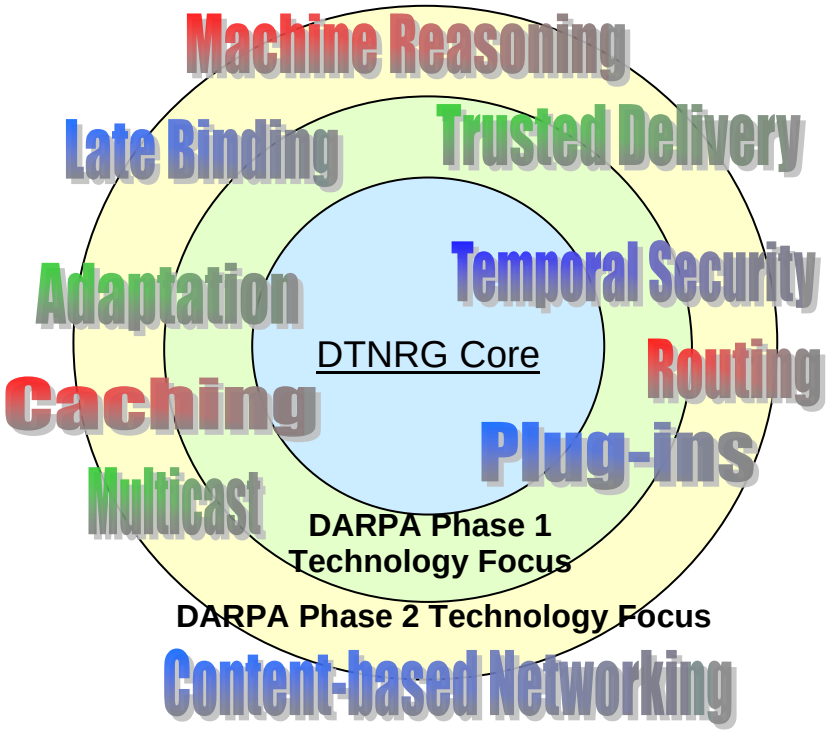
An Introduction to
DISRUPTION TOLERANT NETWORKING (DTN)
WAND Industry Day

27 February 2007

Approved for Public Release, Distribution Unlimited

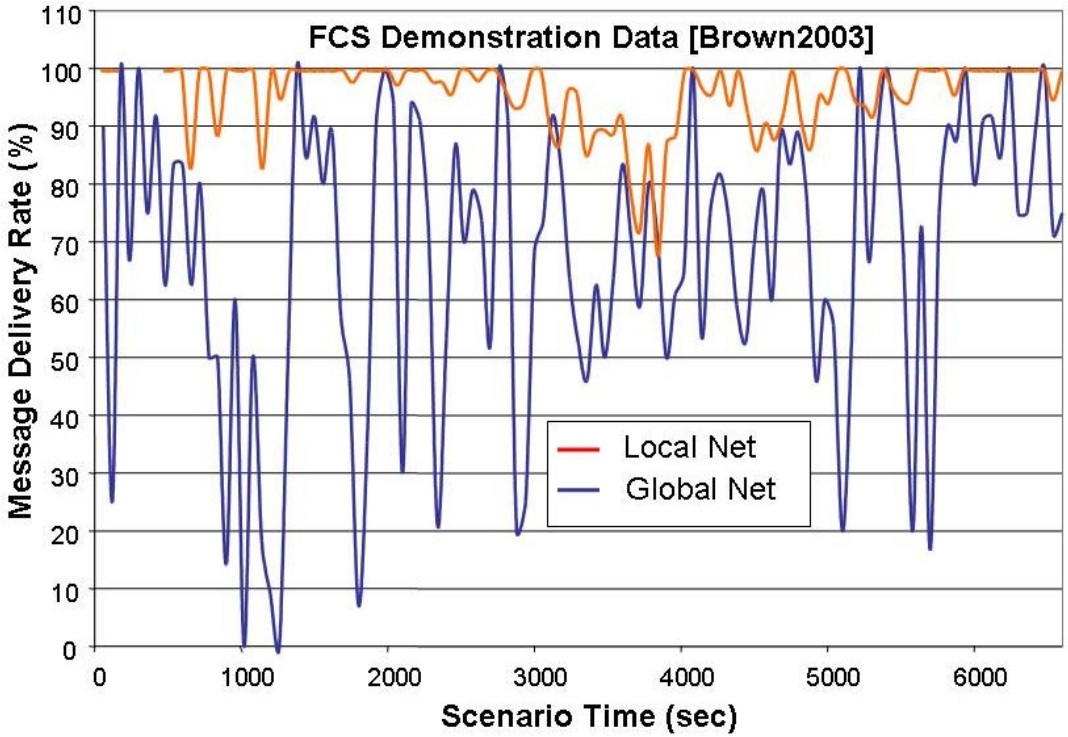
Outline

1. Motivation: Why not stock IP?
2. What is DTN? Building functionality out from a core set of functions
3. Performance: DTN v. stock IP
4. Developing COTS DTN gear that meets military needs
5. Current DTN Status
6. Caching and Content-Based Networking
7. DTN & Security
8. DTN Timelines



Approved for Public Release, Distribution Unlimited

Military Need: Why Not IP?



FCS Vehicle, Ft. Benning 2006

FCS Communications Position Reports Used as Measure

Highly Favorable Metric Used

Loss of 2 Successive (1 Sec Interval) Reports Considered as Disconnected

IP is unreliable in tactical military networks

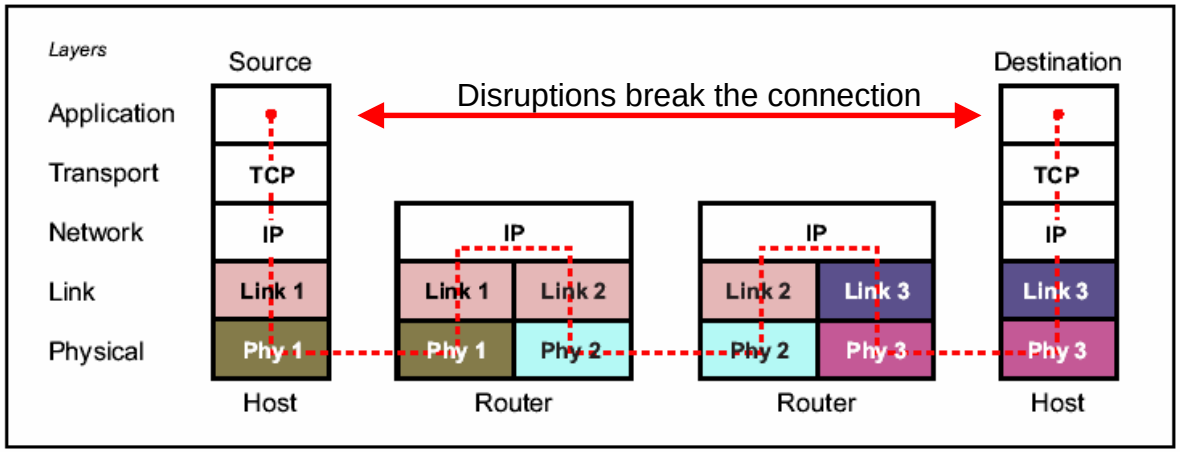
- **Dynamic military MANETs see rapid topology changes and episodic connectivity**
- **Tactical radio users know user names, roles, or frequencies, not IP addresses**
- **Tactical/edge military networks may be a mix of IP and non-IP radios – no general mechanism for IP apps to bridge heterogeneous networks**

Wireless networks tend to have usable local connectivity, but often can't reach back to infrastructure

Traffic in military tactical networks tends to be highly correlated, not gaussian as in the Internet

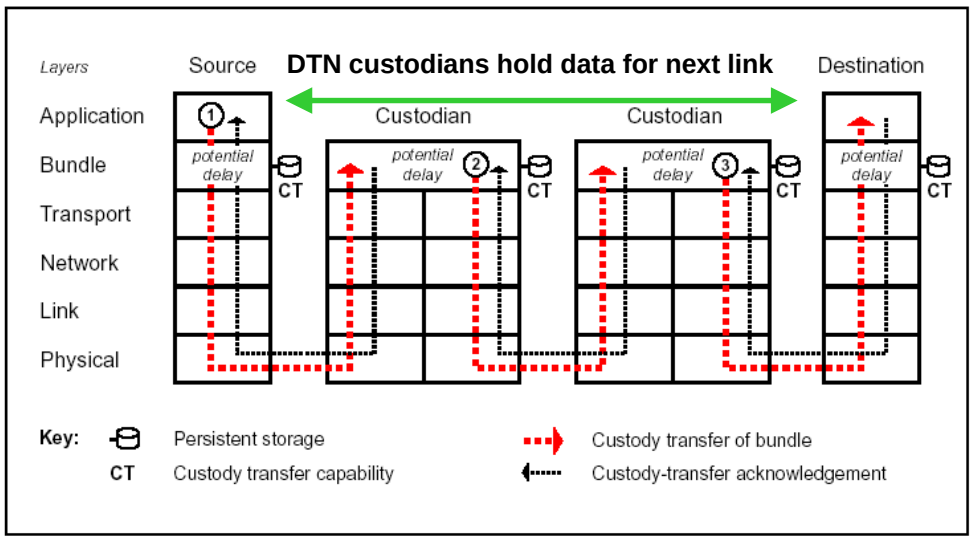
Approved for Public Release, Distribution Unlimited

IP Routing vs. DTN Delivery



IP (UDP or TCP) works only if there is IP continuity between nodes for duration of transfer (+ routing time)

DTN bridges IP and non-IP paths, & holds data during intervals when links along the path are not available



Approved for Public Release, Distribution Unlimited

DTN in a Nutshell

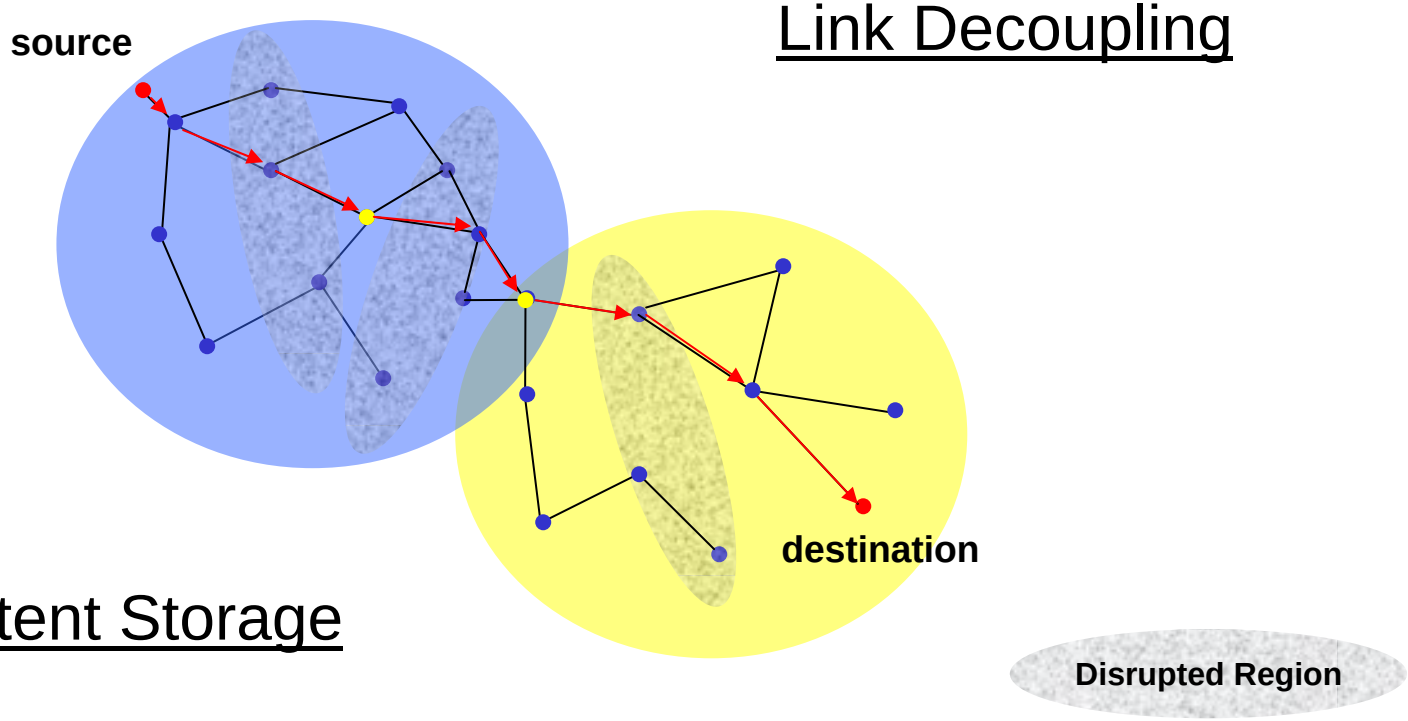
"Postal model" of Communications

Store and Forward, minimal interactivity

Link Decoupling

Routing

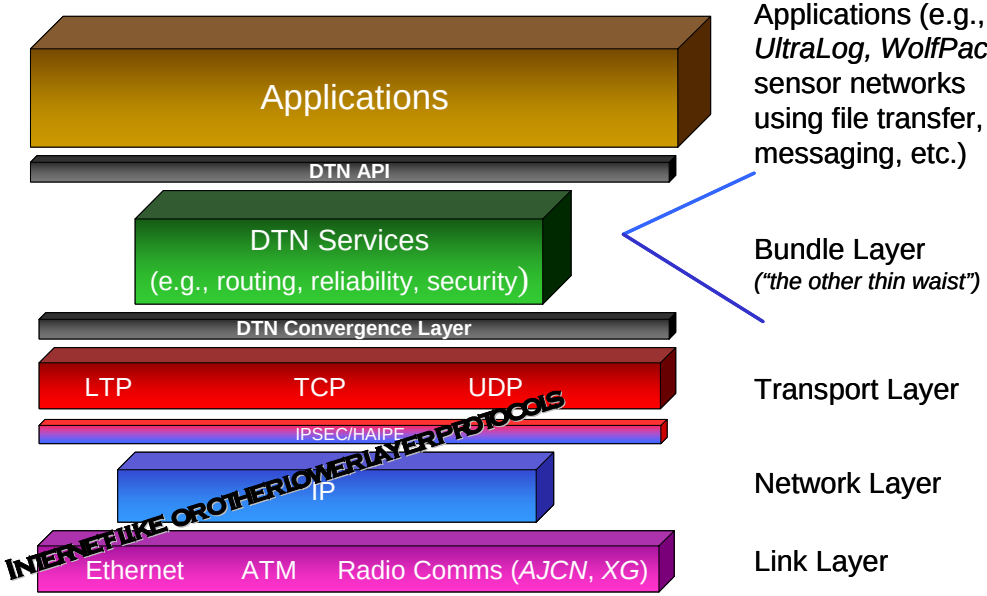
Persistent Storage



DTN provides network services across disruption and massive differences in delay and bandwidth

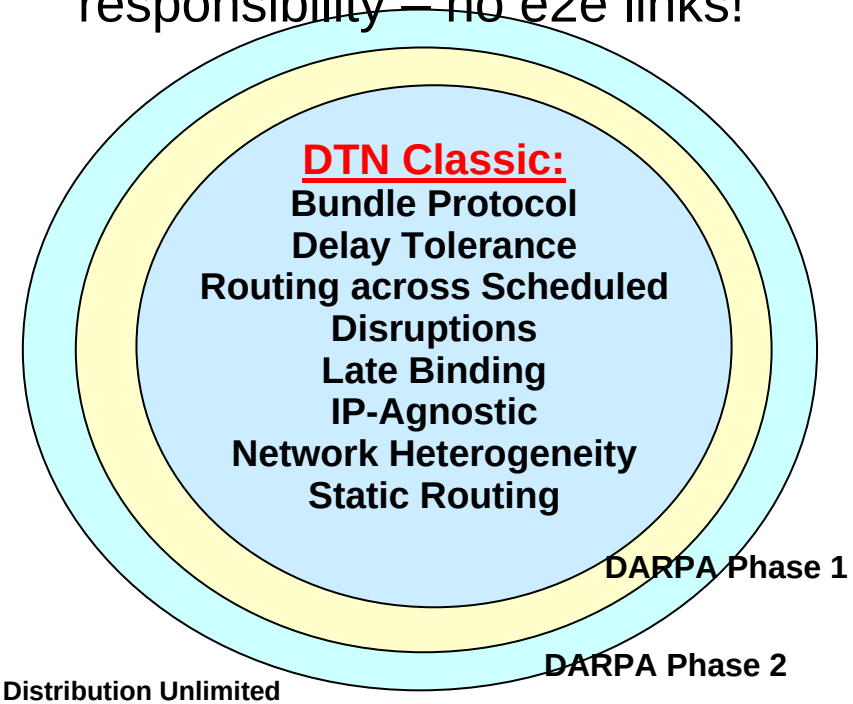
Approved for Public Release, Distribution Unlimited

DTN Network Stack



- Organize information flow into self-contained bundles
- Create intelligent networks that manage the flow of bundles thru the network
- Pass messages thru the network incrementally, with successive responsibility – no e2e links!

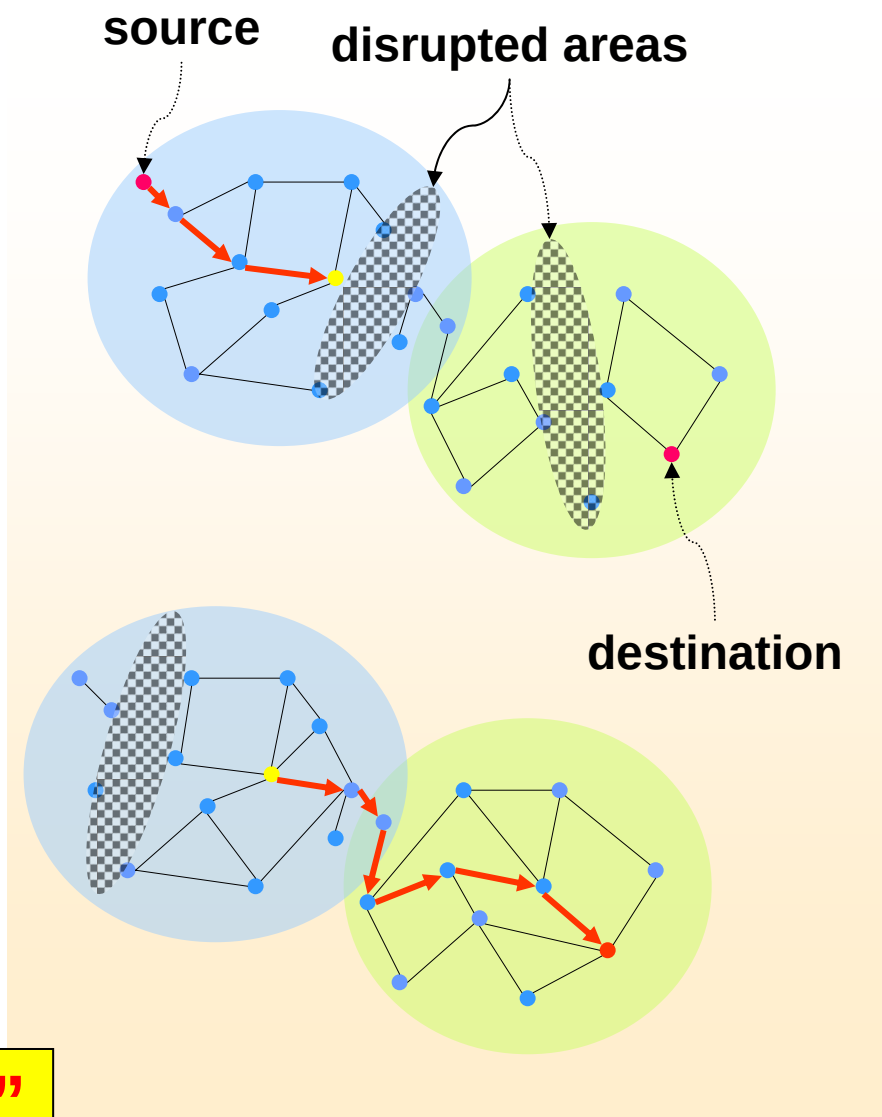
- Opportunistically leverage link availability, multiple routes..
- Agnostic to lower layers in the stack – use existing transport and network layers via shims, or interface to native link layer
- Bridges heterogeneous networks with common API



Approved for Public Release, Distribution Unlimited

DTN "Classic" Design Principles

- Maintain advances thru the network, advance messages incrementally – don't plow the same ground twice
- Minimize network chit-chat – build complete transactions to make best use of scarce link uptime – eg DNS
- Build a sequence of local control operations and use late binding – avoid dependence on remote information
- Take advantage of network hetero-geneity – allow different network components to use local technology and optimizations

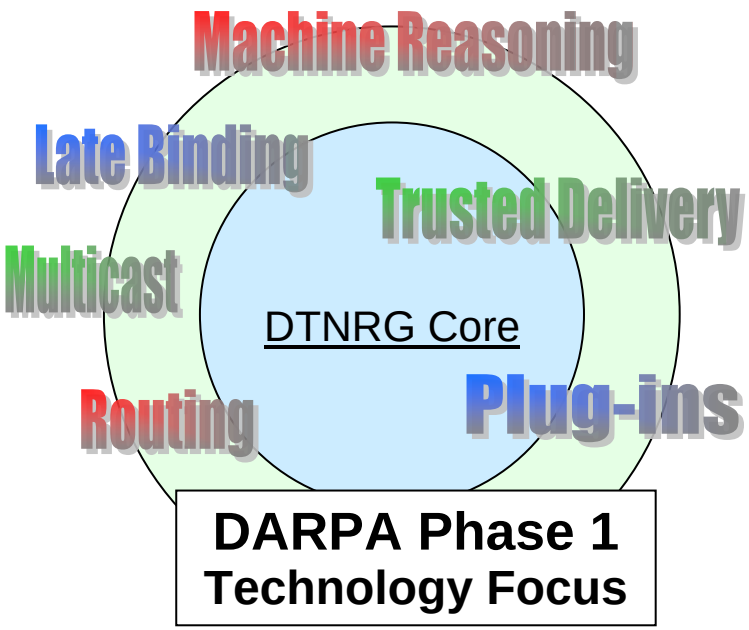


"Think globally, act locally!"

Approved for Public Release, Distribution Unlimited

DARPA DTN Phase 1 Technology Focus

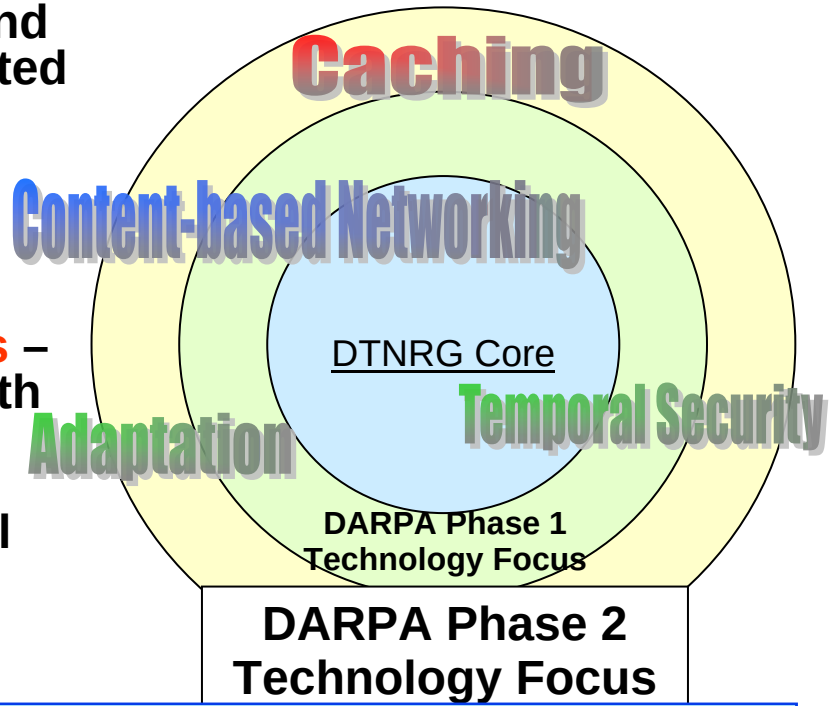
- **Fuzzy Delivery Scheduling – Making network routing decisions when available / optimal paths are uncertain**
- **Policy-based Resource Planning and Utilization – Moving Intelligence into Network to Make "Best" Choices on Delivery**
- **Late Binding – Enable Network to Deliver Traffic Without end-to-end Address and Routing Info**
- **Trusted Delivery – Provide authentication in the absence of connectivity to PKI etc – Security intrinsic in DTN, not an afterthought**
- **Multicast – multiple flavors built-in with store-and-forward**
- **Plug-in Architecture – Tool-chain-independent extension of non-military core to military-specific behaviors**

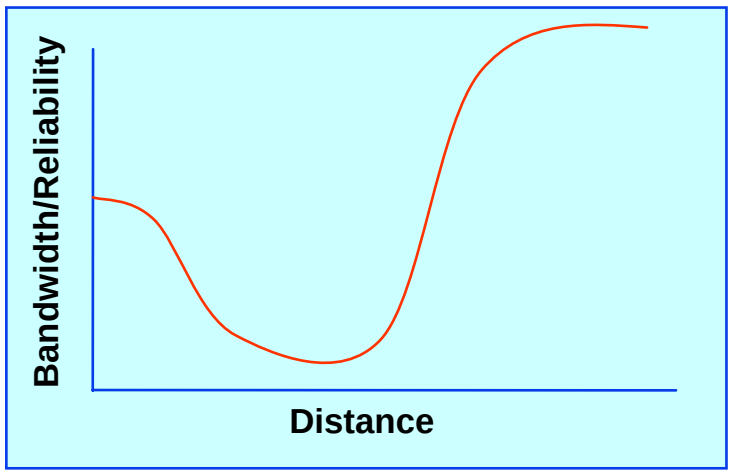


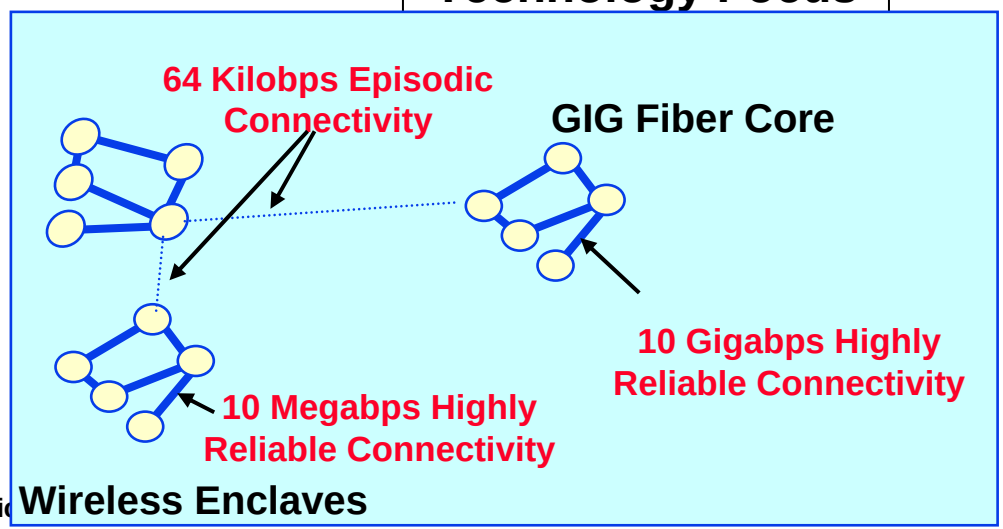
Approved for Public Release, Distribution Unlimited

DARPA DTN Phase 2 Technology Focus

- **Use DTN storage as cache** – bandwidth and latency reduction associated with correlated demand on one end of a thin pipe
- **Content-based access to information** – allows collaboration & data sharing at tactical edge – get away from addresses
- **Support for continuously-changing edges** – DTN nodes need not be on the routing path
- **Policy adaptation for rapid deployment**
- **Temporal Security** – a new security model for protecting information on portable devices





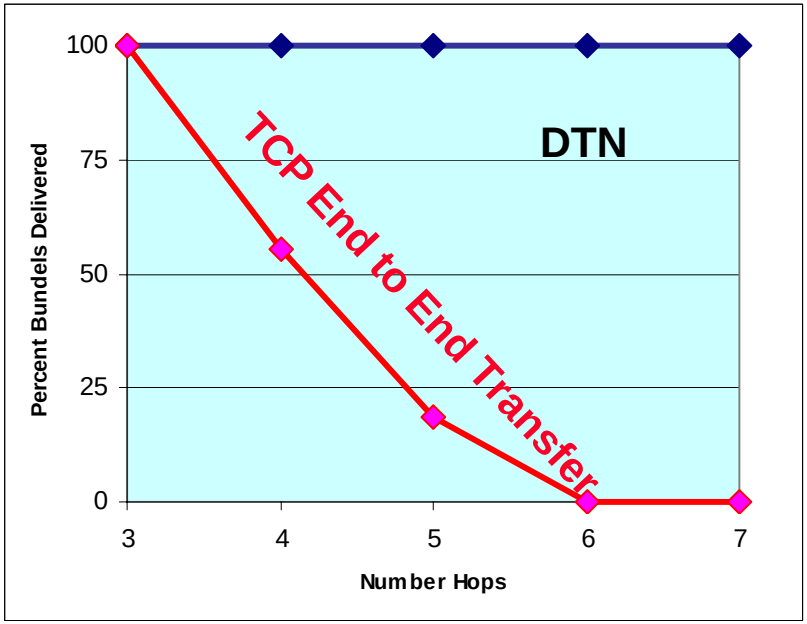


Performance: DTN v. e2e IP

Approved for Public Release, Distribution Unlimited

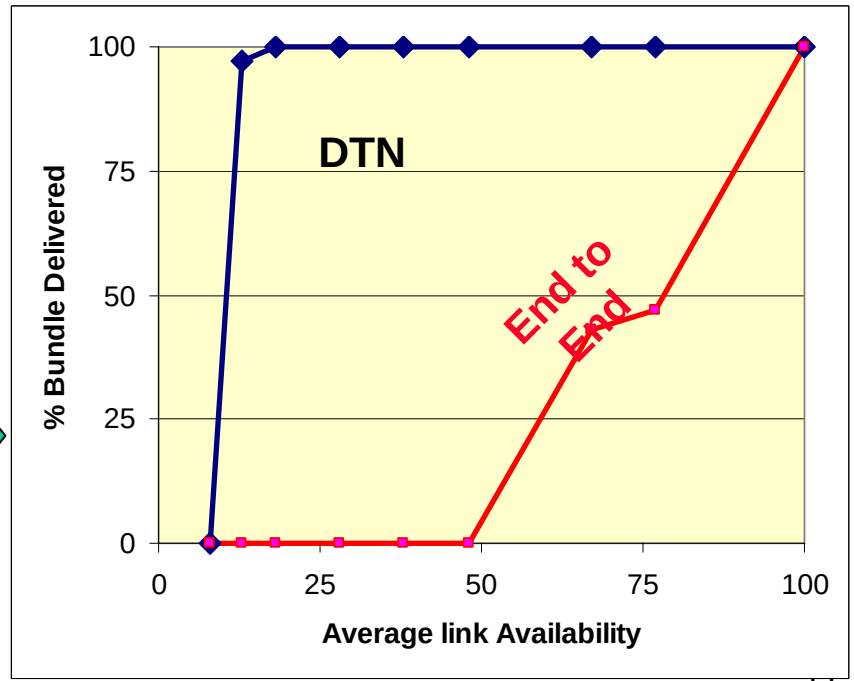
DTN Delivery Performance

Delivery Performance for DTN and E2E



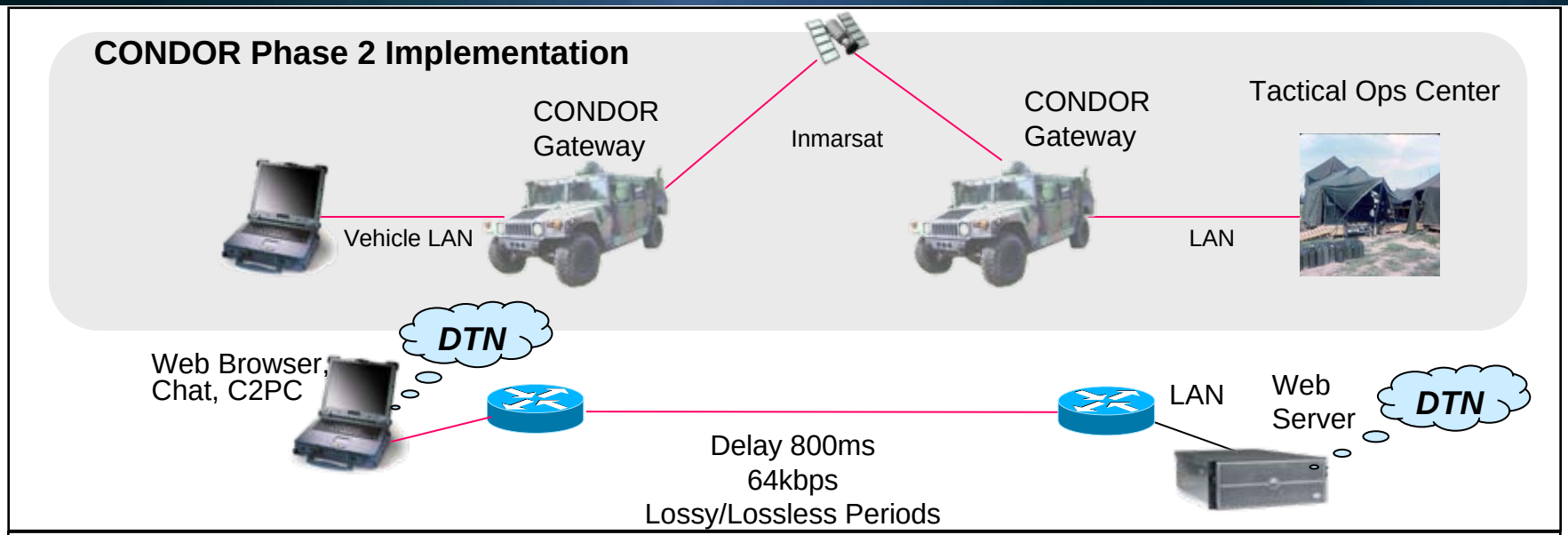
- DTN opportunistic routing delivered all traffic, regardless of hop count
- No complete e2e paths at >6 hops
  - Required Complete Path be Available
- e2e is fundamentally unsuited for military ops
  - 80% available links result in 21% available e2e network connectivity over 7 hops
  - 20% available links result in 0.001% available e2e connectivity over 7 hops

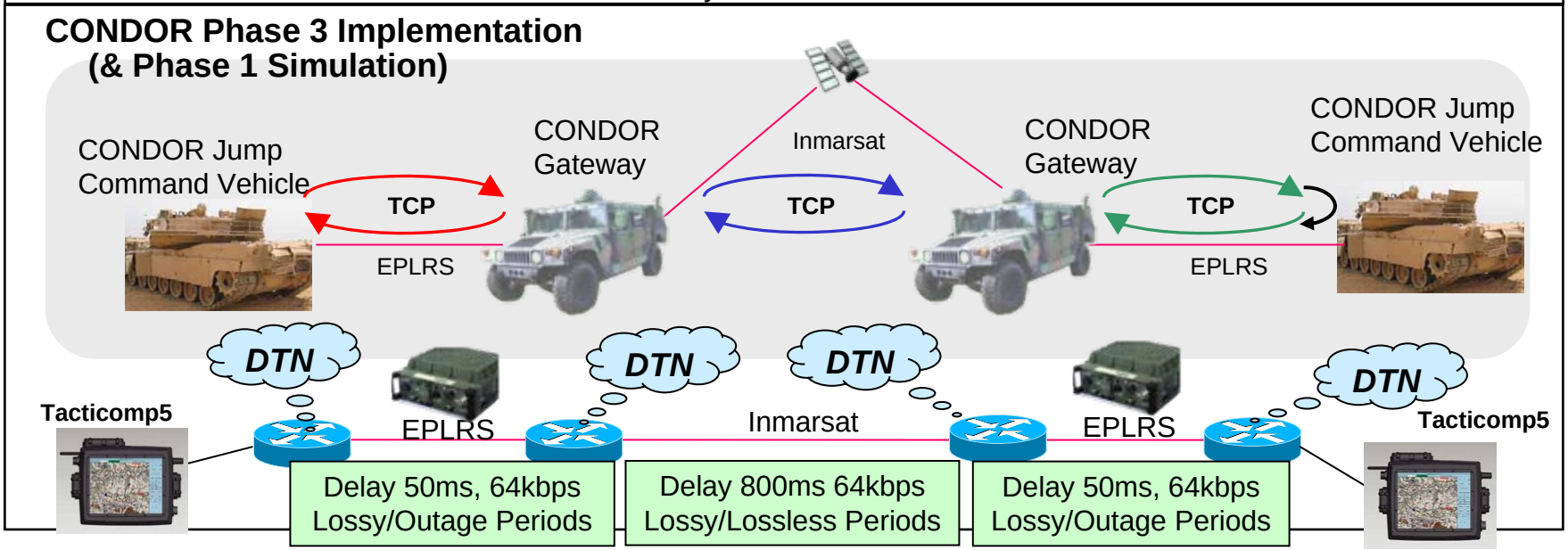
- DTN delivered all messages within the simulation time for avg. link availabilities > 20%
  - With longer simulation would have delivered all messages for <20%
- Insufficient e2e paths to deliver all messages in ***any*** disrupted scenario
  - Failed completely when link availability below 50%



Approved for Public Release, Distribution Unlimited

DTN in CONDOR Context





Approved for Public Release, Distribution Unlimited

DTN v. TCP: CONDOR Simulation

DTN Phase 1 – initial work

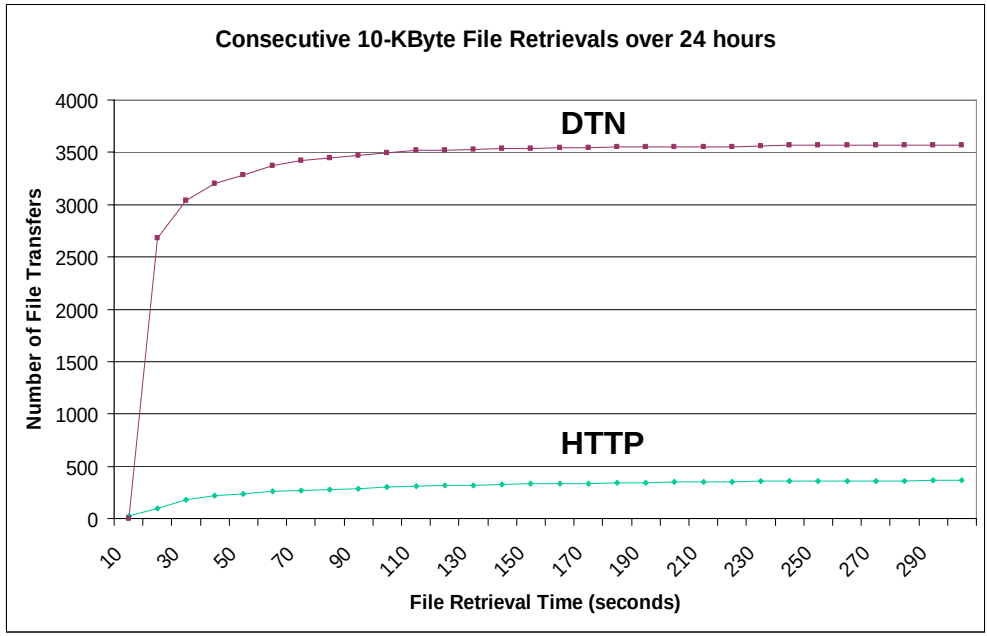
- Simulated network connectivity betw EPLRS to EPLRS over SATCOM
- Demonstrated 10x improvement in latency & completion rate

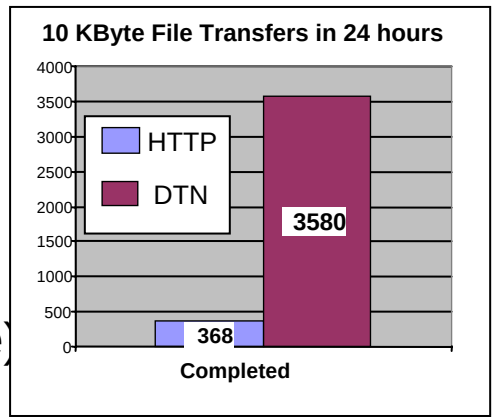
DTN Phase 2 – Building DTN into CONDOR

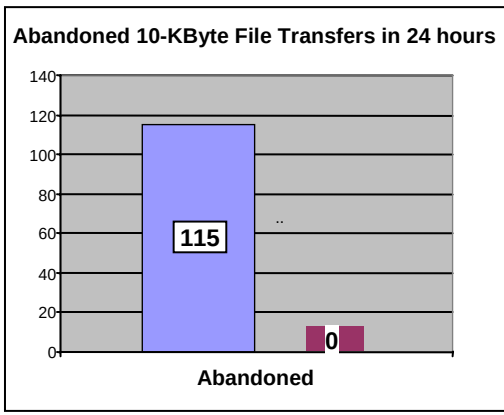
- Develop a CONDOR-specific DTN installation
- Experiment & demonstrate DTN/CONDOR utility
- Desire Phase 3 MoA

DTN Phase 3 – under future MoA

- Integrate Phase 2 & Phase 3 DTN technologies into CONDOR
- Transition technology into USMC operational use (CONDOR to edge)







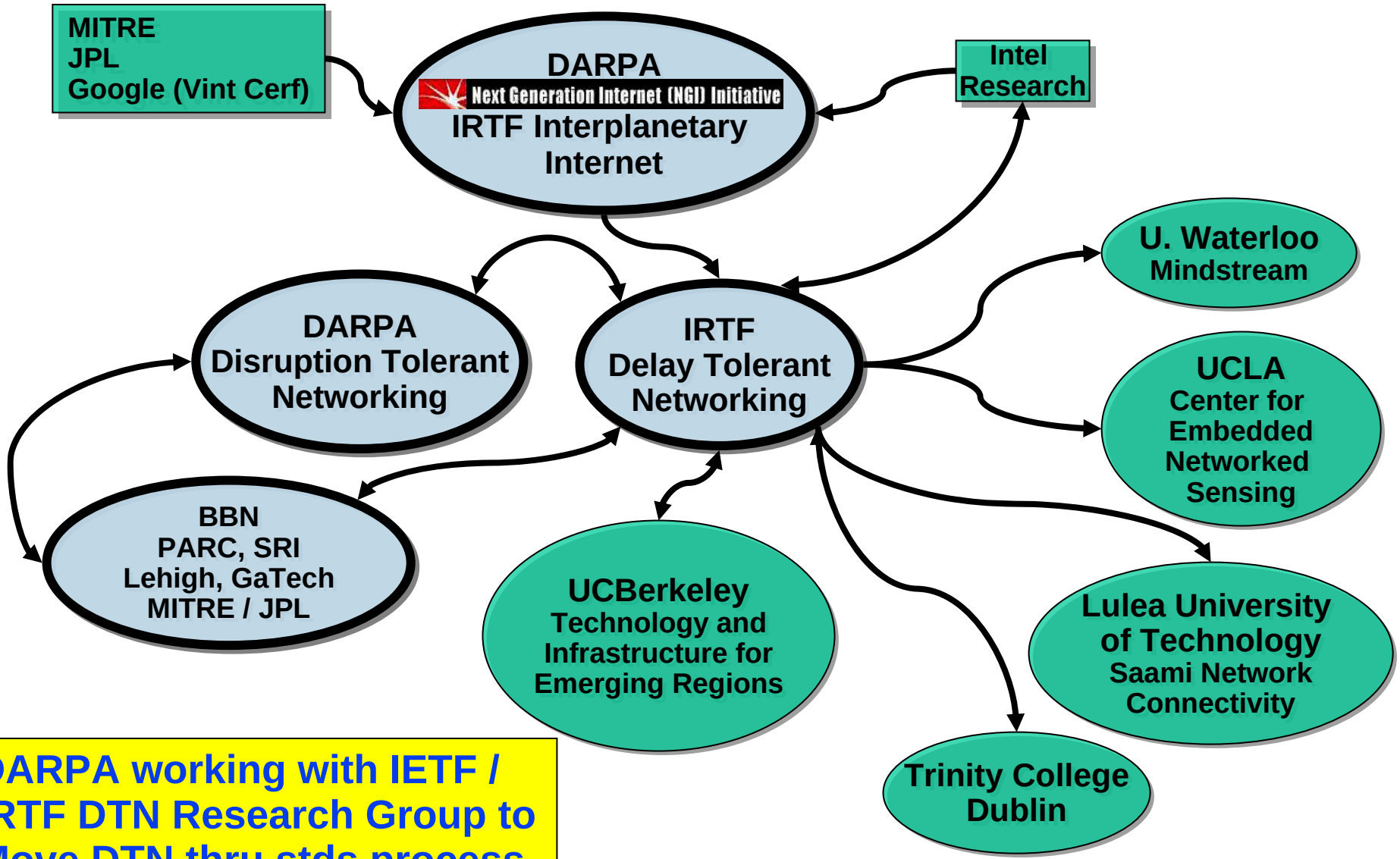
DTN Resolves Issues Identified In DARPA CPOF Transition

Approved for Public Release, Distribution Unlimited

Developing an Extensible COTS DTN

Approved for Public Release, Distribution Unlimited

DTN "Family Tree"



DARPA working with IETF / IRTF DTN Research Group to Move DTN thru stds process

Approved for Public Release, Distribution Unlimited

DTN Internet Drafts & RFCs

- **DTNRG: www.dtnrg.org**

  Documents at www.dtnrg.org/wiki/Docs

  Code at www.dtnrg.org/wiki/code

- **DTNRG Internet drafts at: www.ietf.org**

  http://tinyurl.com/38yca6

  And http://tinyurl.com/2u6vy2

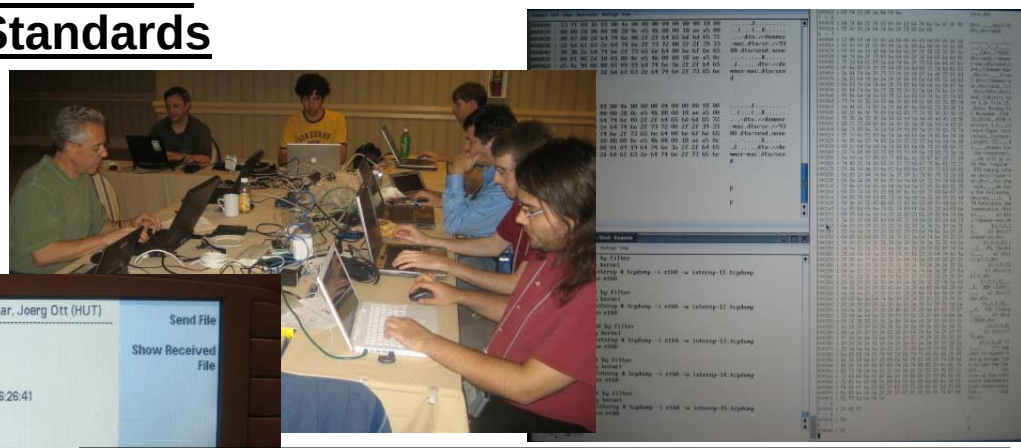
- **GSAKMP: RFC at http://www3.ietf.org/proceedings/06mar/IDs/draft-ietf-msec-gsakmp-sec-10.txt**

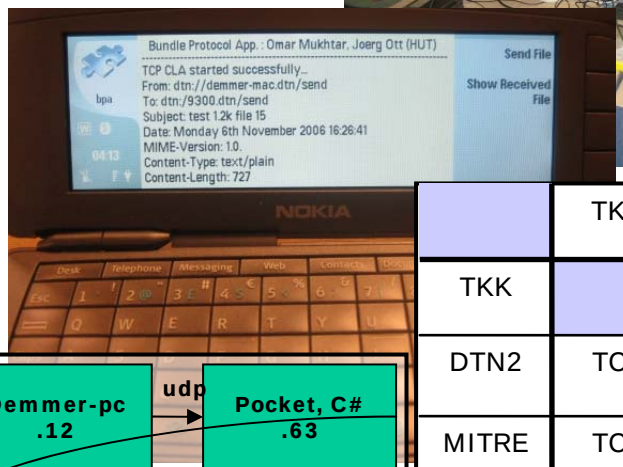
  Java download at: http://gsakmp.sourceforge.net/

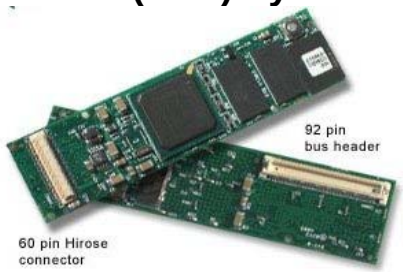
Interoperability

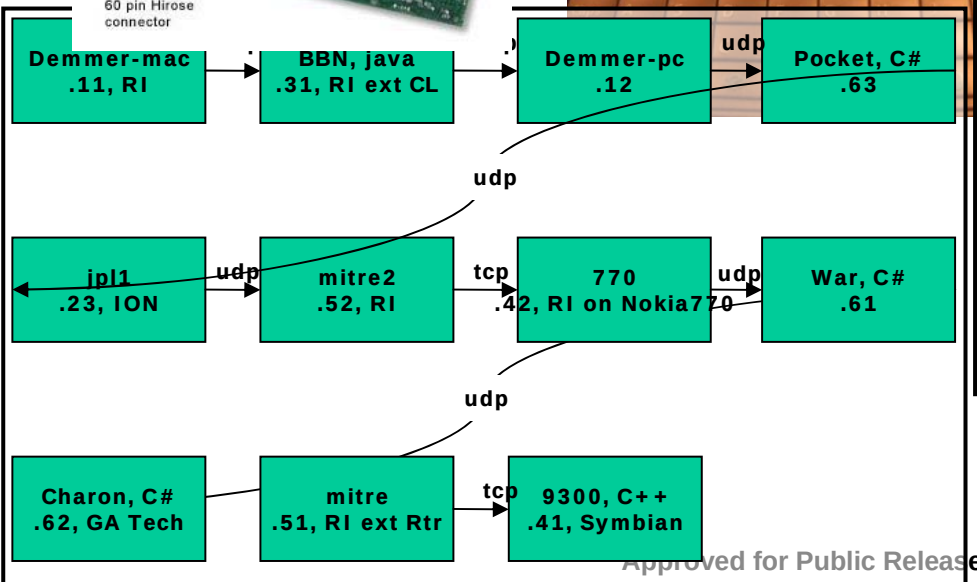
Interoperability Testing at IETF 67 (6-10 Nov 06) of Six Implementations of DTN Standards

1. DTNRG reference implementation (UCB)
2. DTNRG w/BBN external convergence layer
3. DTNRG w/MITRE external router
4. NASA/JPL ION
5. GaTech .Net
6. Helsinki (TKK) Symbian







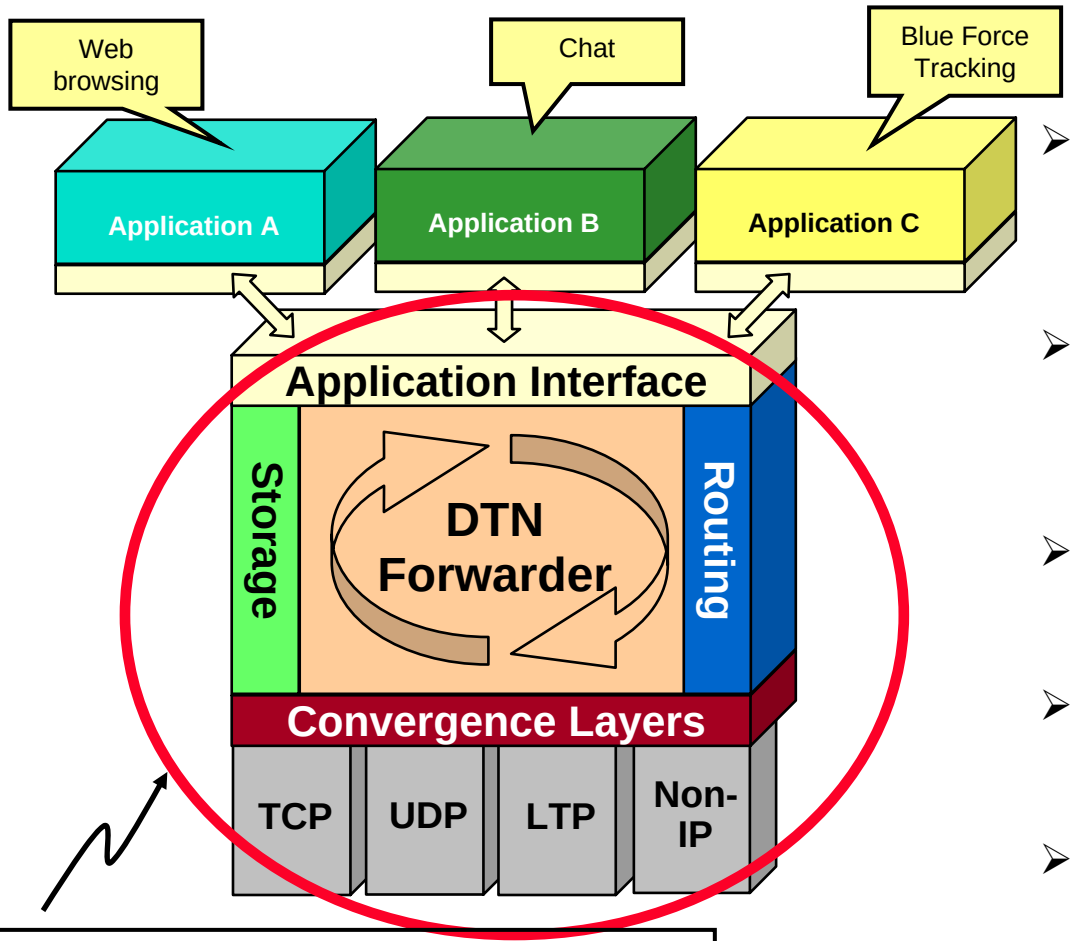


	TKK	DTN2	MITRE	BBN	GA Tech	ION
TKK		TCP	TCP	TCP	via router	via router
DTN2	TCP		TCP, UDP	TCP, UDP	UDP	UDP
MITRE	TCP	TCP, UDP		TCP, UDP	UDP	UDP
BBN	TCP	TCP, UDP	TCP, UDP		UDP	UDP
GA Tech	via router	UDP	UDP	UDP		UDP
ION	via router	UDP	UDP	UDP	UDP	

Six Implementations Interoperated Successfully

Approved for Public Release, Distribution Unlimited

DTNRG Framework



Original Monolithic DTN Implementation Framework

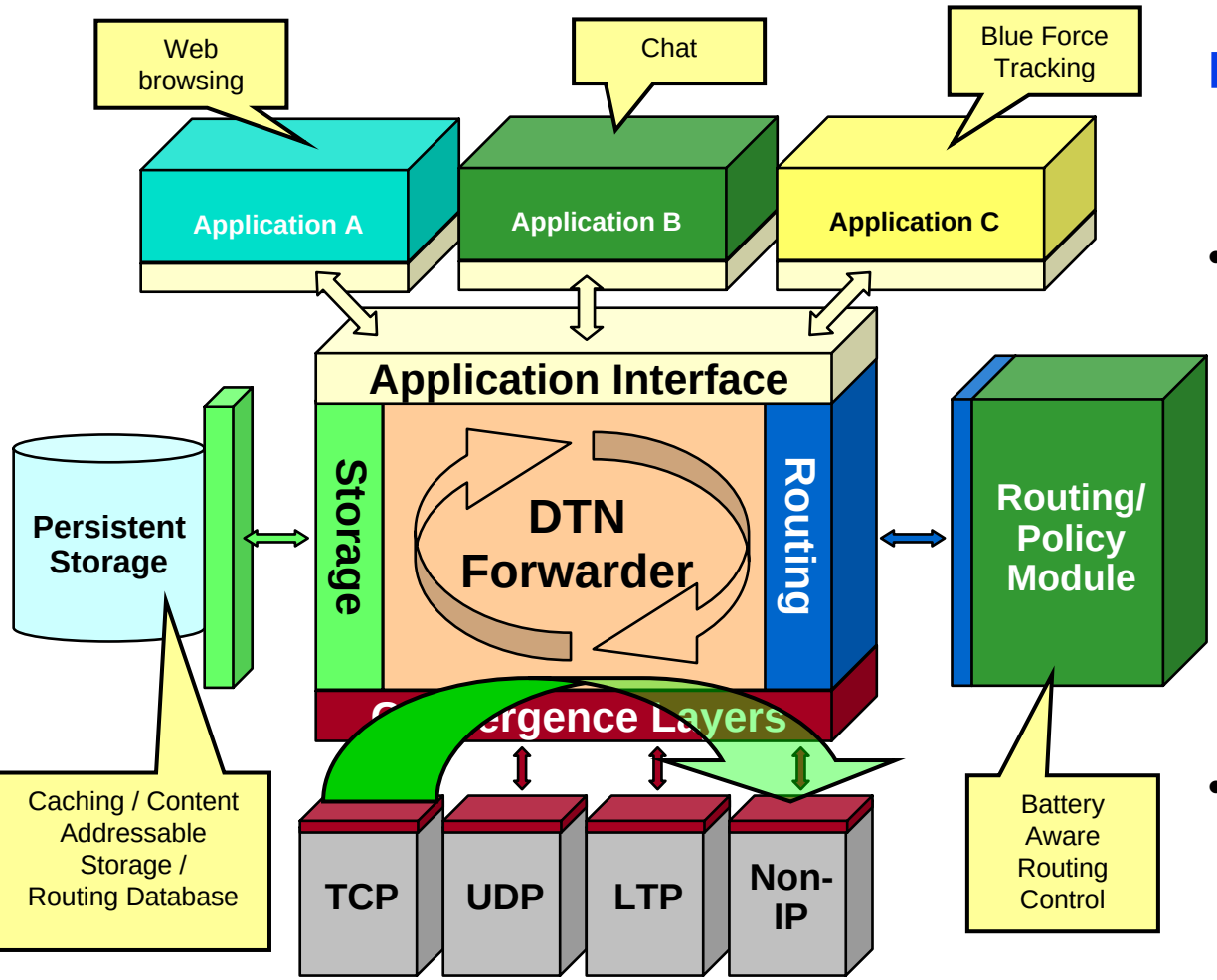
Storage, Routing & Convergence Layers All Within the Same Code Base

- *Original specificiation* assumed monolithic (not extensible) implementations – "take it or leave it" functionality
- Likely to lead to Cisco/Nortel boxes, but like Cisco/Nortel IP equipment, not extensible to military-specific behaviors
- DoD would have to maintain specialized sersions, could not ensure interoperability
- Each program would have to manage its own DTN implementation
- Military needs would be exposed to other users

COTS economies of scale but with the COTS functionality straitjacket!

Approved for Public Release, Distribution Unlimited

DTN Plug-in Architecture



Modularization thru RPC-like/XML interfaces – toolchain independent

- **Isolates core forwarding functionality by specifying plug-in extension interfaces.**
  - **Benefit from COTS economies of scale**
  - **Allow DoD-specific extensions**
  - **No need to stovepipe**
  - **Plug-ins allow cost control**
  - **Export control simplified**
- **No Military Code / Requirements in Open Source Product**

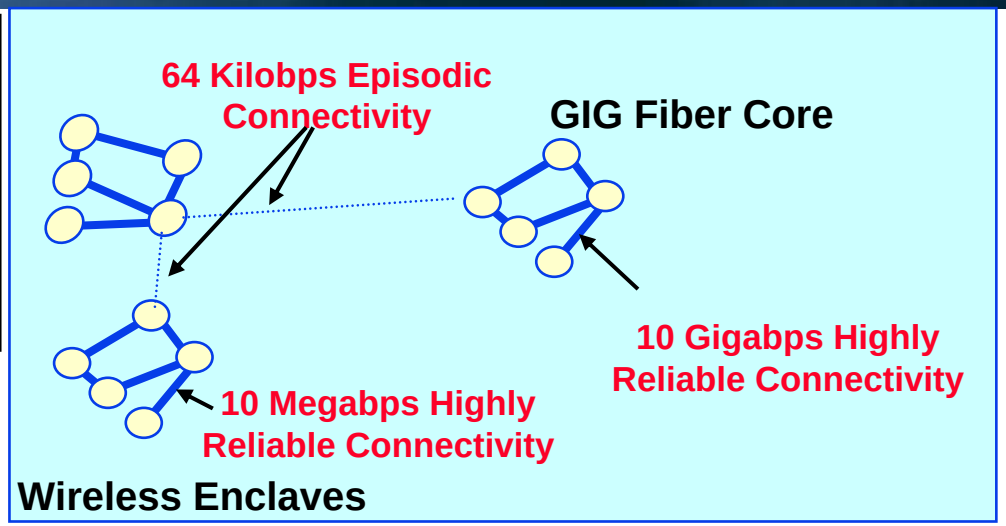
Bridge between heterogeneous networks

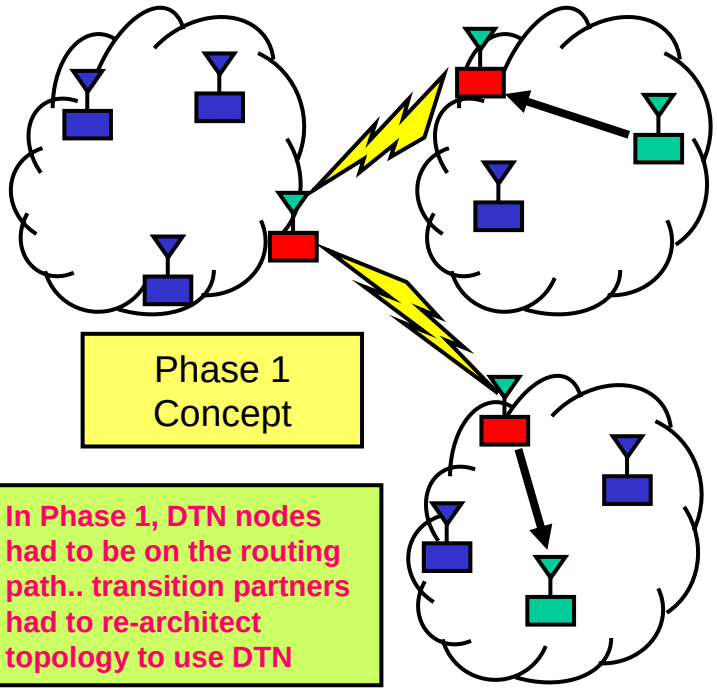
COTS economies of scale *without* the COTS functionality straitjacket!

Approved for Public Release, Distribution Unlimited

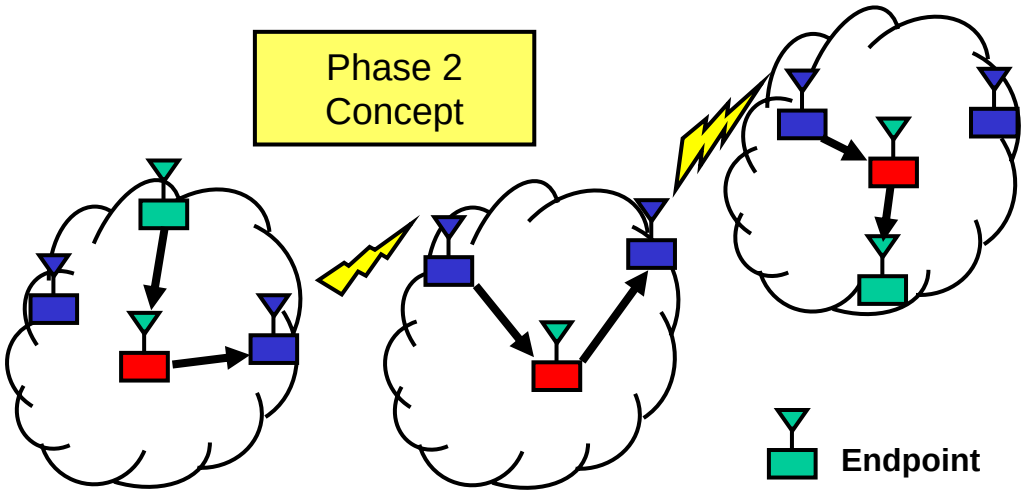
DTN & Network Topology

- DTN leverages local connectivity
- DTN can work in any architecture
- No DTN-specific adaptation needed for insertion
- DTN supports continuously changing edges
- DTN bridges heterogeneous networks





In Phase 1, DTN nodes had to be on the routing path.. transition partners had to re-architect topology to use DTN



DTN Augments Existing Networks without Being Inserted into Topology

Approved for Public Release, Distribution Unlimited

Self-Forming Caches and Content-Based Networking

Approved for Public Release, Distribution Unlimited

On Beyond Disruption!

DTN leverages storage, processing, local connectivity, and the correlation of information requests in tactical nets to provide:

Caching in the tactical clouds – ***storage can be more than a dumb transit buffer***

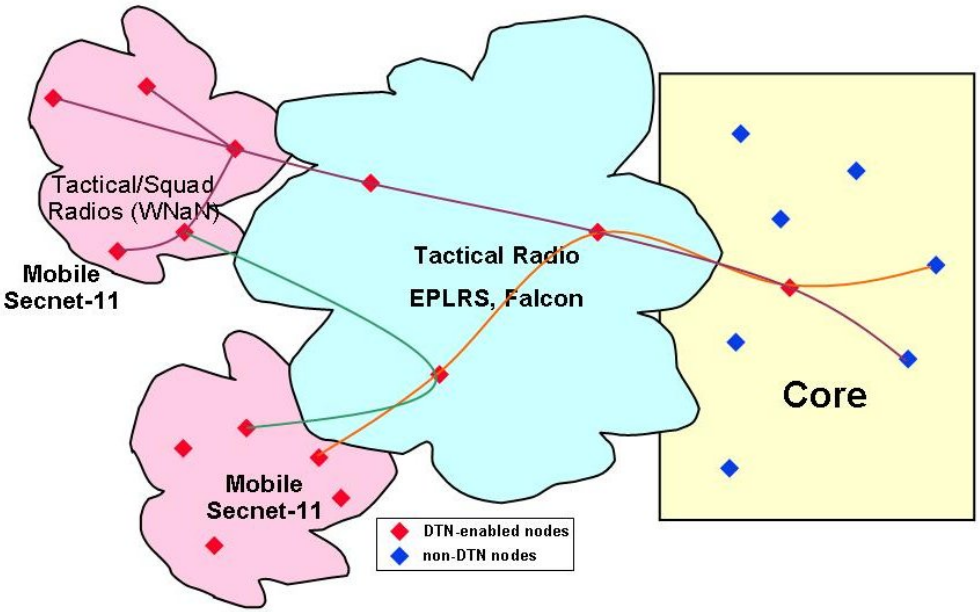
- **Reduces bandwidth demands back to core**
- **Reduces latency**

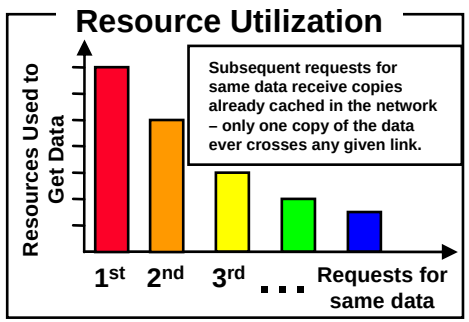
Create dynamic self-forming "Akamais"

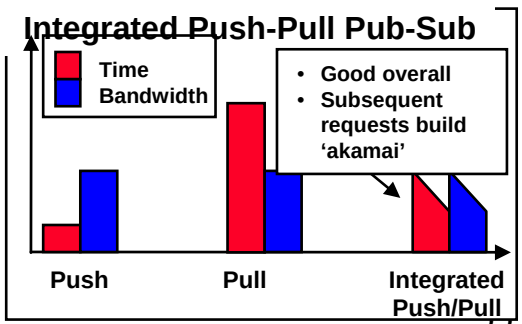
Integrated push-pull pub-sub dissemination of data

Access to information by content description, context, or type rather than by network address

Network-managed persistence of information flowing thru the net







Approved for Public Release, Distribution Unlimited

DTN Military Impact

Caching and disruption tolerance can improve performance at the tactical edge, eg blue force tracking / SA

Content-based addressing provides a mechanism for sharing data at the edge, supports transition *from C2 to a collaborative environment* (CPOF)

Supports a wide variety of use cases, such as:

"I want maps for my area", not "I want to ftp to 192.168.4.17"

"Give me a map of NW Baghdad with all intel since 0400 linked to it"

"Send this information to any unit w/i 200m of any bridge over the Tigris"

"Cache data relevant to the current mission"

"Send this information to blue forces w/i a klick of me"

"Acquire and report back to me sensor data w/i a klick of my current position"

"Monitor and report to me information as it becomes available about red forces on the road to the airport"

Enable two connected edge nodes to exchange blue force data even when server disconnected

CBN Design Philosophy:

Rich descriptions of content

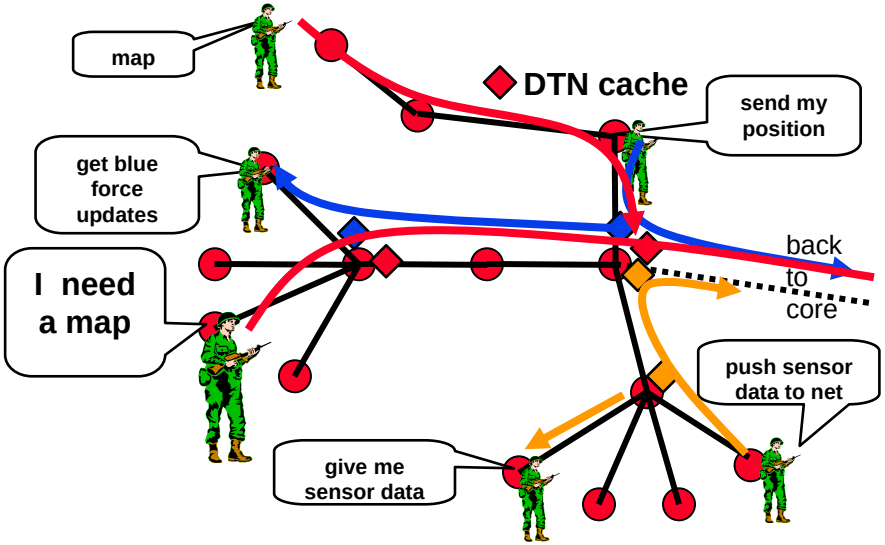
Rich descriptions of nodes

Organize content distribution around supply and demand

User describes content to the network, not address of content

User accesses nodes with names or roles, not address

Tactical deployments largely use static address assignment – IP address assignments drive deployments.. overhead on deployment



Empower the Lower Echelons

Each Node Can Provide Content *to Any Other Node*

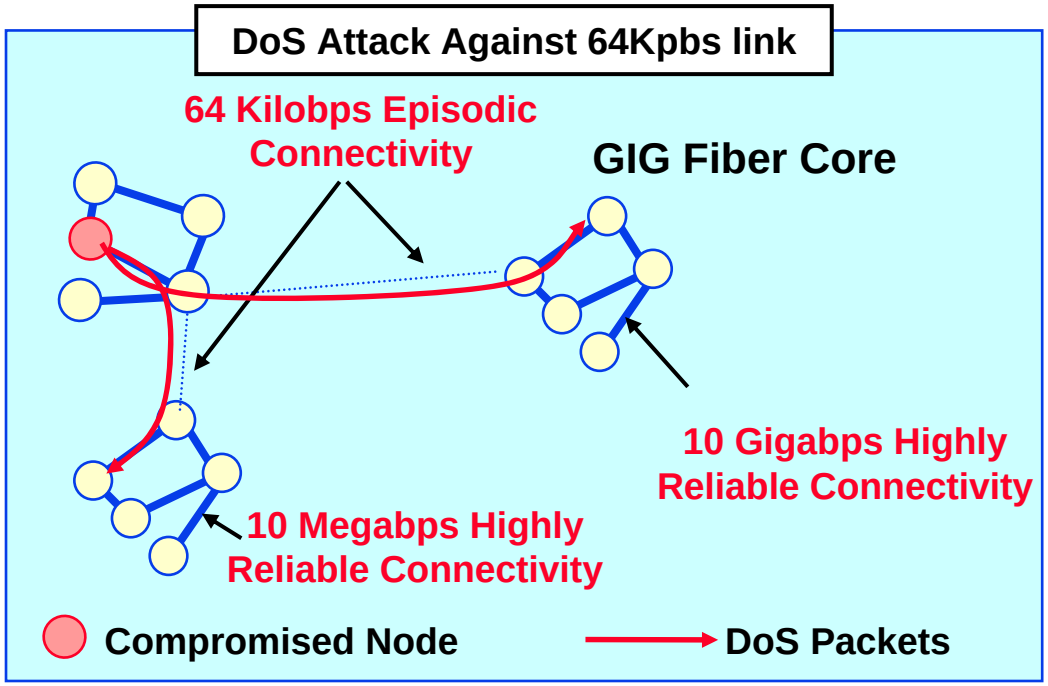
DTN & Security

Approved for Public Release, Distribution Unlimited

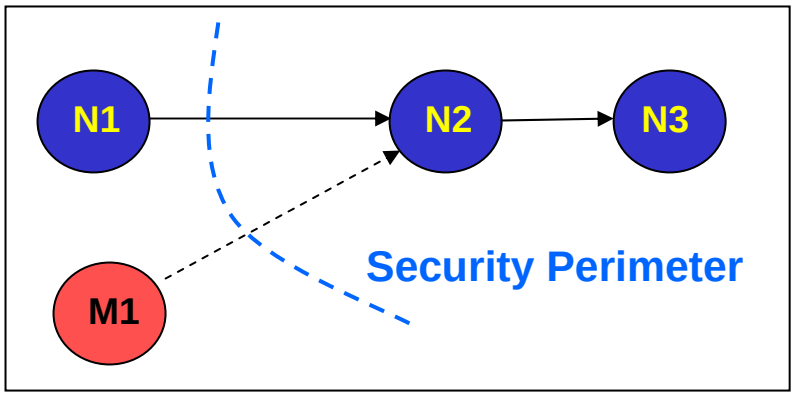
DTN & Security

Three Security Problems in tactical networks

1. **Denial of Service (DoS) attacks against a thin pipe by a compromised node**



Authentication should have been built into the Internet from the beginning



Applications that use DTN can use security for free

DTN Bundle Security Protocol Provides a General Mechanism for Authenticating Bundles Before They Enter a DTN Network

Approved for Public Release, Distribution Unlimited

DTN & Security: Temporal Security

Three Security Problems in tactical networks

1. **Denial of Service attacks against thin waist by a compromised node**
2. **Loss of equipment exposes decrypted data on the node**

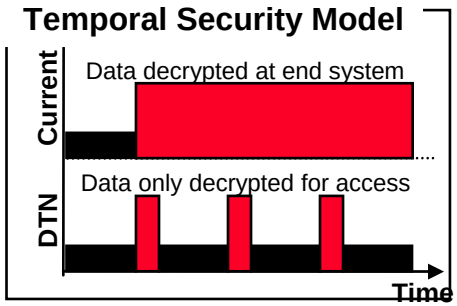
Standard COMSEC – red-black separation w/encryption in the network – says nodes are physically secure, so data is safe when it's at the node (can be red/decrypted), but data in the network may be tapped, so needs encryption (black).

Low-cost nodes (WNaN radios, laptops, PDAs) no longer physically secure, so a lost radio or laptop exposes the data on it.

The current security model doesn't work for portable devices!

Instead of red-black physical separation, provide red-black temporal separation – transitory access to the data thru bundle layer decryption

Data stays black until/unless the application is processing it, and goes away when the application goes away.



DTN bundle security mechanism moves the security infrastructure to the tactical boundary.

DTN & Security

Three Security Problems in tactical networks

1. **Denial of Service (DoS) attacks against thin waist by a compromised node**
2. **Loss of equipment exposes decrypted data on the node**
3. **Protection of data that network node is not authorized to read**

Solution: ***keep data in black in servers, network caches, and local cache.***

Decrypt data only when app asks for it, and scrub data when app exits

Creates a New Problem: ***in DTN, every bundle can be protected with a different security association .. How to operate a cache with encrypted bundles?***

Solution: ***1) Associate metadata with data, encrypt metadata with common key every node has***

2) Separate protection mechanism for data and metadata

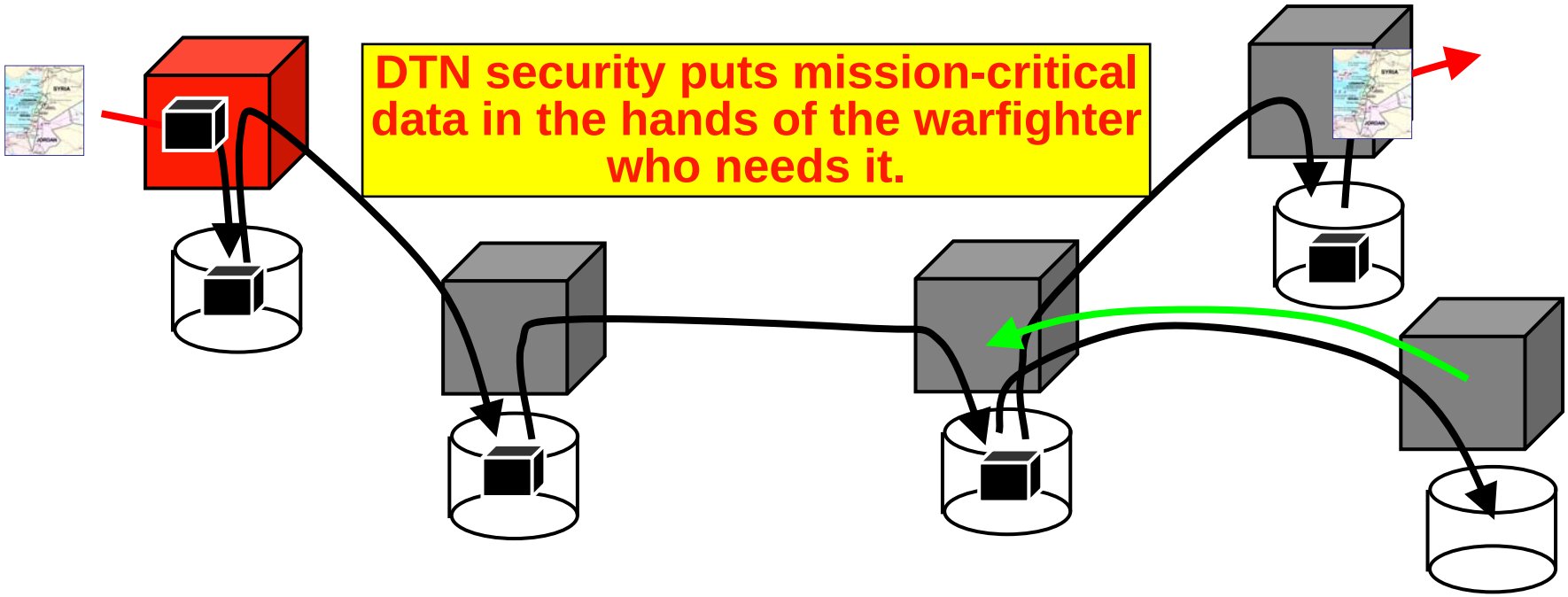
3) Cache hits by matching on metadata

Common Encrypted Metadata Allows Encrypted Data to be Identified and Delivered from Network Node Cache to End Point

Approved for Public Release, Distribution Unlimited

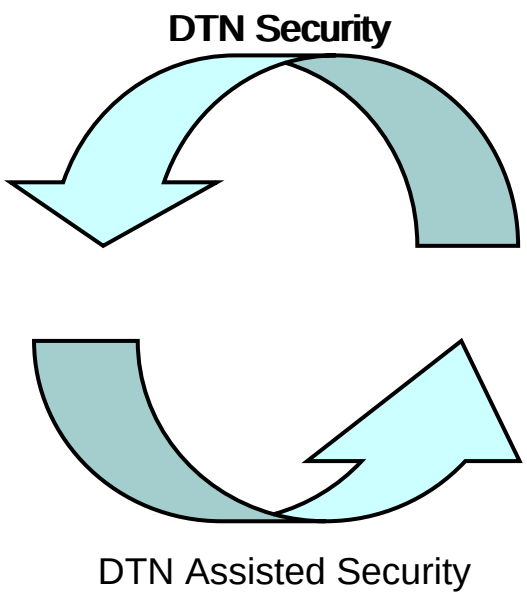
DTN & Security

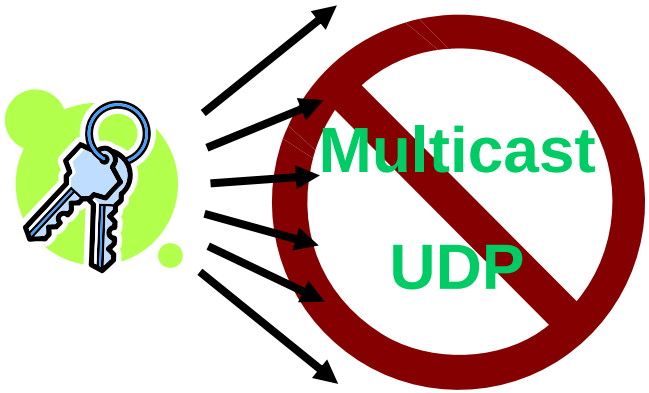
Problem:	Solution
DoS attacks against thin pipe	DTN BSP protects each hop
Lost equipment exposes data	E2E crypto, decrypt in bundle layer
Caching sensitive data / matching on encrypted data	Separate protection mechanisms for data & metadata

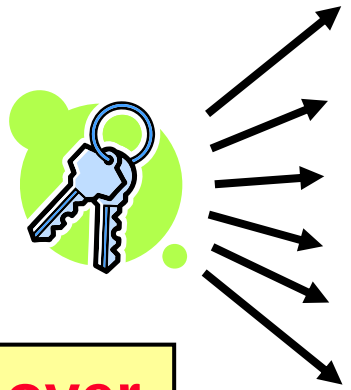


Approved for Public Release, Distribution Unlimited

Security Enables DTN Caching, DTN Supports Security Keying







DTN enabled key management systems

DTN Enables Reliable Keying over Episodic Networks

Approved for Public Release, Distribution Unlimited

DTN Timelines

Approved for Public Release, Distribution Unlimited

DTN Go/No Go Metrics

Phase I

Mar 05 – Feb 06

- **Demonstrate Bundle Delivery Mechanism with 80% Utilization and 100% Reliability on Links of 20% Availability**
- **Demonstrate Trusted Delivery**

Phase II

Aug 06 – Jan 08

- **Demonstrate Bundle Mechanism in IP Networks**
- **Information Binding on Demand from Cache**
- **Demonstrate Policy Language Control Over Delivery Choices**
- **Maintain Phase 1 Metric**
- **Establish MOA for Implementing Phase III in Typical Military System**

Phase III

Feb 08 - Aug 09

- Adaptive DTN-on-demand
- Demonstrate late Binding in IP Networks

Approved for Public Release, Distribution Unlimited

DTN Progressive Maturity

Protected, High Performance DTN for Static Applications with Store and Forward

Phase 1

- Integrate Push and Pull Metaphors
- Cognitive Caching
- Information Addressing (not Network Addressing)
- Multiple Native Networks (JTIDS, IP, EPLRS, …)
- Initial Demo Board Implementation

Phase 1 + Protected, DTN for Medium Scale, Static Applications with Caching and Distributed Query

Phase 2

- Self-Organizing in Response to Network needs
- Large Scale
- Red/Black Management of Persistent Data

- **Demo in Military Scenario to Assess Utility**
- **Implement in Longer term, non-Military Application for Operational Experience**

Dynamically Self-Organized Organized, Secure Local Store, Application Linkages, Proven

Phase 3

- **Integrate into Military Networks**
- **Implement in Longer term non-Military Application to Acquire Experience**

Progressive Technology Development Resulting in Proven and Deployable Product

Approved for Public Release, Distribution Unlimited

Questions?