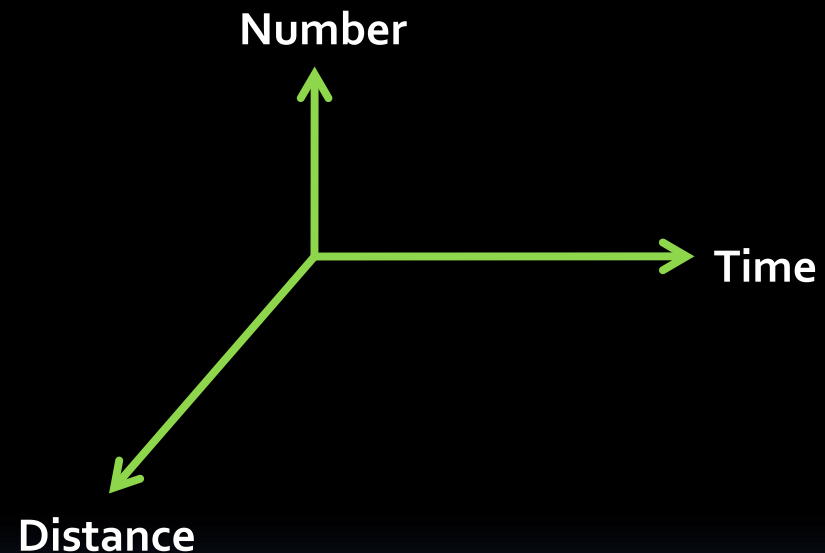


# ***DELAY / DISRUPTION TOLERANT NETWORKING***

*Axes of scale*



Dr. Keith Scott  
keithlscott@gmail.com

The views, opinions, and/or findings contained in this article/presentation are those of the author/presenter and should not be interpreted as representing the official views or policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the Department of Defense.



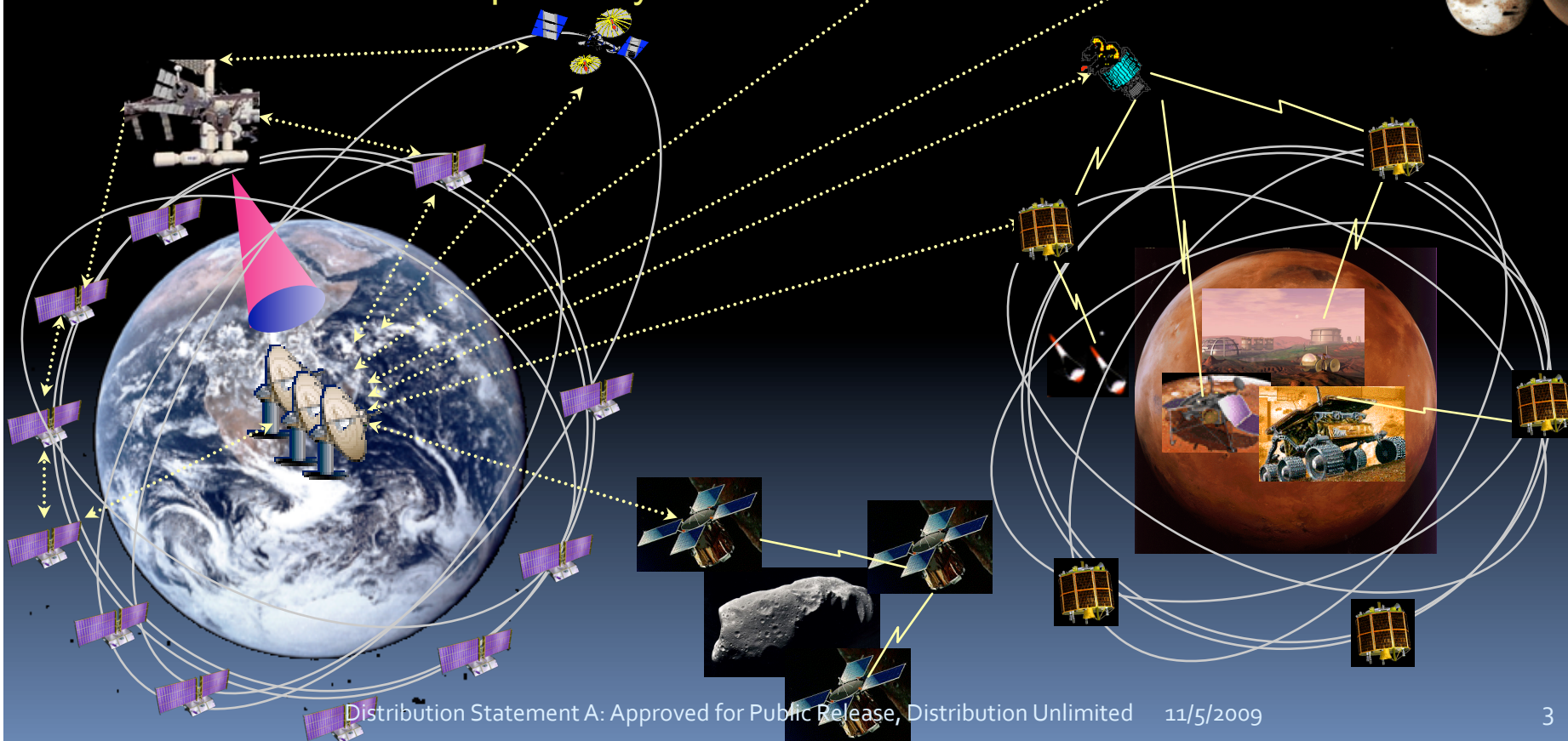
# Outline

- History and motivation
  - Interplanetary Internet
    - Large distances
    - Intermittent (but generally scheduled) and *expensive* connectivity
    - No end-to-end data path
- DTN Approach
  - Store-and-forward on (large) time scales
  - Naming and routing when DNS resolves take 10 minutes
  - Protocol mechanisms (including security)
  - DTN and content-based networking
- Future Directions
  - Large scale in terms of numbers
    - What if every access point were a MANET point-of-presence?

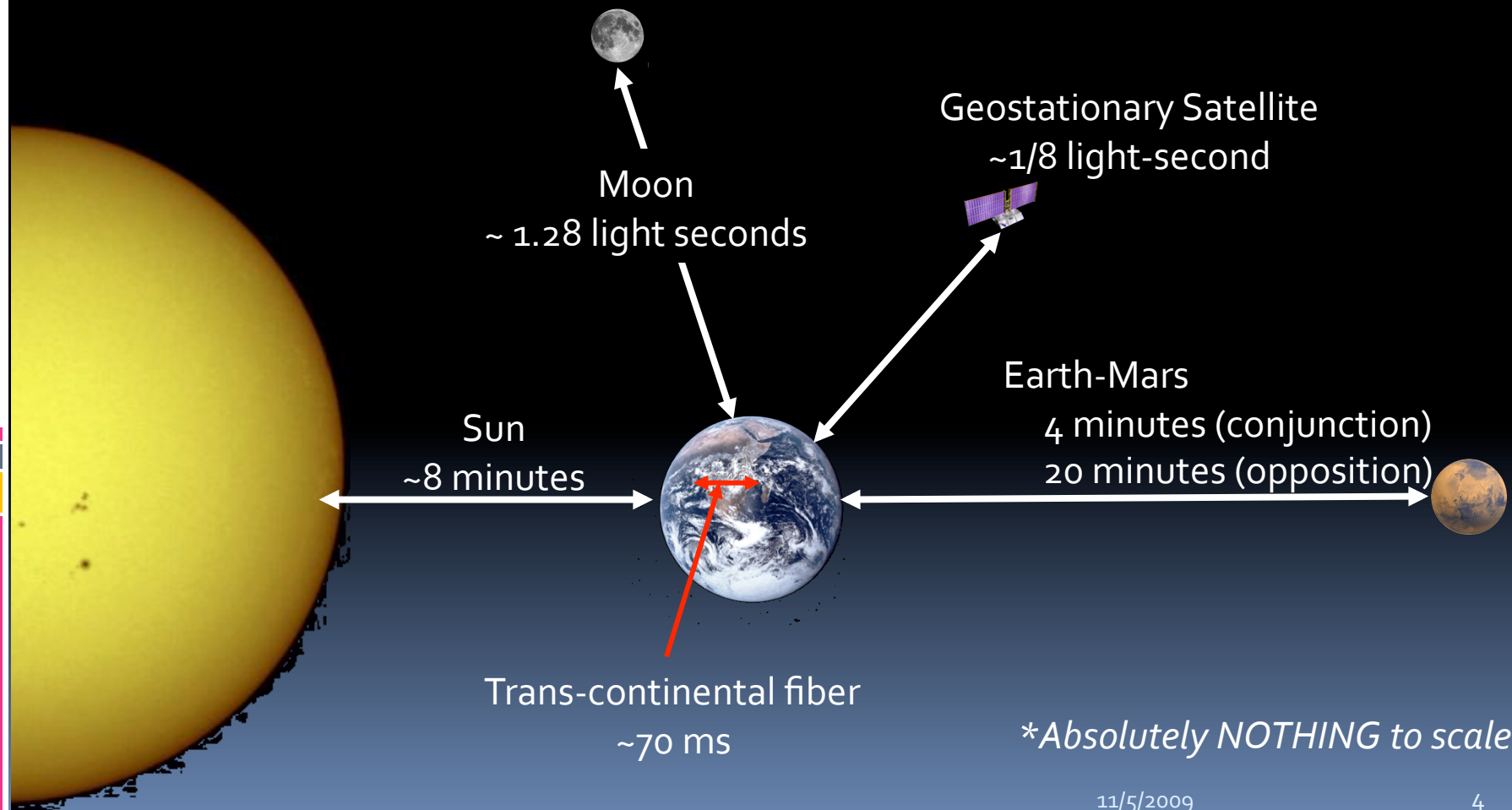


# Interplanetary Internet

- End-to-end information flow across the solar system
- “IP-like” protocol suite tailored to operate over long round trip light times
- Layered open architecture supports evolution and international interoperability



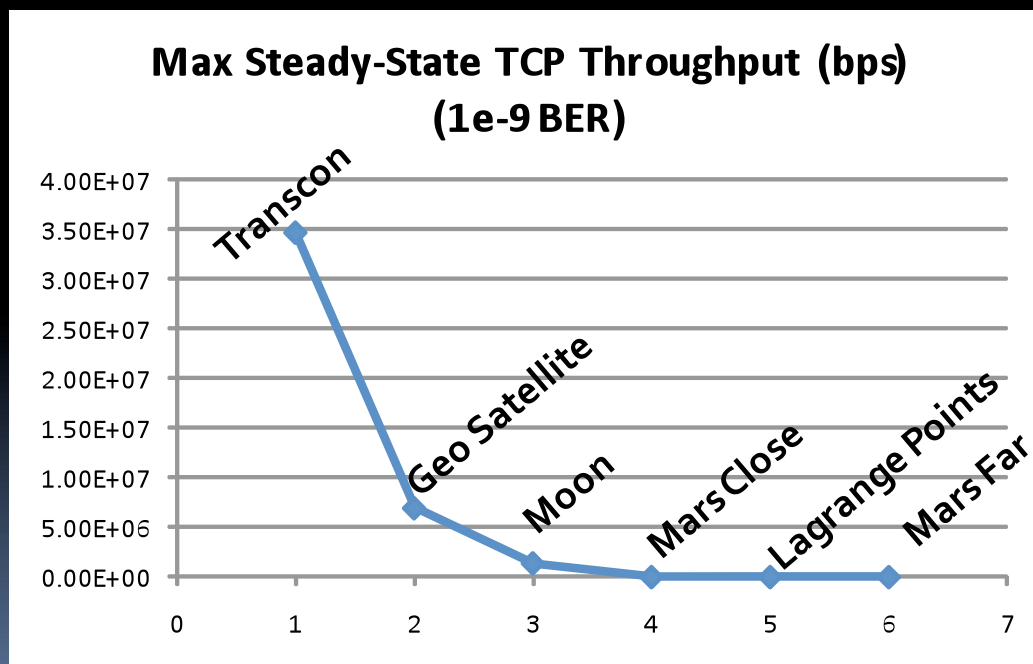
# Scaling in Distance: One-Way Light Times\*



*\*Absolutely NOTHING to scale*

# Delay Causes Disruption

- Stock TCP implementations fall off quickly with distance



$$BW < \left( \frac{MSS}{RTT} \right) \frac{1}{\sqrt{p}}$$

# Scaling in Time: Intermittent Connectivity

- Mars Exploration Rovers return ~98% of their data via orbiting relays
  - Orbiter – Lander connectivity
    - ~4 passes per day; 6 – 15 minutes per pass



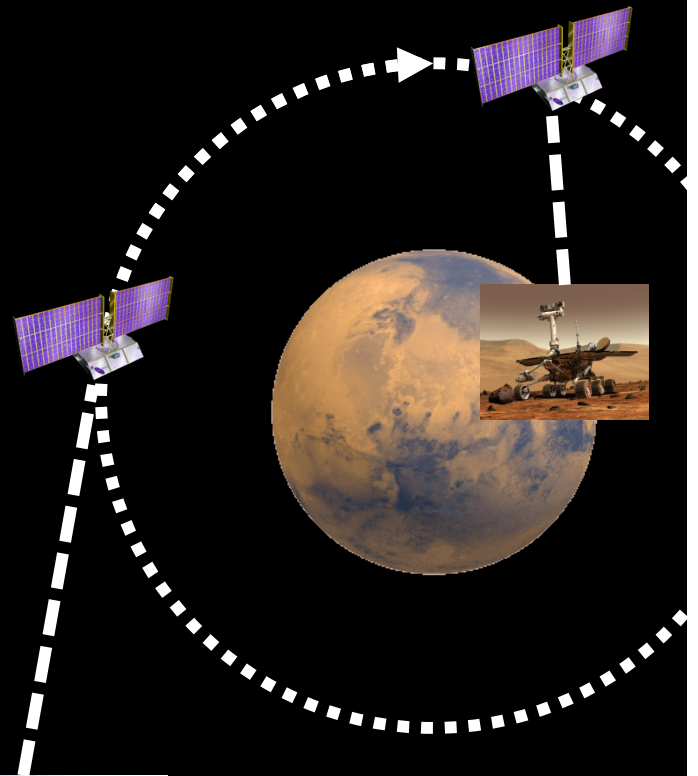
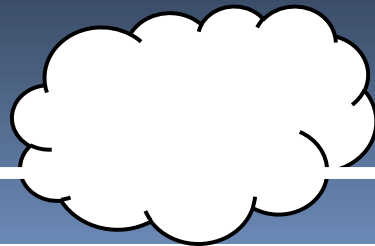
- Orbiter – Earth connectivity
  - 1 or 2 2-4 hour tracking passes per day




- No end-to-end connectivity
- Round-Trip time may be measured in HOURS

# Disruption Causes Delay

- Intermittent Connectivity + Store-and-Forward = Delay

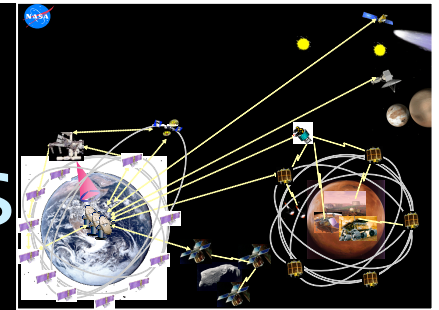




# Why Delay / Disruption Tolerance?

- There are a number of *inherent assumptions* in the Internet architecture and protocol implementations that break under long delays / intermittent connectivity:
  - There's always an end-to-end path
  - Round trips are cheap
  - Retransmissions from the source are a good way to provide reliability
  - End-to-end loss is relatively small
  - Endpoint-based security meets most security concerns
- Environments exhibiting some / all of these characteristics:
  - Space communications (high latencies, intermittent connectivity due to view periods / antenna schedules)
  - Sensor networks (nodes powered down much of the time to conserve energy)
  - Tactical communications (line-of-sight radios, intermittent SATCOM, urban/wooded environments, jamming, ...)
  - Mobile networks

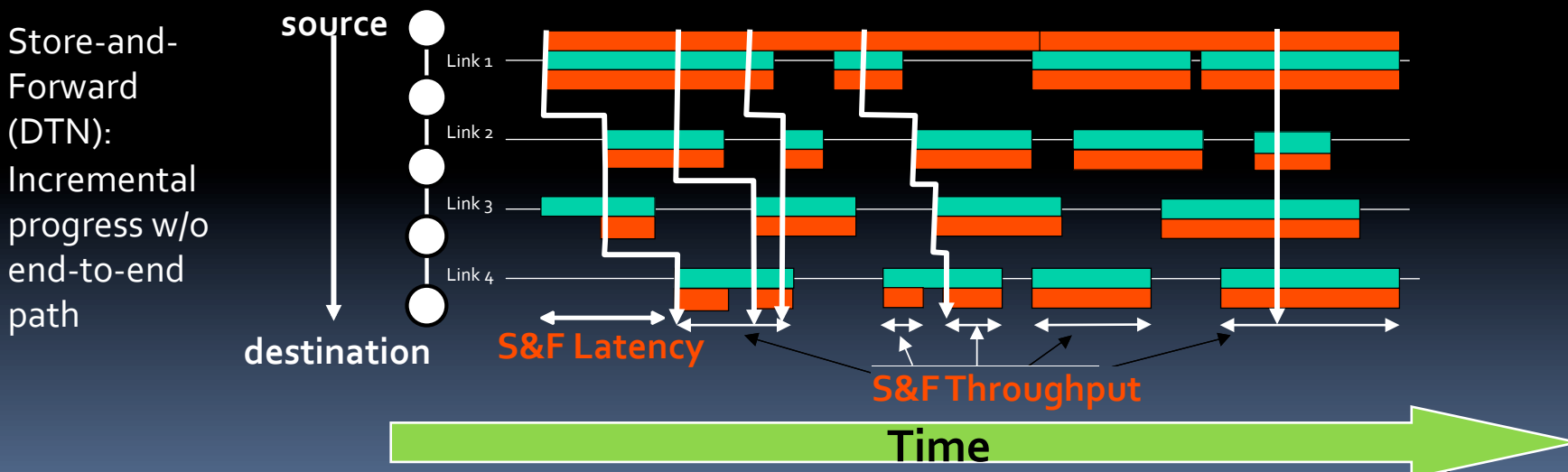
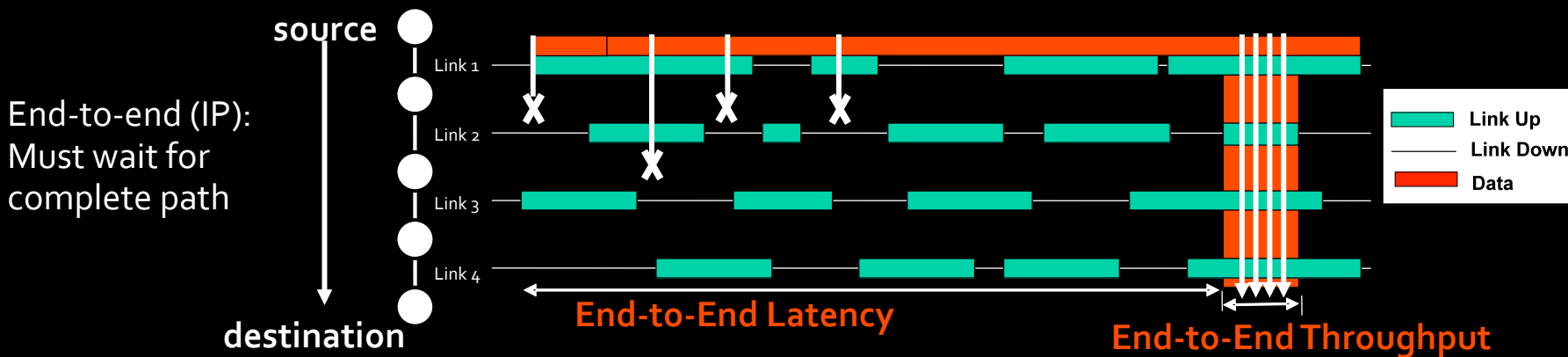




# First Round Conclusions

- Deploy “standard” internets in low latency environments
- Bridge high latency environments with an IPN Backbone
- Create gateways and relays to interface between low- and high-latency environments
- Construct a network of internets
  - Bundle Layer: A layer that bridges internets, providing end-to-endedness

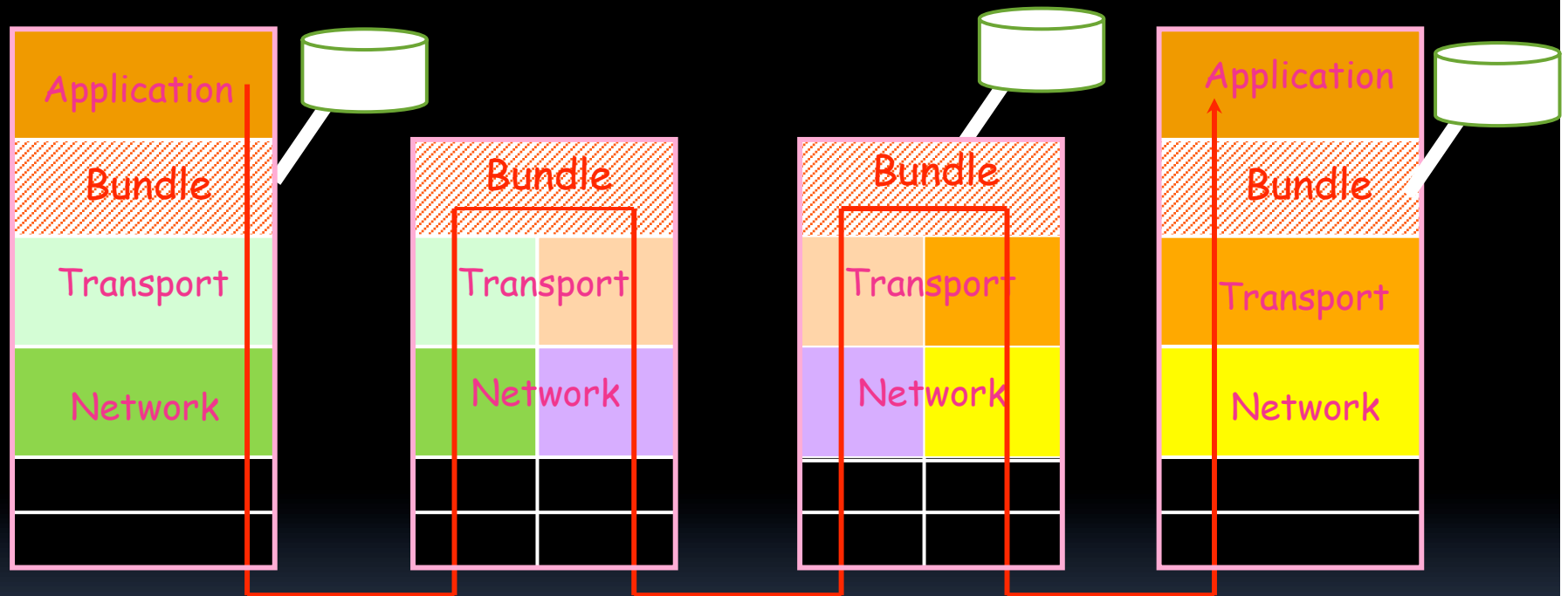
# Store-And-Forward Delivery



***DTN Can Reduce Delay and Increase Throughput***

# Bundle Space

Network of internets spanning dissimilar environments



Bundle space supports end-to-end transfer across IPN domains and/or heterogeneous network protocol stacks

# DTN's Derived Design Rules

- Don't plow the same ground twice – hold the gains you've achieved
- Don't engage in unnecessary chit-chat – build complete transactions and make network accesses count
- Don't depend on information from inaccessible / remote places if you can avoid it – build a sequence of local control operations and use late binding
- Don't force homogeneity – allow different network components to use environmentally-relevant optimizations

# Naming in the Bundle Protocol

- Bundle Protocol endpoints (applications) are identified by *name*
  - Intent was to allow *progressive binding* of names to actual nodes while a bundle is in transit
  - Derived from interplanetary internet notion of 'Regions'
    - "I don't know where [www.example.com](http://www.example.com) is, but it's on Earth, go that way." (but withOUT resolving to a destination IP address)
- Bundle Protocol names are URIs...

# BP Name Examples

- `dtn://mymachine/ping`
- `dtn://marsOrbiter8/instrument2/thermister4`
- `dtn://sensornet_mojave?tempValue>20c`
  - All sensors in the sensor network with current readings > 20 degrees c?
- `dtn://I495cars?speed<20mph`
  - All cars on I495?

# More BP Name Examples

- `dtm:flood:sql:batterylevel<0.25`
- `dtm:flood:sql:police_1000m_<LATLON>_haveKg`
- `dtm:pop:mailto:keithlscott@gmail.com`
  - Route the bundle until it makes sense to email it (as the content of a MIME attachment?)
- <http://tools.ietf.org/html/draft-irtf-dtnrg-dtm-uri-scheme-00>



# Routing

- IP routing builds a picture of what the network looks like *right now* and uses that picture to forward packets
  - Part of why mobility is an issue
- Because DTN can store bundles at intermediate nodes, it can route taking *time* into account
  - Route *this* way because there *will be* connectivity there later



# Routing in DTNs

- Ports of Internet routing protocols (Distance-Vector and Link-State)
  - Expedient, and can be extended to include some resilience to network partitioning
- Probabilistic routing
  - Usually applied to probabilistic nodes (e.g. zebras)
- Scheduled routing
  - Take advantage of a known schedule to route according to what the network *will* look like later
  - Spacecraft
  - Some aircraft
- Database-name, query-like support...?



# FAPH: DTN Enables OTM-to-OTM Comms and Reliably Delivers Data



Dynamic Routing Alone Can't Exploit Future Connections – DTN Enhances Dynamic Routing with Storage for Delivery over Disconnected Paths

## DTN Delivers:

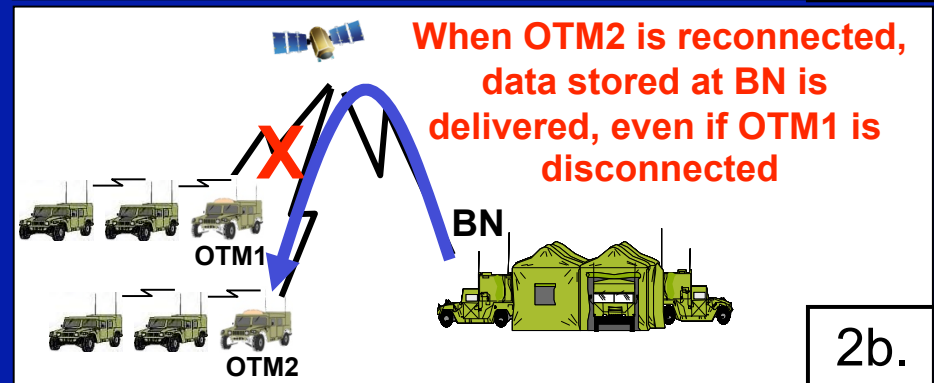
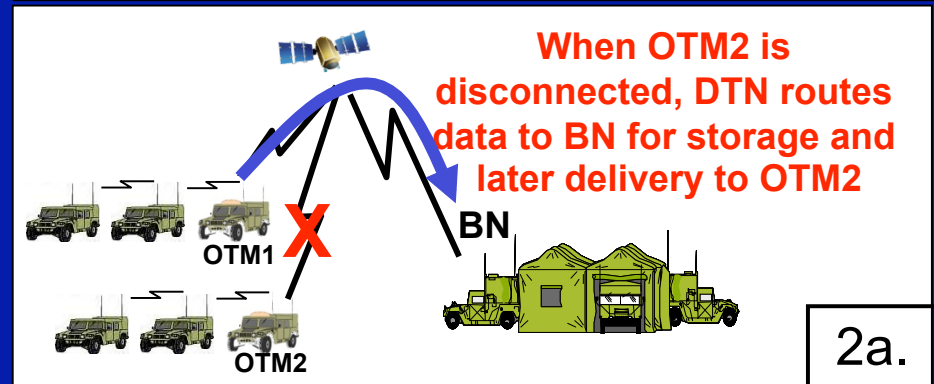
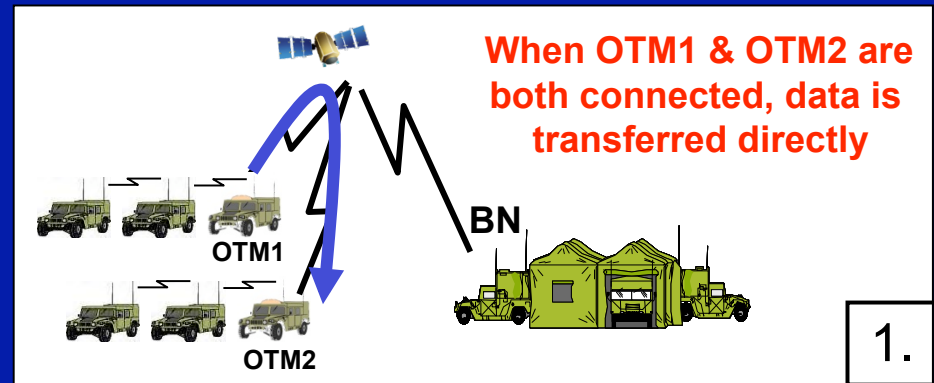
1. Along direct paths when they exist
- 2a. To advantaged nodes (custodians) when no direct path exists
- 2b. Custodians deliver data when destination becomes reachable

Original sender need not be connected to complete delivery!

DTN routing uses 'advantaged' locations (e.g. BN) for temporary data storage

Off-shortest-path storage makes reliable delivery possible

**DTN Routing & Storage Deliver All Messages that Live Across Link Outages**



# Protocol Mechanisms

- Bundles composed of collections of 'blocks'
- Per-bundle and per-block processing directives
  - Replicate block in each fragment
  - Discard bundle if can't process block
- Status reporting flags
  - Report on [receipt, custody, transmit]
  - Separate 'report-to' address

**Primary Bundle Block**

**Other Block (s)**

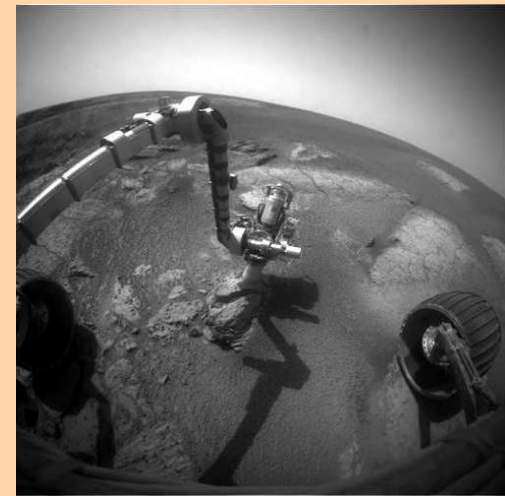
**Payload Block**

# Support for Content-Based Naming and Addressing

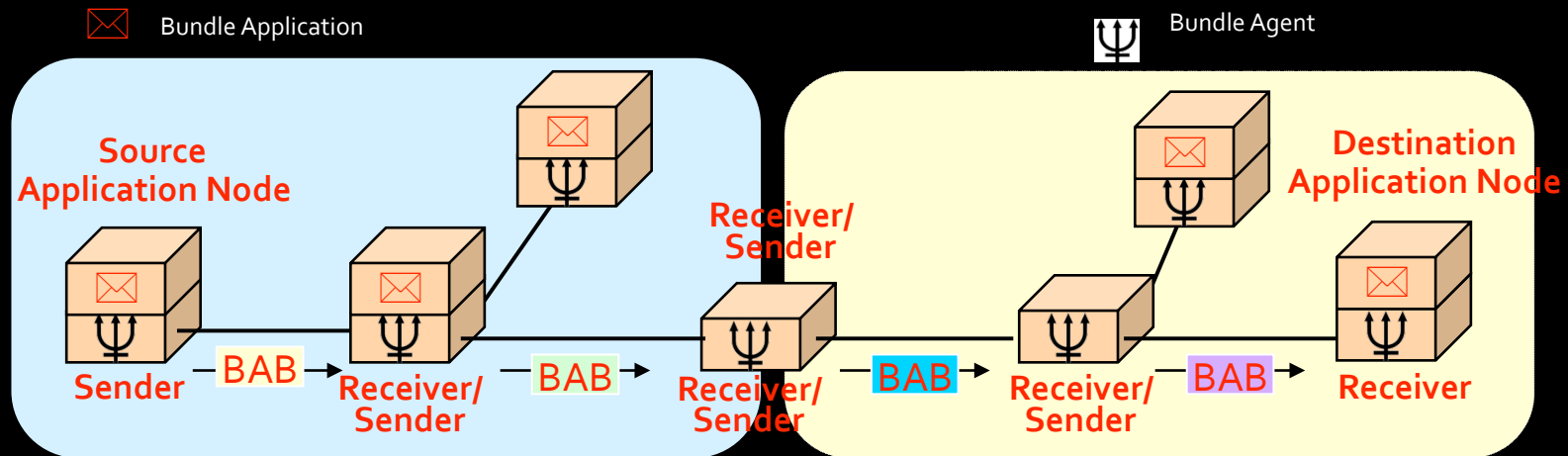
- URI-based naming
- Metadata blocks can identify content
  - Could be used to implement 'network as a database'
  - Can be encrypted separately from the payload
- Can serve as input to routing
  - Routing 'hints' so that every node doesn't have to do a full routing lookup

**Primary Bundle Block**

**Metadata: jpg image of rover arm**

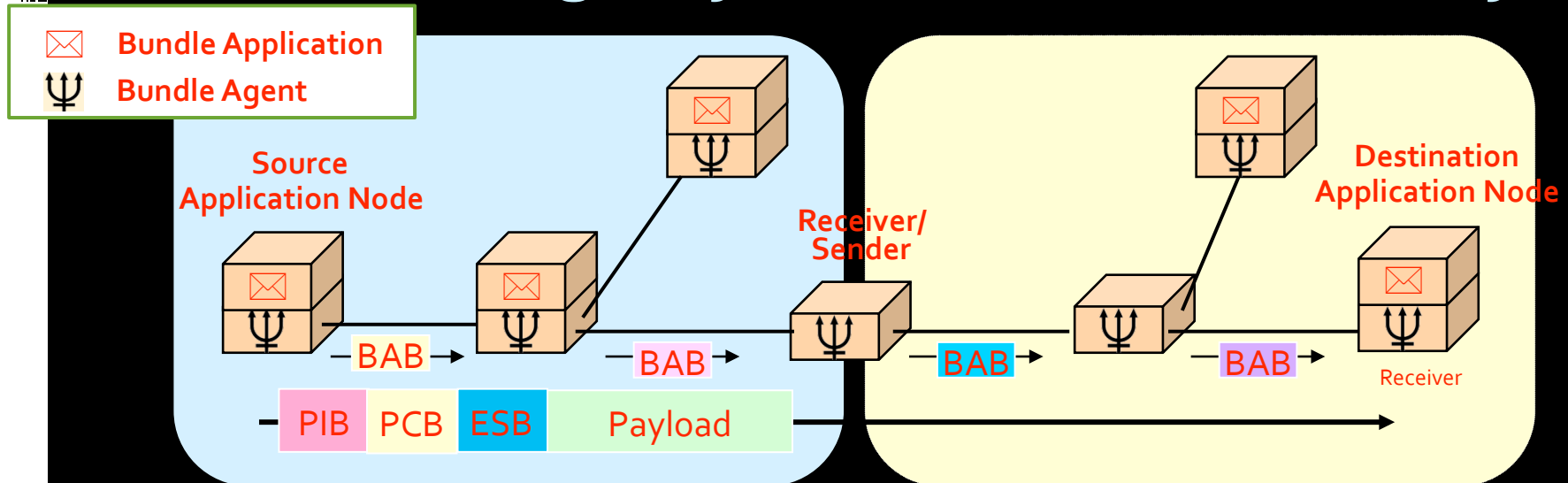


# Security: Prevent Unauthorized Resource Utilization



- **Bundle Authentication Block (BAB)** provides hop-by-hop authentication and integrity protection for the bundle between adjacent bundle nodes
- Protects against unauthorized use by enabling bogus or modified bundles to be detected and discarded at the first node at which they are received
- Each node needs only keys to interact with adjacent nodes
- Minimizes dependencies on a key server, which may be many hops away

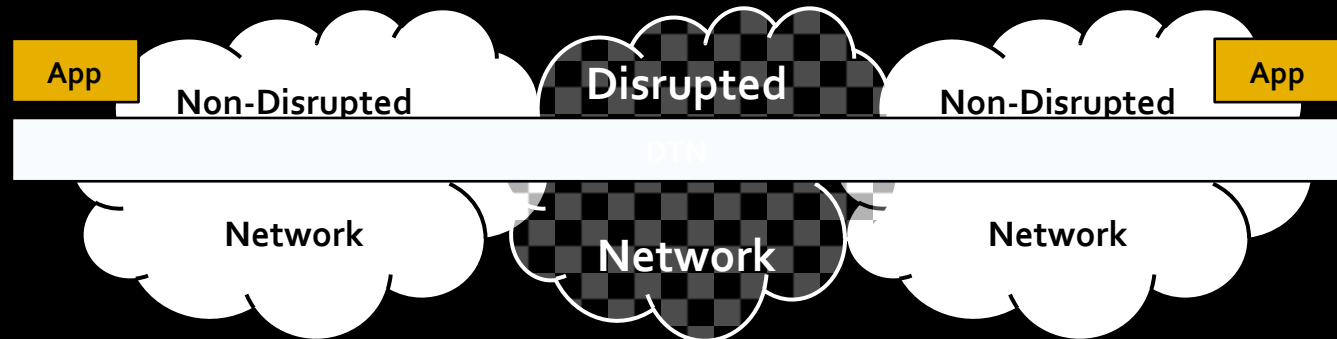
# “E2E” Integrity and Confidentiality



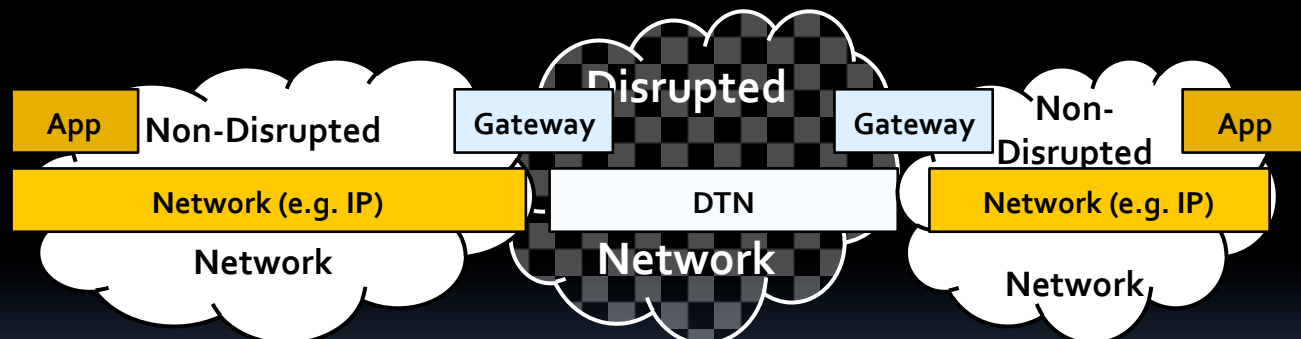
- **Payload Integrity Block (PIB)** provides “end-to-end” authentication and integrity on the non-mutable parts of the bundle between any source and destination nodes
- **Payload Confidentiality Block (PCB)** provides “end-to-end” encryption on the payload (and perhaps other parts of the bundle) between any source and destination nodes
- **Extension Security Block (ESB)** provides “end-to-end” encryption and integrity (depending on ciphersuite) of an extension block between any source and destination nodes

# Supporting Applications

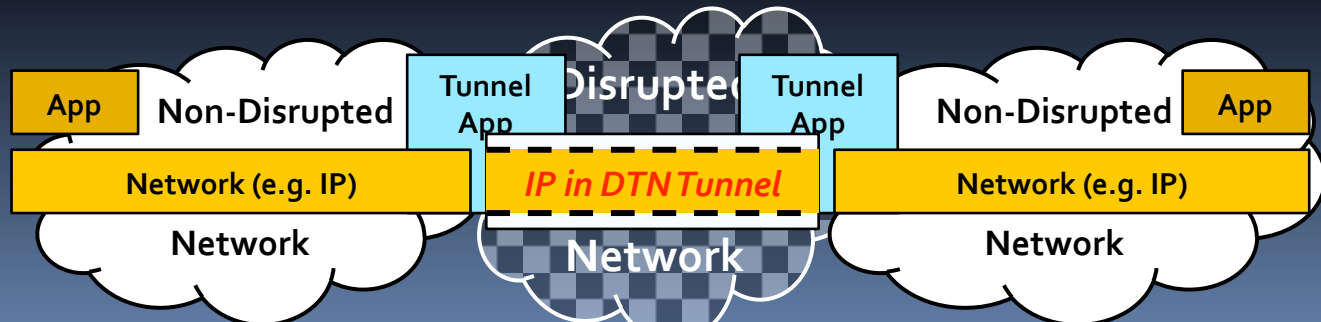
## 1. Native DTN Applications



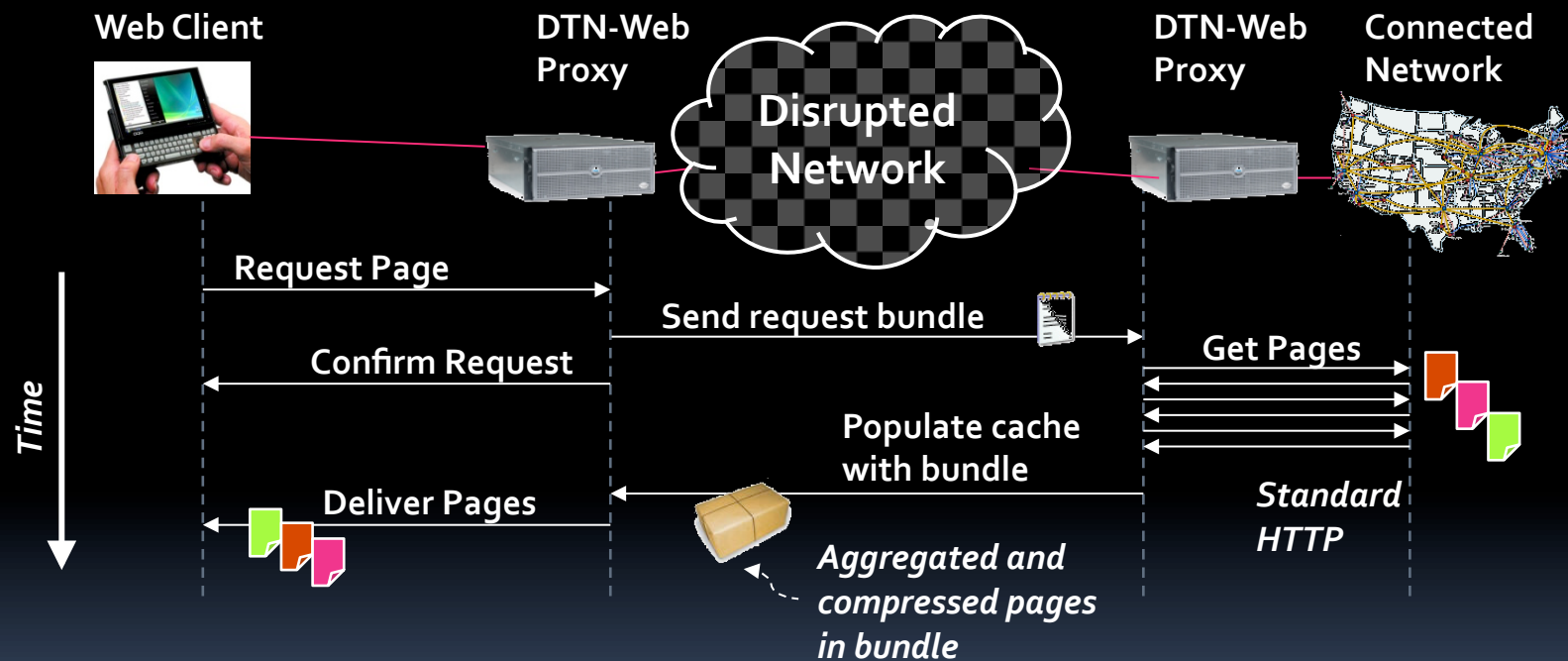
## 2. Application Layer Gateways



## 3. Tunnel Network Through DTN



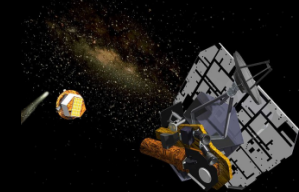
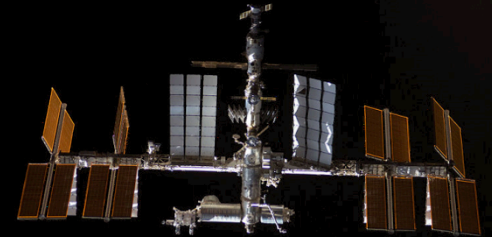
# Example: DTN-Web Proxy





# DTN Deployments

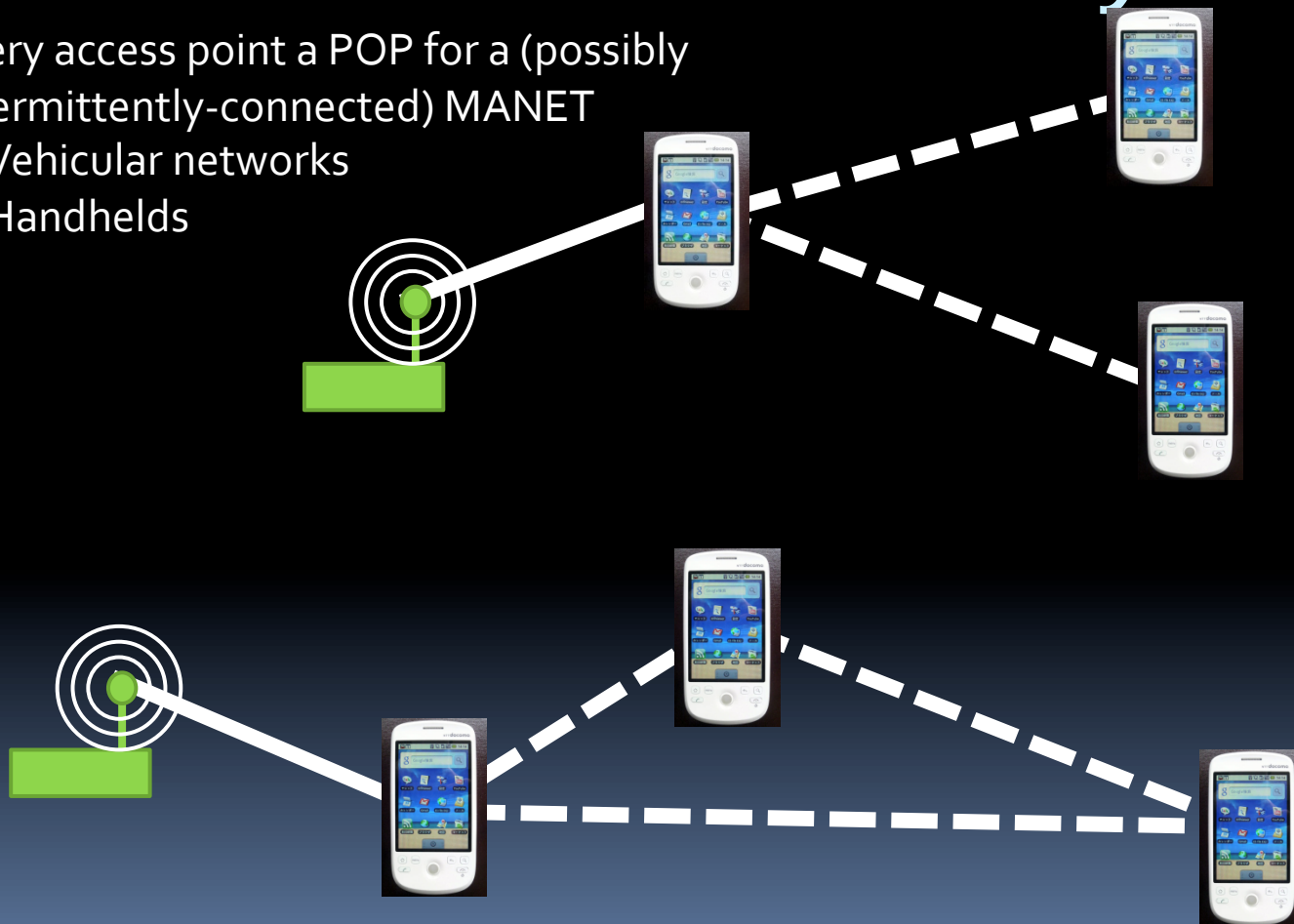
- NASA
  - Experiments on the International Space Station
  - Deep Impact Networking Flight Experiment
- University / Experimental
  - DieselNet
- Connectivity to 'disadvantaged' users
  - Sami community



# Scaling in Number: A Sea of Connectivity

Every access point a POP for a (possibly intermittently-connected) MANET

- Vehicular networks
- Handhelds





# Challenges to Scaling in Number

- Naming
  - How far can we push the URI-based name scheme? Can metadata 'hints' (or something else) extend that?
- Routing
  - Knowing how to appropriately address
    - Reachable now
    - Used to be reachable via this path but not there now
    - Scheduled to be reachable via some path in the future
- Connectivity
  - Difference between 'not connected now' and 'not coming back'
  - What can be served by the infrastructure and what can't?
- Culture
  - "Wait, MY phone is routing YOUR data?"



# Thanks

- DARPA
- DTNRG
- MITRE
- NASA