Communication Networks for Critical Infrastructures - topics under research at INESC Porto

Manuel Ricardo
DEEC, Faculdade de Engenharia, Universidade do Porto
mricardo@fe.up.pt
Outline

• What is it?

“Sistemas ciber-físicos para inteligência ambiente: redes de sensores em infra-estruturas críticas”

• Related research topics @ INESC Porto
Critical infrastructure

- Critical infrastructure – term used by governments to describe assets essential for functioning of society/economy

- Infrastructures commonly associated with the term
  - electricity, gas, oil
  - telecommunications
  - water
  - agriculture, food
  - public health
  - transportation
  - financial services
  - security services
Ambient Intelligence

• Embedding intelligence in everyday objects

• Object gains the ability to
  – Gather information from its environment
    possibly react by adapting its function
  – Process information
  – Exchange information with neighbour objects or Internet
The Intelligent Object

- Computers are becoming small

- Common object becoming also a computer
Ambient Intelligence in Critical Infrastructures

- *Objects* of critical infrastructures will become computers
- New objects (criticality related) will be added to infrastructure
- As a result, critical infrastructures expected to become efficient, reliable, secure
The Challenges of Interconnecting Objects

- Thousands of computing-objects to be interconnected through wireless, auto-configurable, high-bitrate, secure networks

- Research-topics@INESCPorto
  - Scalable auto-configurable networks
  - Intermittent connectivity / mobility
  - Enabling high bitrates
  - Network congestion control
  - Information aware networks
  - Moving PAN
  - Secure Networks

© 2008 INESC Porto
Telecommunications and Multimedia Unit
Scalable and Auto-Configurable Networks

- Plug & play network
  - Ethernet like network
  - Big network = big LAN
- Some network services
  - DHCP, ARP, IPv6 link local
  - Routing protocols
  - Generate broadcast traffic
  
Network becomes congested

- Research@INESCPorto
  - Re-design network services to avoid broadcast traffic
    Using prune + data suppression/compression techniques
  - Design large virtual Ethernet networks over existing technologies
Intermittent Connectivity and Mobility in Large Networks

- Global frequent routing update leads to excessive overhead
- Ad-hoc routing protocols are inadequate for large networks
- Research@INESCPorto
  - New routing techniques for wireless and mobile networks
  - New/lost links reported only to relevant nodes
Enabling High Bitrates - Directional Antenna

• Bitrate of a wireless link depends on
  Bandwidth, Rx power, SINR

• Directional antenna enables
  - More received power /longer links
  - Less interference
  - More links

• Research@INESCPorto
  - What criteria use to form beams?
  - How to combine
    • on demand-links and routing techniques?
    • beams with multichannel?
Enabling High Bitrates – Avoiding Hidden Nodes

- Wireless networks rely on CSMA/CA shared access mechanisms
- CSMA/CA performance depends on
  - Number of nodes
  - Number of hidden nodes

- Research@INESCPorto
  Network topology control
  - reduce number of hidden nodes for less collisions
  - dynamic selection of radio channels
Network Congestion Control

• Current congestion control mechanisms
  – inadequate for variable bitrate media
  – unfair for real-time/short traffic flows

• Research@INESCPorto
  – Use of explicit control techniques
    network nodes control the sources rate
  – Feedback signal considers
    nodes congestion and energy
  – Management of traffic priorities
Information Aware Networks

• Application and physical networks are different
e.g. P2P application over ad-hoc networks

• Research@INESCPorto
  – Define network paths based on
    • link quality, node energy
    • type of information
  – Network topology constrained by application
Moving Personal Area Networks

- Multi-technology PAN
  Intra/extra PAN connectivity

- Research@INESC Porto
  - PoA selected based on user-defined policies
  - Centralized single tree routing
  - Adaptive IP autoconfiguration
Secure Networks

- Networks need to be secure
  - Security between any pair of nodes

- Research@INESCPorto
  - Hierarchical distributed PKI
    - Ephemeral certificates
      - Used to authenticate a node
      - Short public keys → low processing power
      - No revocation lists → support of intermittent connectivity
  - Secure group communications
    - Authentication by certificates
    - Short symmetric keys
    - Key distribution using multicast techniques