to their local regulatory domain.
  - IEEE 802.11k: it is an amendment approved in 2007 to 802.11, to facilitate radio resource management and maintainance.
DFS Test

```
root@sc228:/home/snet# hostapd /etc/hostapd/hostapd-ac.conf
Configuration file: /etc/hostapd/hostapd-ac.conf

wlan2: Interface state UNINITIALIZED -> COUNTRY_UPDATE
wlan2: Interface state COUNTRY_UPDATE -> HT_SCAN
wlan2: Interface state HT_SCAN -> DFS
wlan2: DFS-CAC-START freq=5640 chan=128 sec chan=1, width=1, sep=122, seg1=8, cac_time=60s
wlan2: DFS-CAC-COMPLETED success=1 freq=5640 ht_enabled=0 chan_offset=0 chan_width=3 cf1=5610 cf2=0
Using interface wlan2 with hwmode=802.11b,g,pcap=26 and ssid "ATH10K"
wlan2: Interface state DFS->ENABLED
wlan2: AP->ENABLED
wlan2: DFS-RADAR-DETECTED freq=5640 ht_enabled=0 chan_offset=0 chan_width=3 cf1=5610 cf2=0
wlan2: DFS-RADAR-DETECTED freq=5640 ht_enabled=0 chan_offset=0 chan_width=3 cf1=5610 cf2=0
wlan2: DFS-RADAR-DETECTED freq=5640 ht_enabled=0 chan_offset=0 chan_width=3 cf1=5610 cf2=0
wlan2: DFS-RADAR-DETECTED freq=5640 ht_enabled=0 chan_offset=0 chan_width=3 cf1=5610 cf2=0
wlan2: IEEE 802.11 driver had channel switch: freq=5180 ht=1, offset=1, width=3 (80 MHz), cf1=5210, cf2=0
wlan2: AP-CTRL-FINISHED freq=5180 of=0
```
Traffic generated by *netperf, iperf*. 
Packets of 1500 bytes
Latency is measured by *hping3*
There are unexpected results
1 Hop Test

- T1: Packet P is received at PHY
- T2: Packet P has been processed by firmware and driver ath10k
- T3: ACK received at PHY
- T4: ACK has been processed by firmware and driver ath10k
  - Original firmware does not present this problem at 40 MHz.
  - At 20 MHz the behaviour is correct in both firmwares.

<table>
<thead>
<tr>
<th>Time</th>
<th>msec</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0</td>
</tr>
<tr>
<td>T2</td>
<td>0.003</td>
</tr>
<tr>
<td>T3</td>
<td>0.027</td>
</tr>
<tr>
<td>T4</td>
<td>3.303</td>
</tr>
</tbody>
</table>
2 Hop Test

Throughput in Mbps

Channel bandwidth in Mhz

TCP  UDP  TCP

RTT in ms

Channel bandwidth in Mhz

TCP  UDP  TCP
Conclusion

• We are studying the dual use of WiFi technology for cognitive radio/networks technology in coalition deployments
• We have proposed to take advantage of rapid prototyping capabilities of ns-3
• We have shown some initial simulation results based on a backpressure routing approach
• We have setup the testbed and we are dealing with some implementation issues to move to prototyping