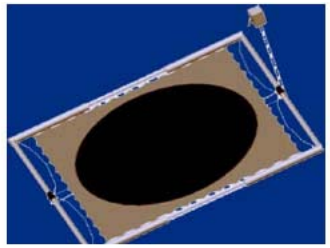
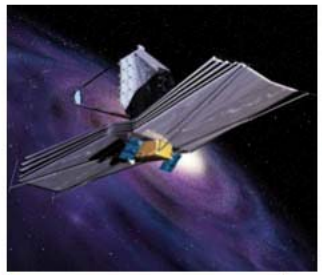
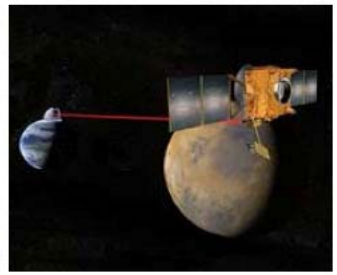
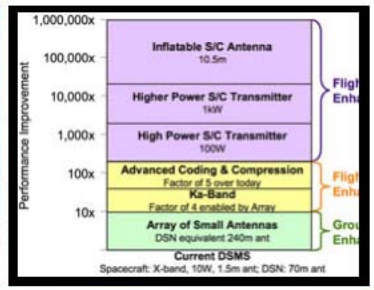
TTI Vanguard
27 April 2006

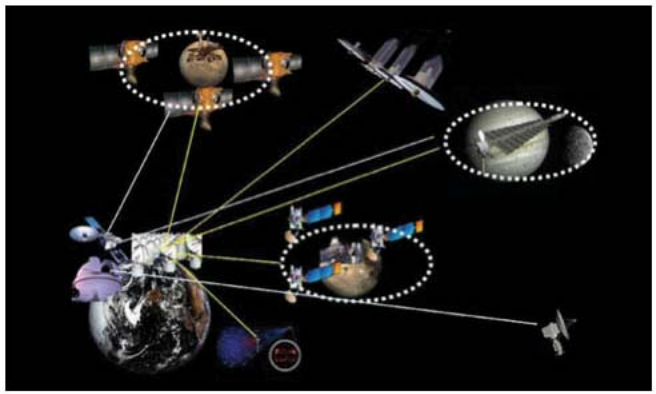
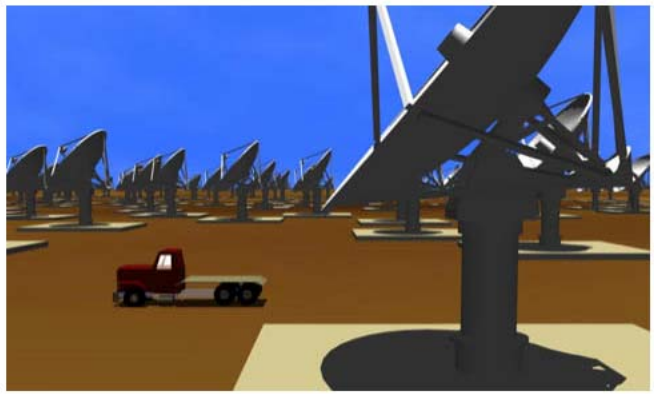
Resilience in Data Communications: Disruption-Tolerant Networking

Scott Burleigh
Jet Propulsion Laboratory
California Institute of Technology






from “Self Reliance”

Oh what is Heaven but the fellowship
Of minds that can each stand against the world
By its own meek and incorruptible will?

Ralph Waldo Emerson
1833

Delay-Tolerant Networking – an Overview

- **Motivation**
  - **Needed a way to operate a data communication network over interplanetary distances.**
  - **Internet protocols weren't the answer: intolerant of disruption in particular and delay in general.**
- **Strategy**
  - **Shift from telephonic communication model to postal model.**
- **Tactics**
  - **An overlay network architecture: use underlying protocols' capabilities as far as possible, then supply whatever is missing.**
  - **Deferred transmission: store as long as necessary, then forward.**
  - **Custody transfer: successful transmission is an achievement, so don't waste it.**

The Underlying Issues

- **Core obstacles:**
  - **Frequent, significant link interruptions (e.g., occultation).**
  - **High signal propagation latency.**
- **The central fact common to both:**

  No network node can be sure that it can obtain timely assistance from any other, for any purpose (route computation, congestion control, etc.), at any given moment.

- **Implications:**
  - **Nodes must be able to make their own operational decisions locally, on their own, with global information that may well be stale or incomplete. Helplessness is not an option.**
  - **The network – that is, all the other nodes – must be able to continue to operate at some useful level even when these decisions are flawed. Failure must be contained.**

Expressions of These Principles

- **Network control can't come just from the endpoints: each node must be able to act autonomously. Can't rely on assistance from neighbors.**
  - **Local route computation using best available data.**
  - **Local assumption of responsibility for reliable transmission.**
  - **Local buffering of data while awaiting forward connectivity.**
  - **Local triage of data whose usefulness has lapsed.**
- **Each router must defend itself against congestion, by refusing inbound data as necessary. Can't rely on simply telling data sources to slow down.**
  - **And each upstream router must respond constructively to refusal of data by a downstream router.**

Expression of These Principles (2)

- **Nodes need information in order to act autonomously. If they can't query for that information at the time they need it, they have to make do with whatever information they receive that they don't ask for.**
  - **So each unit of data transmission must contain enough metadata to enable the node to deal with it.**
  - **This "bundling" of metadata with application data is the origin of the name "Bundle Protocol".**

The Law of Demeter

- **As applied at JPL (e.g., Mars Pathfinder flight code):**

  A method shall act only upon the arguments and the pre-existing state of the object.

- **Translated from programmer lingo:**

  When required to do XYZ, the only information you've got to work with is what you already know, plus XYZ itself.

- **That is, you can't ask questions; all you can – and must – do is assert what you've decided.**
  - **Asynchronous (rather than synchronous) messaging.**
  - **Management by policy rather than by command.**
    - **Roman empire**
    - **Ships at sea**

Expression of These Principles (3)

- **Local fault recovery: no node can assume that any other node is operating correctly.**
  - **In fact, no thread of control in any node should assume that any other thread in any node is operating correctly.**
- **Local self-defense against attack: can't rely on effectiveness of admission control anywhere else.**
  - **If only "edge" nodes were suspicious, subversion of any edge node would expose the rest of the network to (for example) a denial-of-service attack.**
  - **Instead, reciprocal suspicion: any node might be subverted, so authenticate each bundle as received from any node.**
- **It's "defense in depth" – Maginot Line versus guerilla resistance.**

But Isn't Division of Labor Good?

- **Modern industrial economies thrive on specialization and interdependence. Coordinated application of complementary expertise benefits everyone.**
- **But modern industrial economies are possible only in relatively benign environments.**
  - **The benefit of specialization is productivity.**
  - **The cost is vulnerability to loss of the specialist.**
- **Specialization is limited even now.**
  - **Butchering and baking used to be skills that many people had. Now they are largely left to specialists.**
  - **But typing, using a telephone, driving a car, using a computer used to be skills left in the hands of specialists. Now most of us have them.**
- **You delegate to specialists when it makes sense.**

Summary

- **The DTN model: we all individually deal as best we can with whatever comes along.**
  - **It's the frontier. Every router is the little house on the prairie.**
- **It's not sufficient – nor even necessary – for routers to be a lot smarter about what they already do.**
- **It's necessary – and arguably sufficient – to deploy them in a structure that leverages the intelligence they already have.**

Bold Generalizations

- **Coordinated action within any system is always advantageous, but in hostile environments it's not always possible.**
- **Where coordination is not possible, the alternatives are:**
  - **Inaction, which typically results in failure.**
  - **Autonomous action, which (if policy is sound) results somewhat less often in failure.**
- **A resilient system is a fellowship of components that:**
  - **Coordinate meekly when they can.**
  - **Act autonomously – by incorruptible will – when they must.**