

# Disruption Tolerant Networking

**Robert C. Durst**

**703-983-7535 • [durst@mitre.org](mailto:durst@mitre.org)**

**DARPA Strategic Technology Office (STO)**



# Report Documentation Page

Form Approved  
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>MAY 2007</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2007 to 00-00-2007</b>	
4. TITLE AND SUBTITLE <b>Disruption Tolerant Networking</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Mitre Corporation, 202 Burlington Road, Bedford, MA, 01730-1420</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>Technology Symposium, 2-3 May 2007, Washington DC</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>10</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



# Project Data (internal use only)

- **Project Number: 0707D070-DT**
- **Ceiling Source: DARPA**
- **Principal Investigator: Robert C. Durst**
- **DARPA Office: STO**
- **Sponsor: Preston Marshall**
- **FY07 Funding Level: \$1.2M**
- **Technical Area: Comm and Networks**
- **External Web URL: [www.dtnrg.org](http://www.dtnrg.org)**

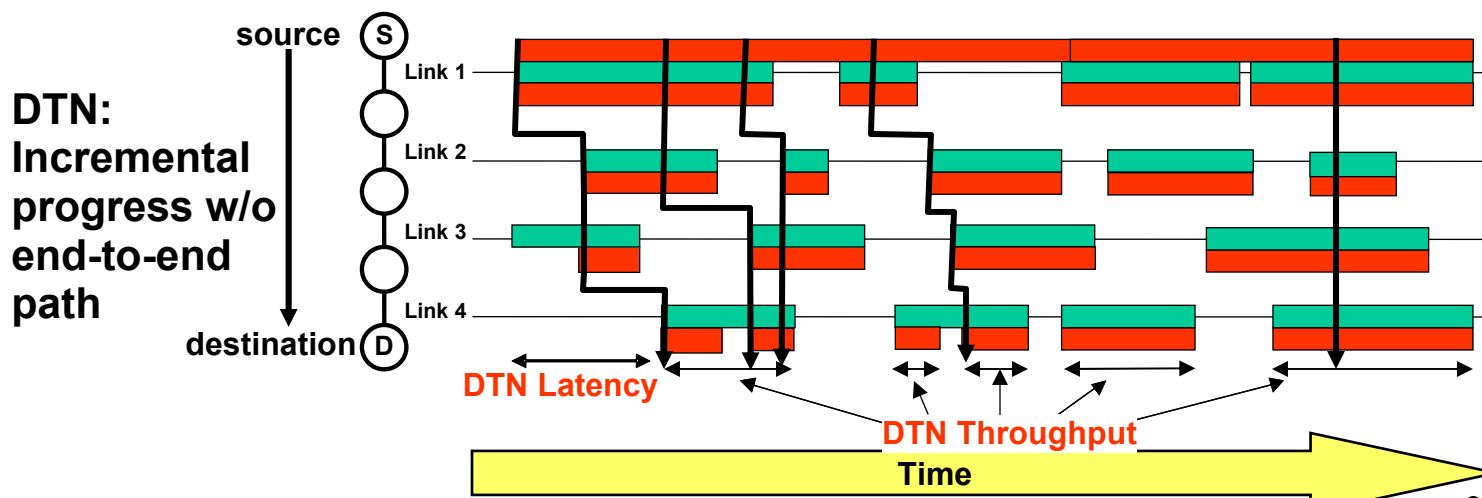
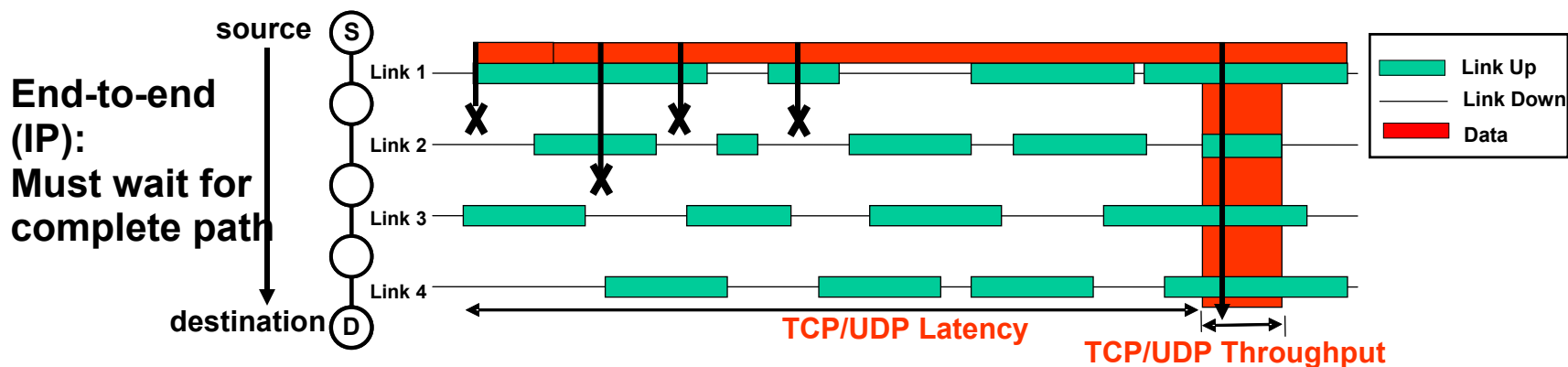


# Problem

- **Network-centric warfare depends heavily on Internet protocols**
  - **These work well with short delays, low error rates, and continuous connectivity**
  - **Military environments can have disrupted connectivity, long/variable delays, high error rates, extreme heterogeneity**
  
- **How to design a communications architecture that spans “connected” and “disrupted” environments, working well in both**



# Background



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



# Objective

- **Design a secure and robust Disruption Tolerant Networking (DTN) architecture and protocols to support networking in extreme environments**
- **Mature specifications toward RFC status**
- **Enhance protocols for military applications**
- **Foster early adoption by services**
- **Integrate with tactical systems and applications**

# Activities

## DTN Network Persistence Can Solve Fundamental Internet Application Shortfalls

Right information... Right place... Right time

- DTN makes applications over disrupted networks robust
- DTN is also an *Opportunity* to solve *Fundamental Problems* we've never before had a handle on, using *Network-Managed Persistence*
  - Access information by content or type rather than by network address
    - “I want maps for my area” instead of “I want to ftp to 192.168.4.17”
  - Retrieve once, provide to local users as requested
  - Learn from actual network usage
  - Exploit in-network storage/caches and pub/sub protocols to create a dynamic and self-forming “Akamai”
  - Use *temporal* security rather than *physical* security

### Integrated Push-Pull

• Good overall  
• Subsequent requests build “akamai”

### Resource Utilization

Subsequent requests for same data receive copies already cached in the network – only one copy of the data ever crosses any given link.

### Temporal Security Model

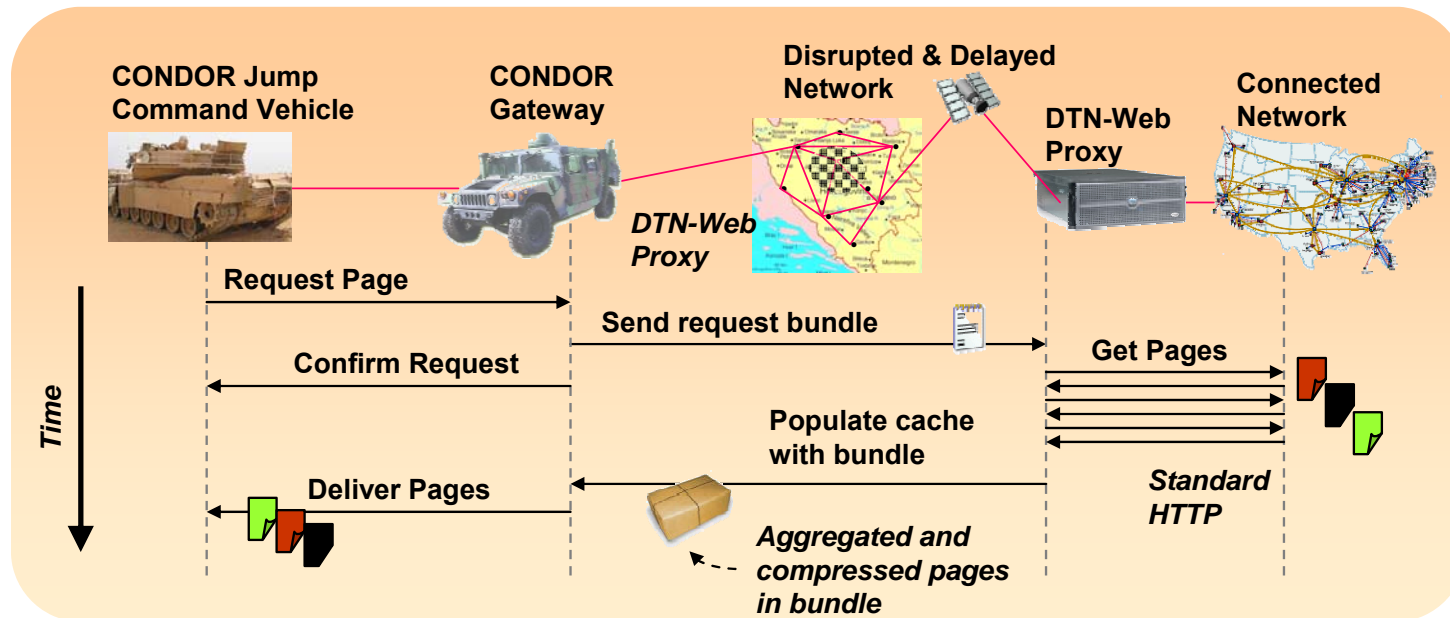
Distribution Statement: Approved for Public Release. Distribution Unlimited.

5

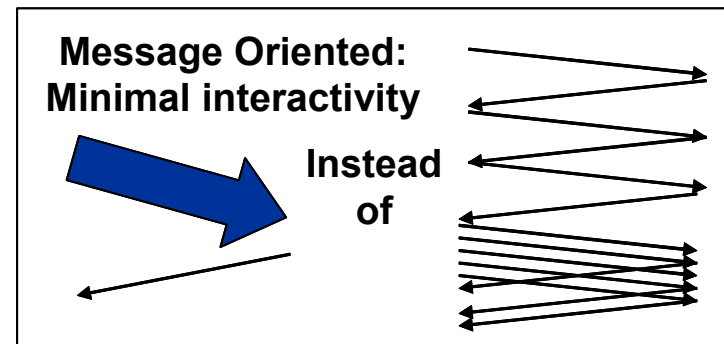
(Approved for Public Release, Distribution Unlimited)

© 2007, The MITRE Corporation

# Highlight: DTN-Web Proxy



- **Routing Across Network Disruption Using**
  - On-demand connections
  - Scheduled connections
  - Predicted connections
  - Opportunistic (unexpected) connections







# Impacts

- **Enable the vision for secure and reliable communications for “distributed ops”**
- **Provide support for *practical* mobile ad hoc networks in tactical environments**
- **Improve network and application performance in disrupted tactical environments**
  - **Higher throughput and utilization over challenged connections**
  - **Connectivity to lower echelons using tactical radios**



# Future Plans

