Network Management in Scalable and Fault-Tolerant Mobile-Agent Systems

Dartmouth Workshop on Transportable Agents (DWTA)

October 6, 1999

Kenneth S. Vastola
The Networks Laboratory
Electrical, Computer, and Systems Eng'g. Dept.
Rensselaer Polytechnic Institute
Troy, New York 12180-3590
vastola@ecse.rpi.edu
http://networks.ecse.rpi.edu/~vastola/

Overview

- **What is Network Management?**
- **Simple Network Management Protocol (SNMP).**
- **Network Management: State of the Art / Open Questions.**
- **Network Management and Mobile Agents.**
- **Network Sensing.**
- **Network Sensing in Wireless Networks.**
- **Summary.**

What is Network Management?

- **What to do when networks don't operate as intended?**
- **Goal: Identify and solve network problems not handled by normal network functions such as routing, congestion control, or medium access control protocol.**
- **Examples of generic network management problems include**
  - **Faults.**
  - **Failures.**
  - **Performance problems.**
  - **Configuration changes.**
  - **Security violations.**

Why is Network Management hard?

- Very large networks
  - Can have > 1000 routers and 10,000 end nodes in one "enterprise network."
- Heterogeneous, multi-vendor networks.
- Multi-domain, multi-authority, e.g. RPI, ECSE, CS.
- Massive amounts of data
  - At every device (router, end node, printer, . . .).
  - At every layer.
  - At multiple time scales.
- Focuses on unusual events.

Simple Network Management Protocol (SNMP)

- **Introduced in RFC 1157 by J. Case, M. Schoffstall, et al.**
- **Updated to SNMPv2 in 1993.**
- **Components**
  - **Managed nodes, each running an SNMP Agent.**
  - **One (or more) management stations running an SNMP Manager.**
  - **Managed Objects (variables). The structured collection of all Managed Objects is called the Management Information Base (MIB).**
  - **A Manager–Agent communication protocol.**
- **MIB variables are represented vendor-neutrally using Abstract Syntax Notation One (ASN.1), an object description language.**
- **A MIB is organized as a directory tree with MIB variables at the leaves.**

SNMP MIB Variables

- **Example MIB Variables (From Interface Group)**
  - **ifIndex = id number of interface.**
  - **ifDescr = (manufacturer, product , version, . . .)**
  - **ifType = ethernet-csmacd or iso88023-csmacd or fddi or slip or basicISDN or . . .**
  - **ifPhysAddress = address below IP layer.**
  - **ifInOctect = total number of bytes received.**
  - **ifOutOctect = total number of bytes transmitted.**
  - **ifInUcastPkts = number of packets delivered to next higher layer.**
  - **ifInDiscards = number of packets discarded (e.g. due to no buffer space).**
  - **ifOutQLen = length of outbound packet queue.**

SNMP Communication

- A simple data base query language.
- Communication via a UDP socket.
- Communication primitives
  - GET: Get values of one or more variables.
  - SET: Set values of one or more variables.
  - INFORM: Manager to Manager communication.
  - TRAP: Problem report by Agent to Manager(s).
- Manager and Agent use UDP port 161 for GET, SET, and INFORM.
- Agent sends TRAP to port 162 on management station.

Network Management: State of the Art / Open Questions

- **State of the Art**
  - **Current network management is really <u>network monitoring</u> with human system administrator called to solve the problem.**
- **Open Questions**
  - **How do we analyze data and extract useful information?**
    - **"Diagnosis."**
    - **Currently done a little in simple proprietary systems (e.g. HP OpenView).**
  - **How do we automate the response to a diagnosis?**
    - **"Cure."**
    - **Current research.**
  - **We will touch on these topics later.**

Network Management and Mobile Agents

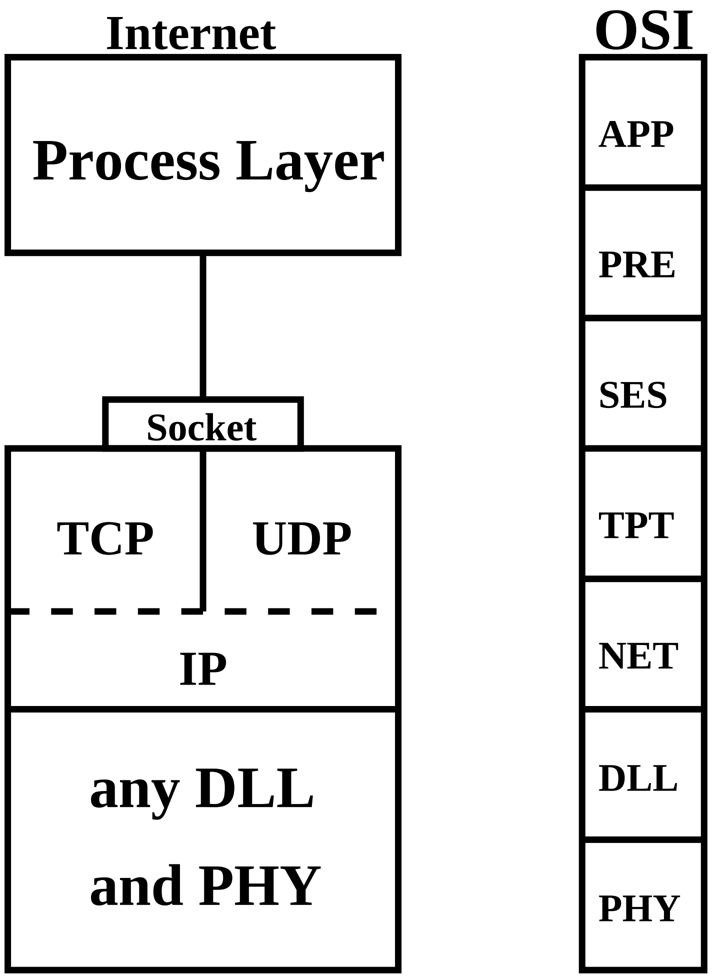
- **Could mobile agents be useful in network management?**
  - **Certainly!**
  - **Good topic for future research.**
- **Can we manage the network expressly to suit the needs of mobile agents?**
  - **No.**
  - **From network's point of view, mobile agents are just one more application.**
- **How can mobile agents get the most out of networks?**
  - **This is network sensing and analysis.**
  - **The main focus of the rest of this talk.**

Why Do Mobile Agents Want to Sense the Network?

- **Example: Agent Jump.**
- **How long will it take to jump?**
  - **Estimate link or path delay and available bandwidth.**
- **When should the agent jump?**
  - **Estimate link or path availability.**
- **In what order of nodes should the agent jump or bifurcate?**
  - **Estimate path availability when the agent gets there.**

Challenge in Network Sensing

- **Layered network architectures require separation of layers.**
- **Application layer programs (e.g. mobile agents) must get all information from the layer below.**



Network Sensing for Mobile Agents: The Do-It-Yourself Approach

- **Have agent system create its own data by probing the network, e.g. using something like "ping."**
- **Problems**
  - **Trying to sense each link and path will create large amounts of new network load.**
  - **Doing network analysis specifically for agents will waste processing resources.**
- **Conclusion: Any approach to network sensing specific to mobile agent systems will not be scalable.**

Network Sensing for Mobile Agents: The Generic Approach

- Create a generic network sensing system built on top of standardized network structures and information.
- Specifically, use SNMP MIB's for only data source.
- How do we use simple SNMP MIB's (e.g. byte counts, packet counts) to discern the state of network links?
- Build Network Sensing System on top of SNMP Manager.
- Innovative approach by Prof. Chuanyi Ji and her students at RPI uses intelligent agents which
  - Model "normal" network behavior.
  - Use deviation from the norm to indicate network ill-health.
  - Scale well by localizing data collection and processing.

Intelligent Agent to Detect Network Anomalies

- **Agent Structure**
  - 5 MIB variables used as input: ifInOct, ifOutOct, ipInRcv, ipInDel, ipOutReq.
  - Feature extraction using AR modeling.
  - Change detection using Generalized Likelihood Ratio produces anomaly probabilities for each MIB variable.
  - Linear combination of anomaly probabilities for each MIB variable produces overall network node anomaly probability.

- **Results so far**
  - Has detected several server faults on a University LAN and on a corporate enterprise network up to 5 minutes ahead.
  - Also detected a protocol error on the enterprise network.
  - Our current DARPA project combines this work with network control (e.g. routing, flow control) to try to solve anomaly.

Network Sensing for Mobile Agents in Wireless Networks

- **Wireless networks**
  - **Have much lower bandwidth.**
  - **Are much less reliable.**
  - **Have fewer traffic streams.**
- **Lisa Shay and I are**
  - **Enhancing Ji's agent to work in wireless networks.**
  - **Sensing link availability.**
  - **Supporting D'Agents as part of MURI project.**

Summary of Conclusions and Open Questions

- **True network management is still a wide open area for research.**
- **How do we diagnose network problems?**
- **How do we cure network problems?**
- **How can we use mobile agents as part of network management?**
- **How can mobile agents most effectively use networks?**