Managing Ad hoc / Ubiquitous Environments

Prof. George Pavlou
Centre for Communications Systems Research
Department of Electronic Engineering
University of Surrey, UK

G.Pavlou@surrey.ac.uk
http://www.ee.surrey.ac.uk/CCSR/Networks/

Ad hoc / Ubiquitous Environments

- **Mobile Ad Hoc Networks (MANETs)**
  - **Self-creating, self-organising, self-administrating**
  - **Dynamic nature and lack of centralisation**
  - **Large scale, smaller devices => Ubiquitous environments**
- **Stand-alone or used as access networks for fixed or cellular packet networks**
  - **One or more devices act as gateways**
- **Fixed (ISP/enterprise) / cellular networks are managed by the owning body**
- **Who, why and how ad hoc / ubiquitous environments should be managed?**

Node Alignment / Programmability

- **Fixed / cellular network nodes and terminals have well-agreed protocol and service infrastructure**
- **In ad hoc / ubiquitous environments a multitude of solutions exist, e.g. for routing, QoS, services, hence the need for terminode alignment**
  - **Common protocols / services can be deployed throughout the network**
  - **Servers can be dynamically relocated for better performance / reachability**
- **Programmability essential for capability alignment**
  - **Also able to support "management by delegation"**

Context-based Operation

- **Context information can be used to drive the network to an optimal operating state given the current surroundings, user needs, etc.**
  - **Switching between a reactive (for highly dynamic topologies) and a proactive (for relatively static ones) routing protocol**
  - **Deploy energy-aware routing to conserve battery power**
  - **Relocate servers for better performance and energy efficiency**
  - **Identify paths of major traffic streams and adapt routing plans (dynamic traffic engineering)**
  - **…**
- **Context capture, modelling, aggregation, dissemination, adaptivity issues**

Fairness, Protection, Security

- All network nodes need to cooperate according to an accepted pre-defined set of rules
  - For example “all nodes should forward packets if their energy level >= 25%”
- Nodes may cheat / misbehave e.g. not forward
  - Need to detect, warn/penalise and eventually isolate them
- Other “spy” nodes may maliciously attack e.g. flood the network with bogus streams
  - Detect and isolate
- General security management issues
  - Who can be in the network, who has access to what, etc.

Management Models

- All nodes are owned by a single entity e.g. military applications, disaster recovery, etc.
- Logically centralised (in terms of goals/policies) but physically distributed management
  - No view of the whole network, management node resilience, etc.
- No single entity owns the nodes e.g. conference / meeting network, campus ad hoc network, etc.
- A set of goals/policies are “brought to the table” and prevailing ones need to be agreed
  - Through semantically rich interaction or simply by voting
- After the policies are agreed, the network is operated as a network owned by a single entity

Current and Future Research

- We have been doing research on most of the previous aspects:
  - Organisational management model (ICC'2004) and policy-based framework
  - Programmability for node alignment (IM'2005)
  - Context-based middleware (ICAC'2005, WAC'2005)
  - Misbehaving node identification and isolation
- A major operator interested in funding work in controlling ad hoc access clouds to cellular networks
- Many more issues to be addressed
- Fertile soil for defining the principles of the new wireless ubiquitous communication paradigm