# Wireless Sensor Networking Support to Military Operations on Urban Terrain

A. Grilo, R. Silva, P. Nunes, J. Martins, M. Nunes

# Layout

- Motivation
- Overview of Project UbiSec&Sens
- MOUT WSN Architecture
- Networking Issues
- Security Issues
- Conclusions

# Motivation

- September 11th 2001: shift to Operations Other Than War (OOTW)
  - ➔"Three Block War" (Gen. C. Krulak - USMC)
  - ➔Military Operations on Urban Terrain (MOUT)
  - ➔Constraining Rules of Engagement (RoE)
- MOUT have many points in common with counter-terrorism HS operations
  - ➔Complexity of urban environments
  - ➔Adversary may have a better understanding about the operational environment

# Motivation

"Network Centric Warfare assisted by robust sensor networking is paramount to reduce situation uncertainty, providing early-warning and tracking of unpredicted intrusions in areas considered already cleared, thus denying the intruder the advantage of surprise."

# Motivation

- Wireless Sensor Networks (WSNs)
  - ➔ Low-cost Nodes equipped with sensors and/or actuators
  - ➔ Ad-Hoc connectivity
    - **No infrastructure, relying on node collaboration**
    - **Nodes implement both data gathering and routing**
  - ➔ Self-organized
  - ➔ Robust
  - ➔ Limitation in terms of processing, communications and energy
    - **Must be optimized to comply with application requirements**

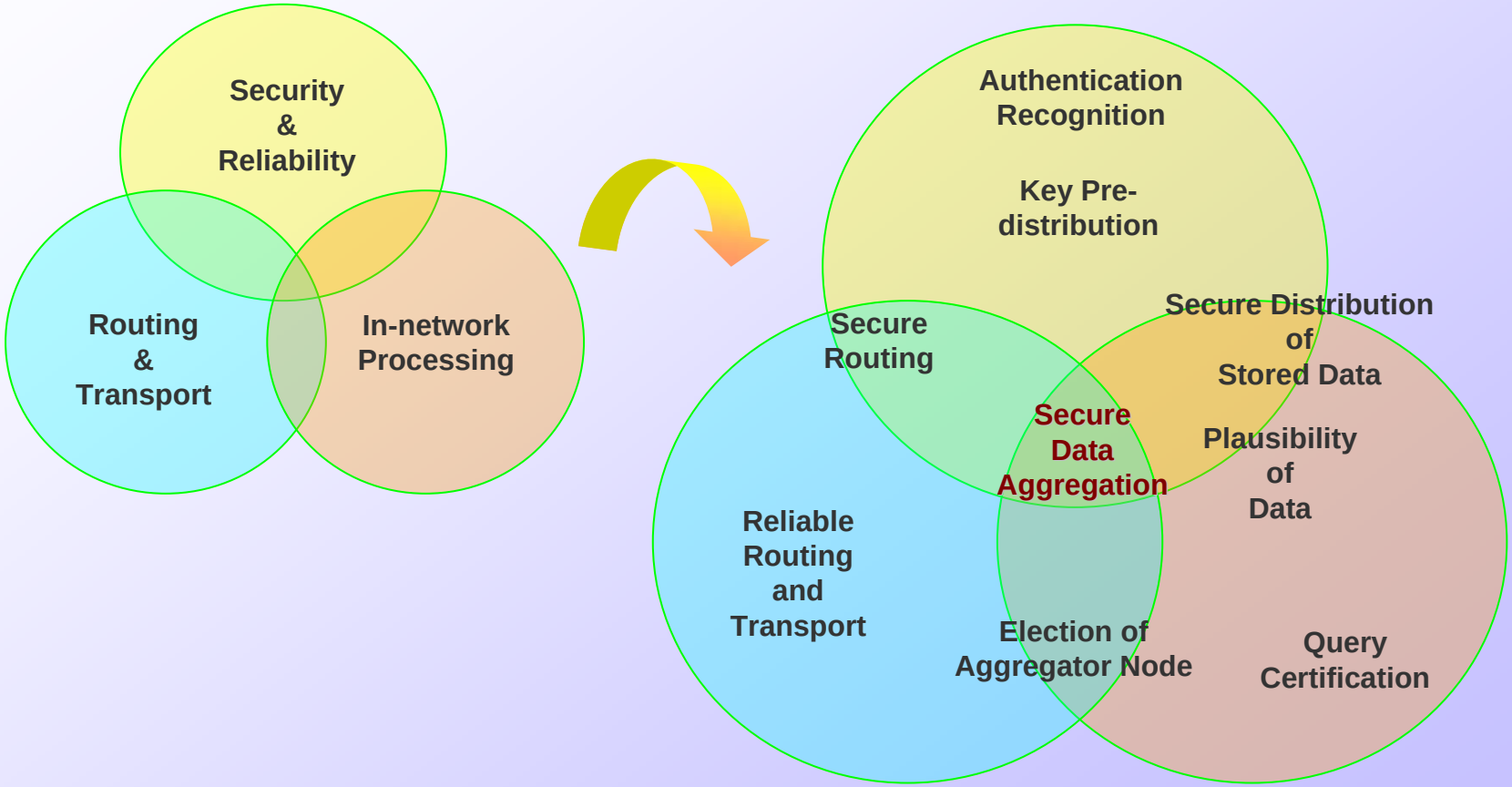
# UbiSec&Sens Objectives

- To build a comprehensive understanding of secure-sensor network architectures.
- To give Europe the lead in this area and to encourage further research and commercial development in the European domain.
- To develop a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security.
- To provide a toolbox of security-aware components, which will be easily configurable by manufacturers and service developers

# UbiSec&Sens at a glance

- Duration 36 months (Jan 06 – Dec 08)
- Effort spanning 6 WPs
- Costs: 2.9 Mio €
- 8 Partners from 5 (4) countries
  - ➔ Germany: Eurescom, RWTH, IHP, RUB, NEC (UK)
  - ➔ France: INRIA
  - ➔ Portugal: INOV
  - ➔ Hungary: BUTE
- http://www.ist-ubisecsens.org/

# UbiSec&Sens Research Areas



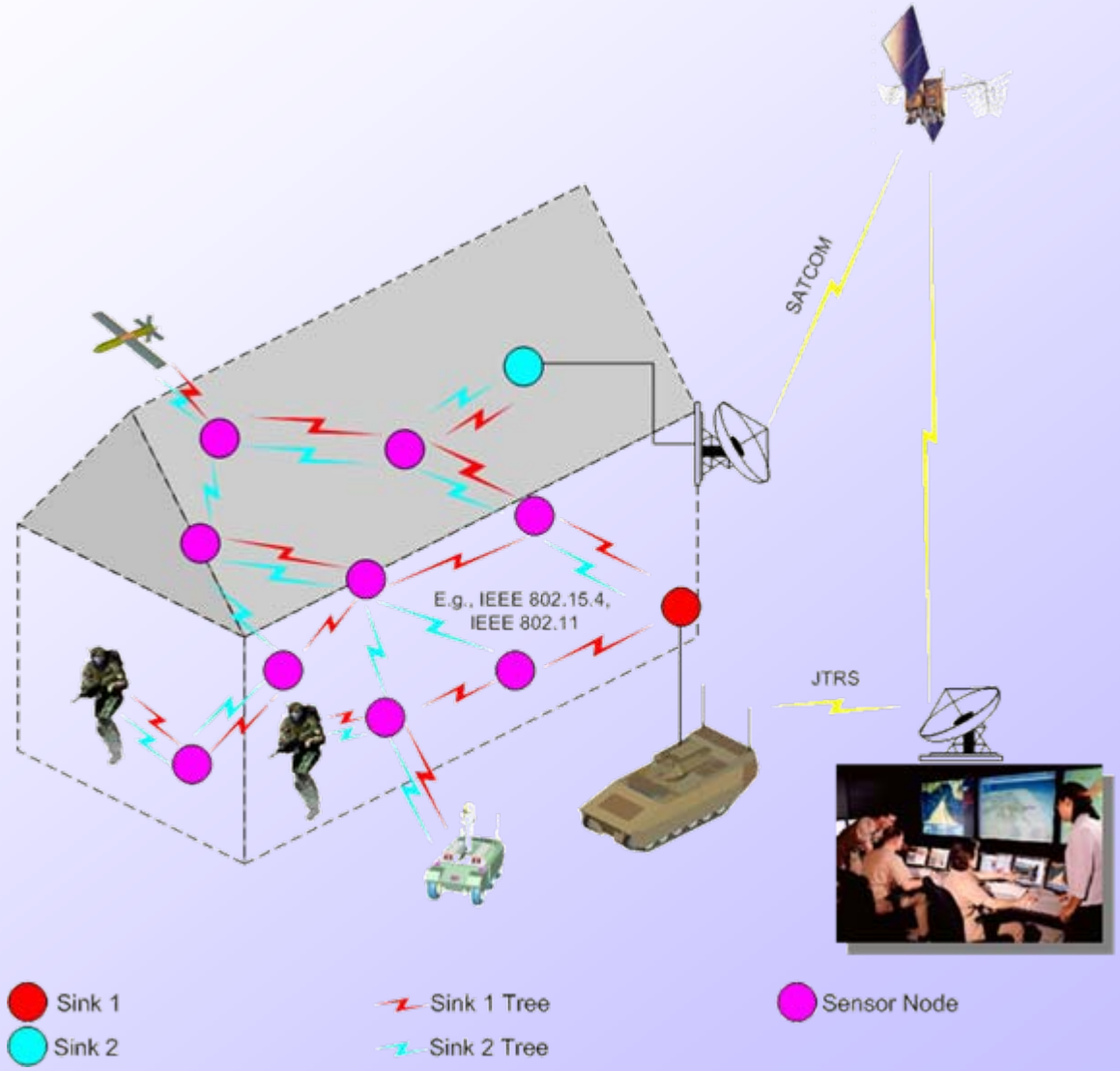
# UbiSec&Sens Demo Scenarios

- Agriculture
- Road Services
- Homeland Security (INOV)
  - ➔ Collaboration with Military Academy:
    - **Requirements definition**
    - **Adaptation to MOUT applications**

# Layout

- Motivation
- Overview of Project UbiSec&Sens
- MOUT WSN Architecture
- Networking Issues
- Security Issues
- Conclusions

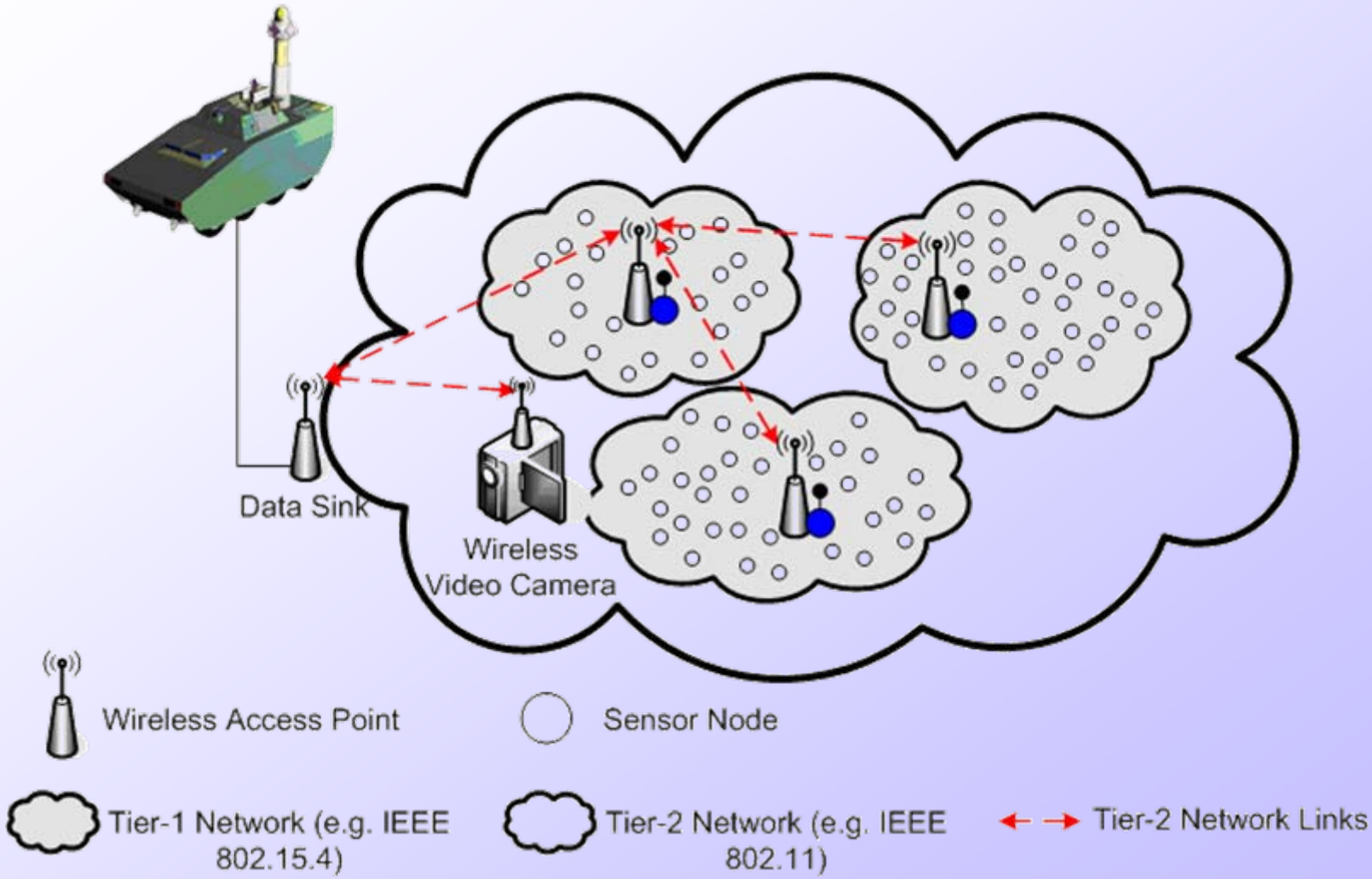
# MOUT WSN Architecture



# Sensor Types

- Functional requirements point to the use of the following sensor types:
  - ➔ Presence/Intrusion
    - **E.g., based on a combination of infrared, photoelectric, laser, acoustic, vibration, etc.**
  - ➔ Ranging
    - **E.g., RADAR, LIDAR, ultrasonic, etc.**
  - ➔ Imaging
    - **Including infrared and LADAR imaging**
  - ➔ Noise
    - **Acoustic sensor able to produce an audio stream**
  - ➔ Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) and Toxic Industrial Material (TIM) detectors
    - **Currently active research topics**

# Two-Tier MOUT WSN



# Layout

- Motivation
- Overview of Project UbiSec&Sens
- MOUT WSN Architecture
- Networking Issues
- Security Issues
- Conclusions

# Networking Issues

- Optimization goals in all protocol layers:
  - Energy Efficiency vs Latency
  - Reliability
  - Robustness
  - Resilience
  - Flexibility
  - Scalability
- INOV research activities in UbiSec&Sens mainly address:
  - Medium Access Control (MAC) layer
  - Transport layer
  - Application layer

# TP-MAC

- TP-MAC: A new MAC protocol suitable for alarm notifications in long-term surveillance applications:
  - ➔Ultra-low duty cycle
  - ➔Low latency

# TP-MAC Basic Principles

# TP-MAC Results and Exploitation

- Analytical results point to significant potential improvements over state-of-the-art.
- More complex than other MAC protocols.
- A new and simpler TDMA MAC protocol is under development, which incorporates lessons learned from TP-MAC (e.g. cascading and multi-sink)

# Reliable and Efficient Transport

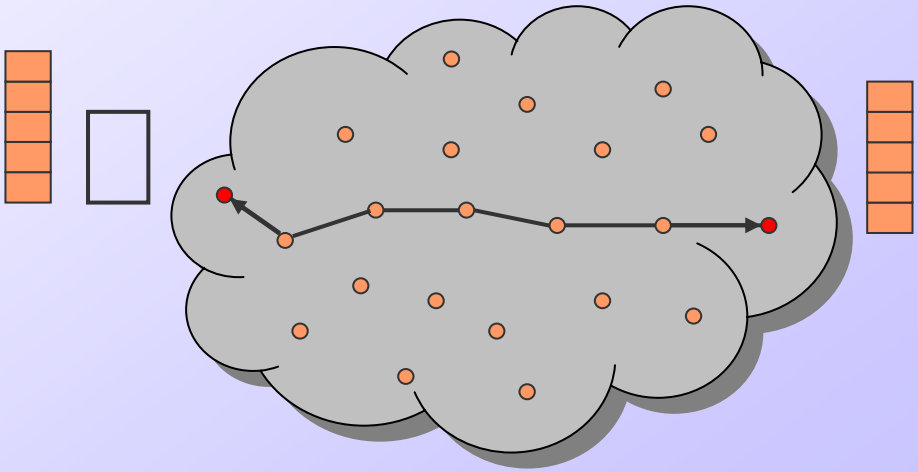
- Motivation:
  - ➔Lack of a multi-functional transport protocol that can be tailored to suit multi-application sensors/networks, sparing code memory resources;
  - ➔Lack of flexibility in current solutions to support different reliability grades (e.g., full + probabilistic);
  - ➔Deficiencies in end-to-end full reliability presented by current solutions.

# Distributed Transport for Sensor Networks (DTSN)

- Assumptions:
  - ➔Reliable MAC layer;
  - ➔Underlying bi-directional routing and global node addressing/ID;
- Features:
  - ➔Support of total and/or partial reliability grade;
  - ➔Robustness in presence of high error rates;
  - ➔Energy efficiency (low overhead);
  - ➔Distributed execution (in-network processing).

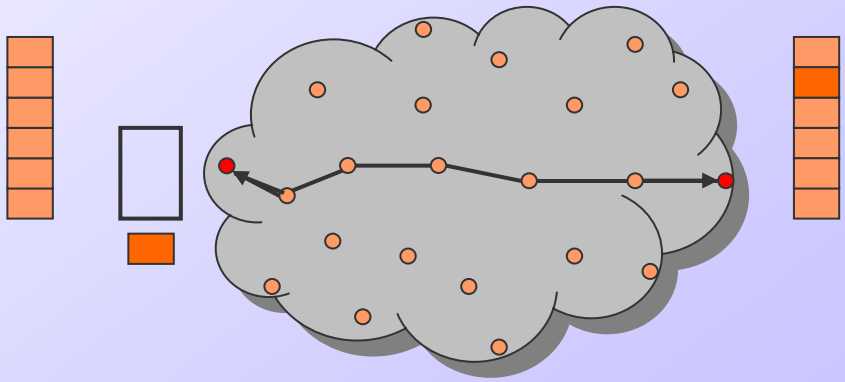
# Basic Transport Service

- Transport service for critical data (essential informative content);
- Sliding window with selective repeat;
  - ➔ Buffering at the source of all the data sent until a confirmation is received;
- Caching at intermediate nodes spares retransmissions.



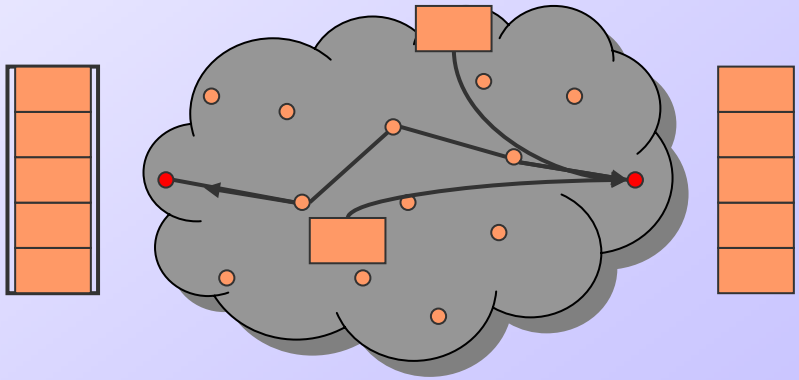
# Enhancements

- Service for loss tolerant communications;
- Enhancement flow and FEC coding can be enabled:
  - ➔ Buffering at the sender of a data core (essential parts of the data chunk);
  - ➔ Enhancement packets not buffered at the sender.
  - ➔ Generation of parity packets.
- Throughput related to data core/enhancement flow ratio:
  - ➔ High values achievable;
  - ➔ Low occupation of memory resources at the sender.



# DTSN Communication Control

- Communication **controlled by the sender** through the generation of acknowledgement requests (may be piggybacked with data).
  - ➔ Receiver can only respond to request messages – low signaling overhead.



# DTSN Results and Exploitation

- DTSN can be tailored to suit different WSN applications, namely intrusion detection;
- Low energy consumption and high reliability;
- Throughput improved by the combination of erasure coding (partial reliability) and intermediate caching.
- DTSN combines well with new MAC protocol.
- DTSN basic service already implemented in TinyOS (as of July 2006) now being enhanced.

# Layout

- Motivation
- Overview of Project UbiSec&Sens
- MOUT WSN Architecture
- Networking Issues
- Security Issues
- Conclusions

# Security Issues

- Information and network assurance are vital to the successful conduct of Network Centric Operations.
- Expected attacks to the MOUT WSN:
  - ➔ Physical attacks against network nodes
  - ➔ Logical attacks against communications

# Physical Attacks

- Capture and analysis of one or more nodes of the WSN must not compromise the security of the whole WSN
- Mechanisms must be in place to minimize the probabilities of successful physical tampering of captured WSN nodes
  - ➔ E.g. Tampering detectors that trigger self-destruction mechanisms.

# Logical Attacks

- Difficult to detect
- Passive and Active attacks
- Active attacks may span all layers of the protocol stack:
  - ➔ Physical/MAC: Jamming (may be low power)
  - ➔ Routing: Black-hole, wormhole, false routes, etc.
  - ➔ Transport: False acknowledgements, false congestion notifications, etc.
  - ➔ Application: Fake/corrupt data.

# Conclusions

- Development of requirements and architecture for a MOUT WSN (INOV + Academia Militar).
- Main networking + security issues and challenges were identified and are currently being addressed in the project.
- Already some achievements in the networking area:
  - ➔ TP-MAC, DTSN
- New networking and security solutions under development:
  - ➔ New lightweight MAC protocol using lessons learned from TP-MAC
  - ➔ DTSN security
  - ➔ Chaos-based key distribution.
- Demonstrator to be ready in 2008

# Contacts

- INOV:
  - António Grilo: antonio.grilo@inov.pt
  - Rui Silva: rs.beja@gmail.com
  - Mário Nunes: mario.nunes@inov.pt
- Academia Militar
  - Maj. José Martins: josecarloslm@netcabo.pt
  - Lt.Col. Paulo Nunes: josecarloslm@netcabo.pt