Challenged Networks
S-38.3155

Introduction

Jörg Ott  jo@netlab.tkk.fi  SE 324
Teemu Kärkkäinen  teemuk@netlab.tkk.fi  SE 328

Overview

- Seminar (3 ETCS points)
- Introductory lecture (today)
- Seminar presentations spread across two days
  - 30min Presentation and discussion per topic
  - One “opponent” per topic
- Overview and assignments: today
- Dates and venue: 27.02.2008, 16:00 (D302)
Requirements

- Seminar presentation
  - 30 minutes
  - Slides (digital: PS, PDF, or PPT)
    - Will be provided on the course web page after the seminar
  - Preparation meeting by individual appointment to discuss contents

- Written summary: 5 – 10 pages
  - Double column style of IEEE journal / conference proceedings
  - Should be sent one week prior to the seminar (13.02. and 20.02. respectively)
    - Also to the opponent
    - Will be published on the course web page

- Material
  - Material available on the course web page (mostly including links)
  - Complement by own literature research as needed (e.g. for some basics)

Examples for DTNs…
Classical IP Networking

Internet Design Philosophy

- **Military network**
  - Survivability: “Communication must continue despite loss of networks or gateways”

- **Hide transient failures completely from higher layers**
  - Route past disruptions
  - Only complete partition of the network will lead to application layer failure

- **Fate sharing**
  - State information maintained only at end points
  - Weak assumptions about the network’s ability to report that it has failed
Packet Switching

- Why the Internet is packet switched
  - Originally designed to connect packet switched networks (ARPANET, ARPA packet radio)
  - Applications were a natural fit for packet switching (e.g., remote login)
  - Packet switching was well understood from the experience with ARPANET

- Is packet switching the right abstraction?
  - It has proven highly successful in a world of fixed infrastructure.
  - Many problems in challenged networks.

The Internet Protocol

- IP (the protocol) makes very few assumptions
  - Lower layers can drop, re-order, corrupt or duplicate packets
  - No IP layer timers

- Some protocol issues exist (at least in theory)
  - TTL field: Originally a measure of time, now a hop-count
  - Identification field: Used to identify fragments

- Implementations make assumptions
  - End-to-end paths can be found
  - Topology is largely static
vegard@gyversalen:~$ ping -i 900 10.0.3.1
PING 10.0.3.1 (10.0.3.1): 56 data bytes
64 bytes from 10.0.3.1: icmp_seq=0 ttl=255 time=6165731.1 ms
64 bytes from 10.0.3.1: icmp_seq=4 ttl=255 time=3211900.8 ms
64 bytes from 10.0.3.1: icmp_seq=2 ttl=255 time=5124922.8 ms
64 bytes from 10.0.3.1: icmp_seq=1 ttl=255 time=6388671.9 ms

--- 10.0.3.1 ping statistics ---
9 packets transmitted, 4 packets received, 55% packet loss
round-trip min/avg/max = 3211900.8/5222806.6/6388671.9 ms
When TCP Breaks

- TCP underlies most of the applications we use every day

- Three way handshake (1.5RTT) before any data can flow
  - Assumes that RTTs are "low", i.e. in the order of milliseconds

- Flow control based on ACKs – Slow start, exponential back-off
  - Assumes that packet losses are rare (<2%) and are due to congestion
  - Assumes flow control in the order of RTT makes sense (again, "low" RTT)

- Generic 2 minute timer – Break the connection due to inactivity
Can We Fix It?

- Performance Enhancing Proxies (PEP)
  - Middle boxes that modify the data streams to hide problems.
  - Transport layer or application layer
  - Link specific – can’t be deployed securely in the global Internet
  - What happens to transparency? Security?

- Protocol Modifications
  - Change the assumptions (e.g. timer values)
  - Only changes the operating point

Abstractions...

- Simplification of a complex reality
  - We don’t start with Maxwell’s equations when writing networking software

- Based on making simplifying assumptions

- Network layering is a typical abstraction
  - Physical layer creates an illusion that we can transmit “bits”
  - TCP creates an illusion of a reliable transport over unreliable network
… Leak. Always.

- Leaks occur when the underlying reality shows through
  - Unexpected behavior that cannot be explained without understanding the underlying reality

- Result of the simplifying assumptions not holding
  - TCP slow start when RTT is in the order of seconds

- Patch the leak or come up with a new abstraction?
  - Patching with PEPs and protocol modifications will only take us so far.
  - The assumptions made by current Internet protocols simply do not hold;
  - New abstraction needed!
Revisiting Communication Paradigms

- Delays may be too long for interactive protocols
  - RTTs of minutes or hours or even days?
- An end-to-end path to a peer may never exist
  - At least not at the order of time IP routers and end systems operate
- Delay tolerance implies disruption tolerance
  - If a peer, a link, or a path is not available, just wait until it comes back
  - Store the “packets” in the meantime
  - Hand the data to someone else who may have better chances of delivery
  - Move (or have someone move) with the data towards the destination
- Use only asynchronous communications
  - Simply modeled after email
  - Store and forward: wait for the next suitable opportunity to send
  - Store, carry, and forward: add physical data carriage as communication option

Creating an Overlay

Contact:
any communication opportunity in the overlay
DTN RG Architecture (1)

- **Purpose**: asynchronously interconnecting different internetworks
  - Which may be based upon arbitrary underlying technologies
  - Which may encompass just a link layer technology or a complete protocol suite
  - Which may cross different administrative boundaries
  - Which may be used for different (presently unforeseen) applications with diverse requirements
  - Which cannot necessarily rely on an always accessible infrastructure

**Example**

![Diagram showing DTN RG Architecture](sensornet_dtnrg.png)

DTN RG Architecture (2)

- **Applications exchange** Application Data Units (ADUs)
  - Semantically meaningful pieces of information (=messages)

- **Bundle** as communication unit encapsulate ADUs
  - **Bundle layer** on top of underlying networks using **Bundle Protocol (BP)**

- Mapping to lower layers defined by “convergence layer”
Routing in Challenged Networks

Contacts

- In the Internet addressable entities are online all the time
  - Disruptions are treated as transient failures => time invariant cost

- In DTNs we expect communication to be possible only intermittently
  - Links have time varying delay and capacity => time varying cost

\[
\int c(t)dt = \text{Volume}
\]
Contact Types

- Persistent
  - DSL
- On-demand
  - Dial-up connection
- Scheduled
  - Deep-space applications
- Opportunistic
  - Ad-hoc connections
- Predicted
  - Based on past observations or other information

Space Paths vs. Space-Time Paths

© 2008 Jörg Ott & Teemu Kärkkäinen

Only for use with the TKK Netlab course S-38.3155 Challenged Networks
Challenges of Routing in DTNs

- The scope of applicability of the DTN architecture is very large
  - In deep-space missions topology and contacts are known ahead of time
  - In rural networks topology is known, but connectivity outages unpredictable
  - In mobile ad-hoc networks all contacts are opportunistic

- A single, grand routing algorithm might not be realistic
  - Need to understand the different classes of DTNs
    - Informal classification by Borrel, Ammar and Zegura [1]
    - Formal classification by Ramanathan, Baus and Krishnan [2]
  - Need to understand the different classes of routing approaches
    - Classification by Zhang [3]


Informal Network Classification

- Space-Path Network (SPN)
  - Space-paths exist between all the nodes
  - The typical “MANET” network

- Unassisted DTN (U-DTN)
  - Space-Time paths exist between all the nodes
  - The typical DTN network

- Assistance-needed DTN (A-DTN)
  - No paths exist between some nodes
  - Separated network islands, needs “assistance” to connect
Informal Network Classification

U-DTN

SPN

strict U-DTN

A-DTN

strict A-DTN

SPN = Space-Path Network
U-DTN = Unassisted DTN
A-DTN = Assistance-needed DTN

Classification of Routing Approaches

- Classification based on knowledge of schedule
  - Deterministic: Future topology and contacts well known in advance
    - e.g., deep-space networks
  - Stochastic: Future topology and contacts not known in advance
    - e.g., (sparse) mobile ad-hoc networks

- Formal classifications exist as well
  - Borrel, Ammar and Zegura
    - Routing centered network classification based on evolving graphs
  - Ramanathan, Baus and Krishnan
    - Classification based on three attributes: 1) end-to-end path required, 2) single copy (no replication), 3) unavailable schedule.
Routing Approaches

- **Deterministic**
  - Space time routing
  - Tree approach
  - Modified SPF

- **Stochastic**
  - Epidemic / Random Spray
  - Prediction-based
  - Model-based
  - Control movement
  - Coding-based

Network and Mobility Models

- Contact characteristics determines routing protocol design
  - Availability vs. unavailability
  - Permanent → regular/recurring → predictable → opportunistic
  - Degree, frequency and distribution
  - Mostly connected vs. mostly disconnected
  - Scale (nodes, node density)

- Contact characteristics are highly scenario-dependent
  - Space vs. desert vs. highway vs. downtown vs. Olympic stadium

- Approaches towards providing the basis for simulations
  - Synthetic generation of mobility: RW, RWP, map-based, group models, …
  - Reality mining: trace-driven from different scenarios
  - Understanding the characteristics of reality to create better models
Some Performance Metrics

- Contacts:
  - Inter-contact time, contact duration

- Message delivery
  - Message delivery rate (e.g., 70%)
  - Message propagation delay (e.g., hours to many days)
  - (C)CDF of rate over delay

- Protocol overhead
  - # message copies in the system (per sent message), buffer occupancy
  - # transmissions per sent message
  - # dropped messages
  - Fraction of control messages

Further Open Areas

- Security
- Reliability
- Congestion control
- Specific applications and meaningful deployment scenarios
- ...
### Topics

1. Routing I  
2. Routing II  
3. Routing III  
4. Performance Analysis  
5. Security (Frag Auth)  
6. Vehicular Networks  
7. Mobility Modeling I  
8. Mobility Modeling II  
9. Content Distribution  
10. Storage and Retrieval

Assignment to the two slots is somehow flexible.