Moving Data Through Disconnected Networks
Delay-Tolerant Networking and the IC (U//FOUO)

The overall classification of this briefing is:
TOP SECRET//COMINT//REL TO USA, FVEY
Outline

1. (U) Delay-Tolerant Networking intro
   i. Outside world: protocols and software
   ii. IC Applications of DTNs
2. (TS//SI//REL) Summary of R4 work
   i. CHIMNEYPOOL integration
   ii. Wireless testing
3. (TS//SI//REL) Interesting details
   i. DTN Routing
   ii. DTN Security
Mobile Ad-Hoc Networks (U)

- (U//FOUO) A wireless network with no infrastructure
(U//FOUO) Many wireless networks will not have end-to-end connectivity.
Delay-Tolerant Networks (U)

- (U//FOUO) DTNs use a store-carry-forward approach to take advantage of node mobility

Destination
Beginnings of DTN (U)

2000: Epidemic Routing
   Vahdat and Becker

1990s: Interplanetary Network
   NASA, JPL

2002, 2004: ZebraNet
   Juang, Oki, Wang, Martonosi, Peh, Rubenstein

2002: Mobility Increases Capacity in Ad-hoc Wireless Networks
   Grossglauser and Tse

2003: A DTN Architecture for Challenged Internets
   Kevin Fall

2003: DataMULEs
   Shah, Roy, Jain, Brunette

2003: Probabilistic Routing in Intermittently Connected Networks
   Lindgren, Doria, Schelen
Beginnings of DTN: Epidemic (U)

- 2000: Epidemic Routing - Vahdat and Becker

Nodes exchange “summary vectors”
- Each node sends the data that the other node lacks
- Summary vectors implemented as a Bloom Filter
- Followed by Immunity concept: Resource and performance tradeoffs in delay-tolerant wireless networks, 2005; Small and Haas
Beginnings of DTN: ZebraNet (U)

- Wildlife tracking project at Princeton
- GPS + other info gathered by collars on zebras
- Data migrated back to base using “History-Based” routing
Beginnings of DTN: IPN (U)

- Inter-Planetary Network
- Long distances → long propagation delays
- Intermittent connections
- Known contact schedule → Contact Graph Routing
- Worked on since the 1990s by NASA, JPL, incl Vint Cerf

[Figure taken from Vint Cerf’s 2010 presentation: “When Intuition Fails”]
Beginnings of DTN: DataMULEs (U)

- *Data MULEs: modeling a three-tier architecture for sparse sensor networks*
- Has mobile MULEs relaying data from sensors to well-connected Access Points
- Similar: A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks, 2004; Zhao Ammar, Zegura
What’s a DTN For? (U//FOUO)

- Wildlife tracking
  - ZebraNet, SWIM, TurtleNet

- Outer space

- Under water

- Underground (mines)
  - [DTN Communication in a Mine, 2010 Ginzboorg, Kärkkäinen et al]

- Rural areas
  - N4C, DakNet, KioskNet, TIER, Bytewalla

- VANETS, Public transit
  - DieselNet, Braunschweig, NICT

- Battlefields/disaster areas
  - DARPA DTN Program

- Sensor nets

- Heterogeneous networks
  - [Integrating Multiple and Heterogeneous Challenged Networks for Large-sized Data Transfer, 2009 Nagata et al]
What’s a DTN for II (U//FOUO)

- Content dissemination
  - [PodNet, 2006 – Present; Legendre, Lenders, May, Karlsson]
  - Haggle Project

- Social Networking

- Distributed Sotrage
  - [TierStore, 2008; Demmer, Du, Brewer]
  - [DTN-based Content Storage and Retrieval; Ott, Pitkanen]

- Cellular Traffic Offloading
  - [Cellular Traffic Offloading through Opportunistic Communications: A Case Study, 2010; Han, Hiu et al]
Standardization Activities* (U)

- DTNRG has been part of the IRTF since (at least) 2002
- RFC 5050 defines the **Bundle Protocol**
- Application-layer overlay that moves “bundles” of data
- Convergence Layers move bundles over different networks
Protocol Highlights (U//FOUO)

- Modular architecture
  - Convergence layers
  - Routers
  - Neighbor discovery
- Security extensions
- Persistent storage
- Hop-by-hop and end-to-end reliability possible
Bundle Protocol Architecture (U//FOUO)

Bundle Protocol Agent (BPA)

Convergence Layer
- TCP CL
- UDP CL
- File CL
- AX.25 CL
- ...
Bundle Protocol Stack Landscape

Vapor

Aalto Java stack

Cisco Java stack

GA Tech C# stack

iPhone TCPCL

SPINDLE

Bytewalla

IBR-DTN

dtns60

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Summary of Intelligence Community Applications (U//FOUO)
Covert Communications (TS//SI//REL)

- (TS//SI//REL) Provide covert comms in denied areas where no infrastructure exists, or where using the infrastructure would compromise the operation.
- (S//REL) Several “brush-pass” wireless hand-offs as an untraceable alternative to scheduled meetings, dead drops.
- (TS//SI//REL) DTN provides an open-source solution running on commercial handheld devices Unattributable.
Close Access (TS//SI//REL)

- (TS//SI//REL) Implant in a secure facility or denied area
- (TS//SI//REL) Need to transfer data and commands over two or more hops
- (TS//SI//REL) May rely on mobile nodes and unwitting data mules
NRO/MSD Collaboration

- (TS//SI//TK) Moving data between ground stations using CubeSats. Coverage every ~1.5 hours. Need DTN

- (TS//SI//TK) They use DTN2, ION, contact graph routing
Crowd Sourcing (U)

- (TS//SI//REL) Provide data flow in and out of closed nations during internet shut-down
- (U) Ambitious BIG idea
- (U) Proposed CONOP not far from current work
- (U) Proposed internally and externally
- (U) State Dept-funded project had an article in NYT
Tagging Tracking & Locating (U)

- (U) Insert GPS trackers in cars or electronics, but we may never see them again
- (TS//SI//REL) Migrate data back to collection point via DTN
- (TS//SI//REL) Original CONOP for RAPTOR GALAXY
# Summary of IC applications (U//FOUO)

<table>
<thead>
<tr>
<th>CovComm</th>
<th>Close Access</th>
<th>NRO CubeSat Comms</th>
<th>Crowd-Sourcing</th>
<th>Tagging Tracking &amp; Locating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unattributable</td>
<td>Data exfiltration from isolated networks and denied areas</td>
<td>Comms between ground stations that only have occasional satellite coverage</td>
<td>Provide data flow in and out of closed nations</td>
<td>Very small hardware</td>
</tr>
<tr>
<td>COTS handsets</td>
<td>TSV field test</td>
<td>Use inexpensive CubeSat platform</td>
<td>Ambitious BIG idea</td>
<td>Record locations and encounters</td>
</tr>
<tr>
<td>Open-source</td>
<td></td>
<td></td>
<td>Proposed CONOP can be done now</td>
<td>Use DTN to migrate data back to collection points</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Proposed internally and externally</td>
<td></td>
</tr>
</tbody>
</table>
DTN work at R4
Things We Have Done (U)

- Porting FOS DTN software to mobile devices
Things We Have Done (U)

- Porting FOS DTN software to mobile devices
- Developing friendly user interface software so anyone can use it
What We Have Been Building (U)

- Porting open source DTN software to mobile devices
- Developing friendly user interface software so anyone can use it
- Testing – determining what actually works
- Field testing different configurations and scenarios
- Implementing security features
- Building new routing modules
- Adding geo-tagging/tracking features
- Experimenting with new neighbor discovery methods
FUZZYLINT and CHIMNEYPOOL integration (TS//SI//REL)
(Not So) Close Access

- (TS//SI//REL) Retrieving data from an implant without visiting the implant ourselves
- (TS//SI//REL) Need to add DTN link capability to the implant
- (S//REL) Data mule may be unaware of their role
- (TS//SI//REL) Rough prototype demoed at Trident Spectre
• (TS//SI//REL) Cross-platform implant built using TAO’s CHIMNEYPOOL framework
  - Ports for Linux, Windows, etc..
  - Endpoint-centric: focused on file exfil from a PC
  - Remote Procedure Call (RPC) based
• (TS//SI//REL) FRIEZERAMP protocol provides covert networking
  - CHIMNEYPOOL comms module
  - Similar to IP, IPsec
  - Only supports static network configuration
• (TS//SI//REL) FRIEZERAMP links are adapters to converge FR packets onto the transport layer below
  - Examples: https, udp, smtp, etc.
Put SBZ on each device ... right?
(TS//SI//REL)

- (TS//SI//REL) File exfil CP modules and FRIEZERAMP treats reliability as **only** an end-to-end issue
  - FR retransmissions are requested by the receiver and only the sender can retransmit
  - Hop-by-hop reliability is desirable
- (TS//SI//REL) Persistent storage module only waits until link is available then “send and forget”
- (U//FOUO) All routes are static and setup a priori
- (TS//SI//REL) Operationally, SBZ on each device is undesirable in some CONOPs
Ultra-lightweight BPA (TS//SI//REL)

- (TS//SI//REL) [REDACTED] has been building an ultra-lightweight BPA that can act as a CP link to a DTN
- (U//FOUO) Locally provides data persistence, discovery, routing, convergence layers
- (TS//SI//REL) FR packets are already fragmented, so this BPA does not need to be as flexible as others
- (S//REL) Can add covert Convergence Layer Adapters
## Platforms and Capabilities (TS//SI//REL)

<table>
<thead>
<tr>
<th></th>
<th>Linux netbook</th>
<th>Maemo</th>
<th>iPhone</th>
<th>Gumstix</th>
<th>Android</th>
<th>Windows and Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTN2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBR-DTN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FUZZYLINT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Current Effort
Wireless testbeds
(U//FOUO)
Reality Ninja (U//FOUO)

Reality

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical
Reality Ninja (U//FOUO)

Reality

Network Emulators

Application
Presentation
Session
Transport
Network
Data Link
Physical

Application
Presentation
Session
Transport
Network
Data Link
Physical
Reality Ninja (U//FOUO)
Mobile Wireless Testbed (U//FOUO)
Mobile Wireless Testbed (U//FOUO)
CMU Wireless Emulator (U//FOUO)
Detailed Channel Modeling (U//FOUO)
Some Interesting Details (U)

- Routing and Reliability Issues
- Security Issues
Routing in DTNs (U)
Flood Routing and Epidemic (U)

- 2000: Epidemic Routing [Vahdat and Becker]
Static Routing Background (U)

- Bundle Protocol Nodes are identified by Endpoint Identifiers (EIDs) that look like:
  dtn://dtnbone.umd.edu.dtn/
  dtn://nodea.dtn/
  ebr://group5.dtn/

- Convergence Layer connections to neighbors are called “Links”
  - For example a TCP connection to a neighbor is a link

- Each link knows the EID of the neighbor associated with it
## Static Routing Tables (U)

One-hop “Direct Delivery”

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next hop</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtn://sam.dtn/</td>
<td>link-0</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://bob.dtn/</td>
<td>link-1</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://amy.dtn/</td>
<td>link-2</td>
<td>FWD</td>
</tr>
</tbody>
</table>

![Diagram showing routing network]

- **Joe** connects to **sam** via **link-0**
- **Joe** connects to **bob** via **link-1**
- **Joe** connects to **amy** via **link-2**
Static Routing Tables (U)

Two-hop “Bundle Ferry”

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next hop</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtn://sam.dtn/</td>
<td>dtn://ferry.dtn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://bob.dtn/</td>
<td>dtn://ferry.dtn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://amy.dtn/</td>
<td>dtn://ferry.dtn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://ferry.dtn/</td>
<td>link-0</td>
<td>FWD</td>
</tr>
</tbody>
</table>
Static Routing Tables (U)
Two-hop “Bundle Ferry” with wildcards

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next hop</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtn://sam.dtn/</td>
<td>dtn://ferry-*.dttn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://bob.dtn/</td>
<td>dtn://ferry-*.dttn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://amy.dtn/</td>
<td>dtn://ferry-*.dttn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://ferry-27.dtn/</td>
<td>link-0</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://ferry-180.dtn/</td>
<td>link-1</td>
<td>FWD</td>
</tr>
</tbody>
</table>

Diagram:
- Joe
  - link-0: ferry-27
  - link-1: ferry-180
- ferry-27:
  - link-0: sam
  - link-1: bob
- ferry-180:
  - link-0: sam
  - link-1: amy
# Static Routing Tables (U)

Multi-hop “Tiered routing”

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next hop</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtn://twitter.dtn/</td>
<td>dtn://tier1-*-dtn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://twitter.dtn/</td>
<td>dtn://tier2-*-dtn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://twitter.dtn/</td>
<td>dtn://tier3-*-dtn/</td>
<td>FWD</td>
</tr>
<tr>
<td>dtn://twitter.dtn/</td>
<td>link-0</td>
<td>FWD</td>
</tr>
</tbody>
</table>

![Diagram](image.png)
DTN Routing Bonanza (U)

- (U//FOUO) People propose routing protocols for many different environments and purposes.
  - Sometimes with novel applications, sometimes with no real need
- (U) Has inspired the phrase “Yet Another Routing Protocol”

<table>
<thead>
<tr>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flooding</td>
</tr>
<tr>
<td>Static with copy links</td>
</tr>
<tr>
<td>Neighborhood</td>
</tr>
<tr>
<td>Epidemic</td>
</tr>
<tr>
<td>Endemic</td>
</tr>
<tr>
<td>Epidemic with Immunity</td>
</tr>
<tr>
<td>mphone</td>
</tr>
<tr>
<td>TIERStore</td>
</tr>
<tr>
<td>DTLSR</td>
</tr>
<tr>
<td>Simple Coupling</td>
</tr>
</tbody>
</table>
DTLSR (U)

- (U//FOUO) Delay-Tolerant Link State Routing
  - Assumes a mostly stable contact graph
  - Nodes all flood their recent contacts
  - Each node maintains an internal picture of the network, and makes routing decisions based on Dijkstra’s alg
“Intelligent” Routing: PRoPHET (U)

- Probabilistic routing in intermittently connected networks, 2003; A. Lindgren, A. Doria, and O. Schelén
- Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET)
“Intelligent” Routing: PRoPHET (U)

- Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET)
Network-Coding in DTNs (U)

- Imagine trying to distribute a 100MB bundle in a DTN
- Idea:

```
10MB
```

```
1MB 1MB 1MB 1MB 1MB 1MB 1MB 1MB 1MB 1MB
```
Network-Coding in DTNs (U)

- Imagine trying to distribute a 100MB bundle in a DTN
- Idea: fragment into 1MB pieces
Network-Coding in DTNs (U)

- Send linear combinations of fragments
- A receiver can collect **any** ten pieces and recover the data
Security in DTNs (U)
Security Threats (U)

- (TS//SI//REL) Protecting against rogue bundles being injected into the network
- (TS//SI//REL) Prevent an adversary from modifying legitimate bundles
- (S//REL) Protection against eavesdroppers
- (S//REL) Authenticate neighbors before establishing links
- (TS//SI//REL) Low Probability of Detection / Intercept
Bundle Security Protocol RFC 6257 (U)

- (U) Provides bundle-layer encryption, authentication, and data integrity
- (U) Lack of connectivity affects choice of algorithms and services
- (U) Security polices may be directional
- (U//FOUO) Managing keys and their accompanying policies is a challenge
Bundle Authentication (U)

- (U) Hop-by-hop Authentication
- (U) Requires each device to generate a shared secret with each of its neighbors
- (U//FOUO) Establishing these keys is a challenge
Bundle Authentication (U)

- (U//FOUO) End-to-end authentication
  - RSA digital signatures
- (U) Intermediate nodes can verify the signature
- (U) Cannot assume connectivity to an external Certificate Authority
- (U) For signatures, the certificate can be appended to the message
Bundle Encryption (U)

- (U//FOUO) Payload data encrypted with AES in Galois Counter Mode (GCM)
- (U) Provides data integrity
- (U) AES key is encrypted with the destination’s RSA public key
Key Management Issues (U)

- (U) How to distribute public keys securely
- (U//FOUO) One option: pass certificates between devices
- (U//FOUO) Another option: pre-placing certificates
  - Memory issues
- (U) Revoking keys of compromised devices
Link-Layer Security (U)

- (U//FOUO) Even with BSP, CL is wide open
- (U//FOUO) Develop a mechanism to authenticate neighbors before allowing them to connect
  - Enables dropping unwanted bundles
  - May prevent DoS through too many connections
- (U//FOUO) Enable different groups of nodes to operate in the same area but maintain separation
Link-Layer Security (U)

- (U) Constraints
  - Lightweight
  - Low setup latency
  - Limited bandwidth consumption
  - Minimal provisioning/maintenance
  - Compatible with short session durations
Covert Discovery (S//REL)

- (TS//SI//REL) Have set up external triggers for establishing DTN links
- (S//REL) Similar work being done outside to reduce power consumption
- (U) Example: Bluetooth beacons triggering a wifi connection
- (S//REL) Another option: use our own radios for some hops
Surveillance-oriented Demo (U)
Data sources at “secret” locations on campus. Queue up or generate data.
Mobile data generator in a car sending segments of audio
Pedestrian relays walk around, and pick up data from source nodes.
Car Players are typical data ferries. They relay data to the destination.
Questions?