Security in dynamic networks where degraded mode is the nominal mode of operation

Thales visit at LaBRI

Topic of discussion: Security

Pr. S. Chaumette, serge.chaumette@labri.fr

Head of Mobility, Ubiquity, Security (Muse) research group

In charge of UAVs activities at LaBRI

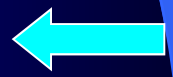
LaBRI, University of Bordeaux, France

Goals and research topics of the Muse research group at LaBRI

Contribute to the definition and development of supporting middleware, tools and mechanisms formally validated that make it possible to take advantage in a secure way of the mobile resources which are wirelessly connected to the network and to develop applications on top of these resources.

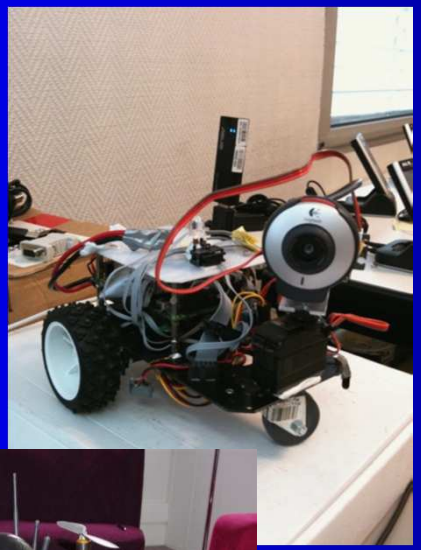
Target systems

Secured fleets of autonomous communicating mobile terminals



Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

Physical targets



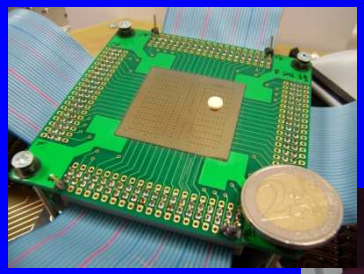
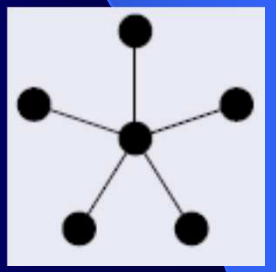


Image courtesy the
Smart Surface project)

Underlying dynamic graphs



Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

Autonomous swarm

- Autonomous as individuals

Image courtesy Fly-n-Sense

- Autonomous as a swarm

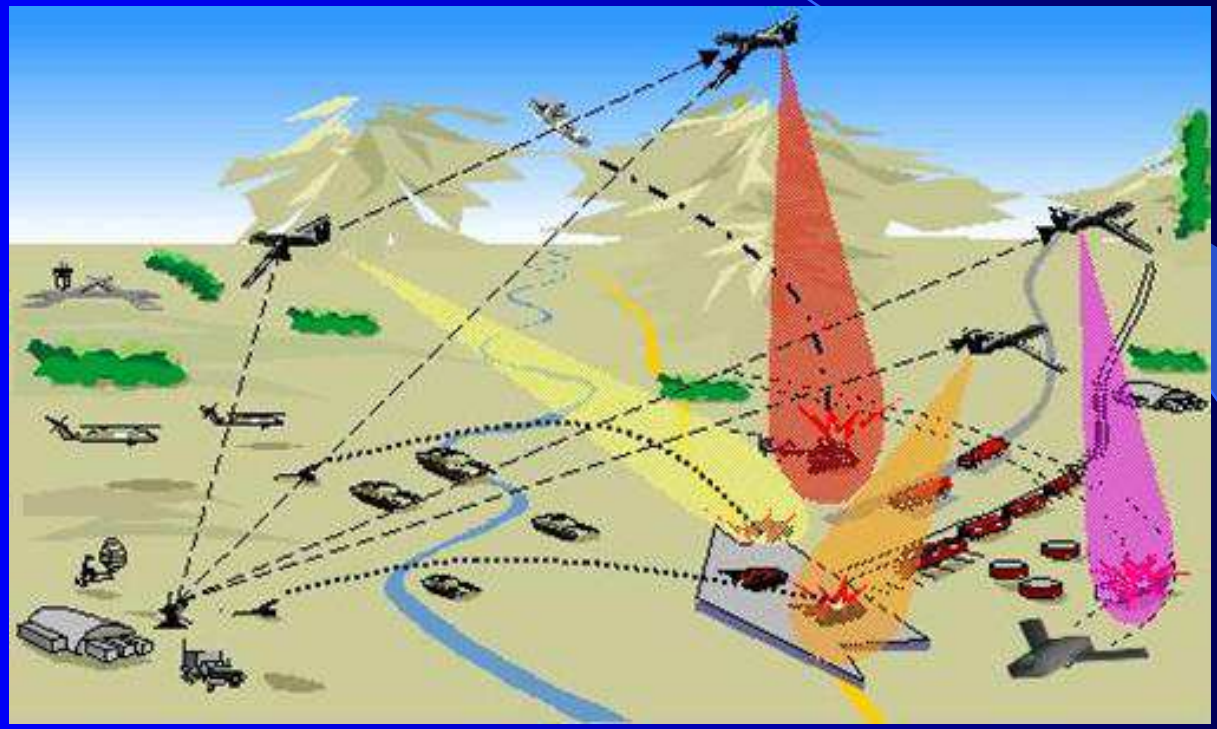
  but still collaborative

  - to achieve missions
  - because of inherent swarming issues

Source: http://wallpapershi.net/birds-swarm-vortex-animal/

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

- Autonomous as a swam of swarms



Source : http://www.cds.caltech.edu/~murray/projects/darpa01-mica/

Swarming raises a number of new mission oriented issues

distributed system, local computation based algorithms, construction of a global view of the overall system based on local information, unsecure boundaries, security, ground control stations, data fusion for situation management, etc.

Degraded mode (scalability)

- *“classical separation between “nominal operation" and "faults" becomes untenable; system is continuously operating under faults”*

  Werner J.A. Dahm, Arizona State University
  in his keynote at
  AIAA Guidance, Navigation, and Control Conference
  19 - 22 August 2013, Boston , Massachusetts

- Among the “faults” are
  - Loss of a UAV
  - Loss of a communication link

➔ Think localy

- Neither rely on communication, nore on the stability of your neighbourhood
  - this is most of the time ignored
  - this leads to probabilistic mission sucess

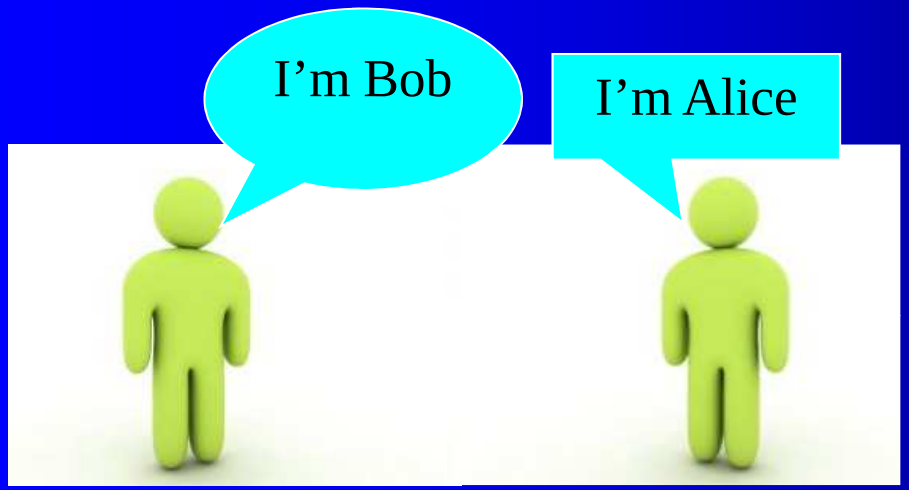
« Always consider other scenarios – ‘’What if ?’’ »

Georges T. Schmidt, Editor-in-chief,
AIAA Journal of Guidance, Control and Dynamics

in his keynote on lessons learned in the Apollo GN &C Program

AIAA Joint Conferences
19 - 22 August 2013, Boston , Massachusetts

Paradigm shift for security



Share keys, authenticate

Recognize
- individually
- group/topic based

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

Impact on security

- The objectives must be lowered because of unsecure boudaries
- Examples:
  - entity based keyes → group/topic based keyes
  - authenticate → recognize
- But … this is real life (as in human crowds) ☺

Paradigm shift for applications

How many people are there ?

Are there many people ?

(or approximate number, lower boound)

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

Current work on a set of collaborative heterogeneous swarms

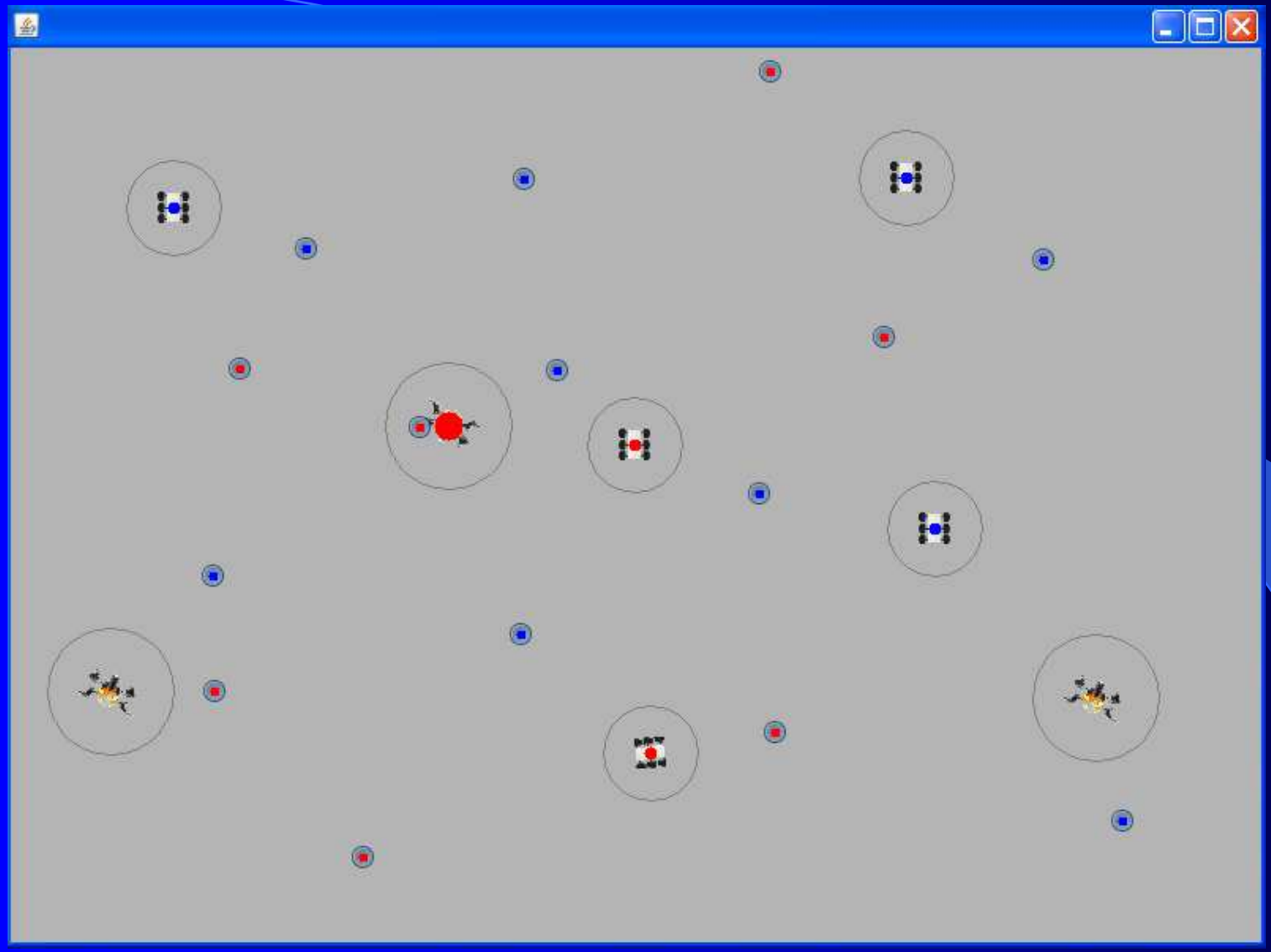
- Scenario 1: **garbage collection in a park**

  funded by the French Army (DGA) and Région Aquitaine

- Scenario 2: **garbage/mines search and destroy with UAVs, UGVs, UUVs**

  funded by the French Army (DGA), Région Aquitaine and Thales

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013



- Blue garbage
- Red garbage

- Blue robot
- Red Robot

- UAV

The JBotSim Library (Arnaud Casteigts)

http://muse.labri.fr/ and http://jbotsim.sourceforge.net/

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

- Scenario 3: **<u>information sharing in multi-convoys of heterogenous swarms</u>**
  - funded by the French Army (DGA)
    - one postdoc hired at Bordeaux and located at USMA West Point
  - funded by ONRG and ARL
    - one postdoc in Bordeaux (open position !)

Serge Chaumette, LaBRI, University of Bordeaux – serge.chaumette@labri.fr – 2013

Summary

- High level security
  - Authentication, Non repudiation,
  - Prevention against attacks (man in the middle, etc.)
- Distributed approaches
  - No central authority
  - Degraded modes of operation
  - Unsecure boundaries
- Reconfiguration (FPGA)