Policy-based Management for ALAN-Enabled Networks

Ognjen Prnjat, Ioannis Liabotis, Tope Olukemi, Lionel Sacks
University College London, Dept. of Electronic and Electrical Eng.
http://www.ee.ucl.ac.uk/ACSE/

Mike Fisher, Paul McKee
BTexact Technologies

Ken Carlberg, Gregorio Martinez
University College London, Department of Computer Science
ANDROID

• Active Network Distributed Open Infrastructure Development
• EC funded - IST; 2 years
• BT, UCL, Netcelo, 6Wind, MediaSec, NTUA, UPM
• Policy-based, event driven management of ALAN enabled networks
Target networking architecture

- User
- Active server
- Active router
- Router
- IP network
- Proxylet
Management principles

• Policies
  – Specifying actions to be taken when events occur

• Events
  – Unidirectional messages communicating system changes

• Components needed
  – Policy/event handling at active nodes
  – Management information distribution (MID)
  – Persistent information storage
  – Specific management components
Policy schema

• XML schema
• Aims to embrace specific features common to all policies and events
• Flexibility
• Platform-neutral
Policy schema

• **Creator**
  – establishes origin of a policy (for multiple points of control)

• **Info**
  – not directly related to the policy rules
  – globally UI; modality; creation, start and expiry time

• **Sender**
  – identifies the forwarding path the policy has taken

• **Subject**
  – entities in the system which are expected to respond to a policy

• **Trigger**
  – relates an event (UI) to the policies that are supposed to handle it
  – triggerless policies can exist - executed straight away

• **Action**
  – behaviour that should result from triggering the policy
  – contains an optional condition expression and a set of strings specifying actions to be taken on particular target components
Event schema

- **Event-id**
  - globally unique string; same for same type of events
- **Time**
- **Time-to-live**
  - for how long event is relevant
- **Source**
- **Sequence**
  - integer incremented with each event produced from a source
- **Information**
- **Data**
  - open-content model containing XML
Policy control

- Management distribution and storage
- IP VPNs
- Resource and security management on active servers
- Current scenario: multicast conferencing groups established by Reflector proxylets. RM and SM.
- Future: IP VPNs established through collaboration of VPN Manager with Reflector proxylets. RM and SM.
MID

- Management Information Distribution
- Each site runs 1 MID server
- Internally events wrapped in XML notification
- MID policy controlled
  - policy linking each event type to a destination
- Event filters
VPN management

• VPN Manager
  – centralises access control of users to the VPN through policies
  – sends events to routers to configure VPN

• Policies defined via use-case and event analysis
Resource and security management on active servers

- RM and SM components
- Control access to the active server and its resources
- XML enabled
  - receiving and interpreting policies and events
  - generating events
- Resource and security management policies
  - defined and categorised based on use-cases and the events
  - given as combinations of events, conditions and actions
RM and SM

• Resource management:
  – Resources: CPU, storage, network interface
  – Monitoring and estimation
  – Allocation and reallocation

• Security management:
  – Deployer authentication
  – Proxylet authentication
  – Proxylet access control
<?xml version = "1.0" encoding = "UTF-8"?>
<policy>
  <creator>
    <authority>
      <admin-domain>AS</admin-domain>
      <role>AS Operator</role>
    </authority>
    <identity>ASOperator1</identity>
    <reply_address>ASOP@asl.org</reply_address>
  </creator>
  <info>
    <policy-id>Policy1</policy-id>
    <modality>obligation</modality>
  </info>
  <subject>
    <domain>
      <role>Resource-Manager</role>
    </domain>
  </subject>
</policy>
<trigger>
  <event-id>eLdPrx</event-id>
</trigger>
<actions>
  <condition>
    <operand>Total-CPU-Usage</operand>
    <operator>LessThan</operator>
    <operand>60%</operand>
  </condition>
  <action>
    <target>
      <domain>
        <role>EEP-Controller</role>
      </domain>
    </target>
    <data>
      <method>aLdPrx</method>
    </data>
  </action>
</actions>
</policy>
Demonstration

- Multimedia (whiteboard, video) conference between partner sites
- Established through Reflector/TAG proxylets + pseudo-manager
Conclusions

• ANDROID management architecture
• ALAN enabled networks
• Wide range of functionality policy-managed
• Trials in progress