Moving Data Through Disconnected Networks

Delay-Tolerant Networking and the IC (U//FOUO)

[redacted] R4 (
R4 (
R4 [redacted]

June 2012

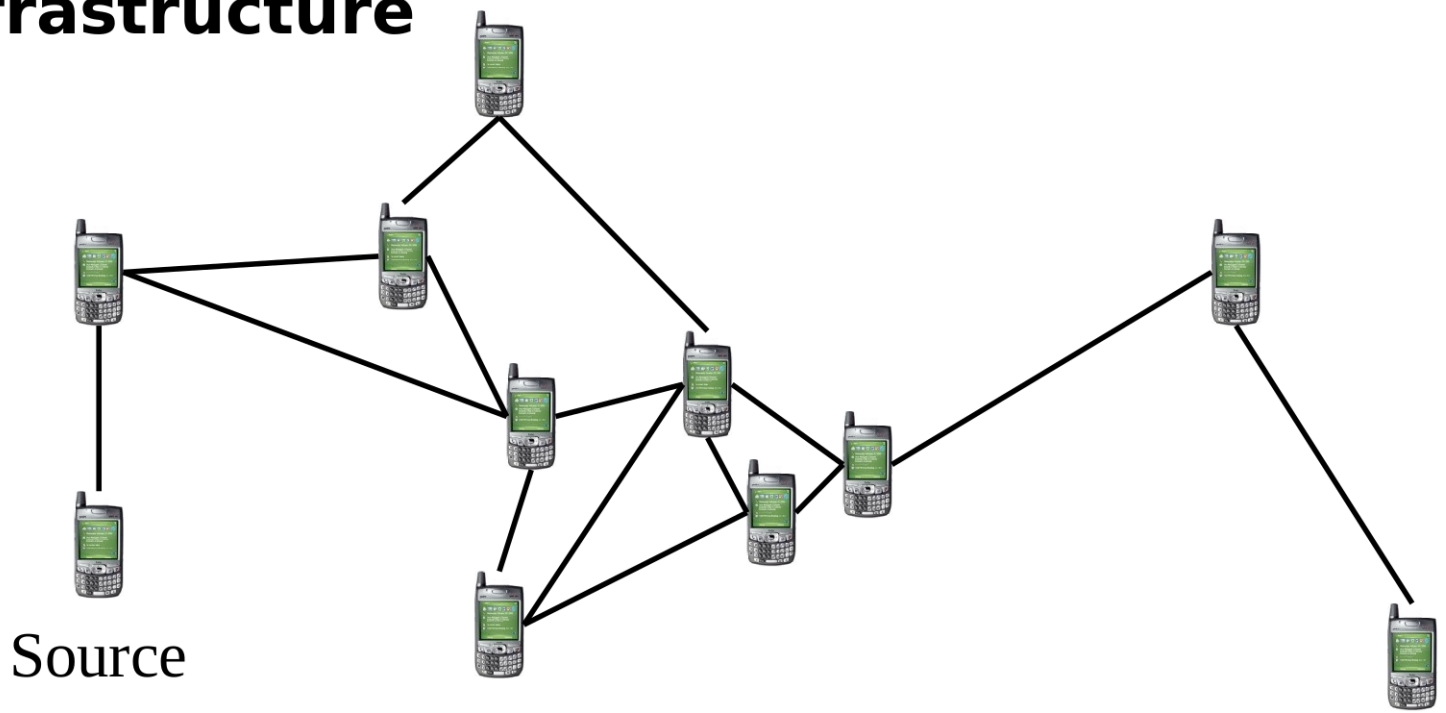
The overall classification of this briefing is:
TOP SECRET//COMINT//REL TO USA, FVEY

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

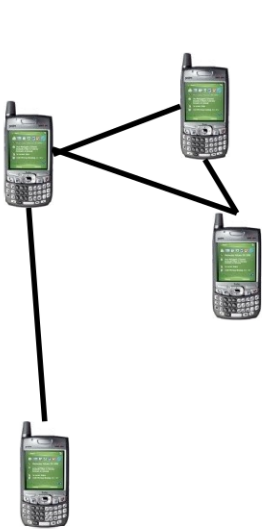
Mobile Ad-Hoc Networks (U)

- **(U//FOUO) A wireless network with no infrastructure**

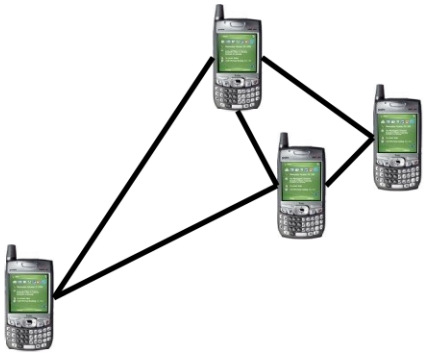


Intermittently Connected Network (U)

- **(U//FOUO) Many wireless networks will not have end-to-end connectivity**



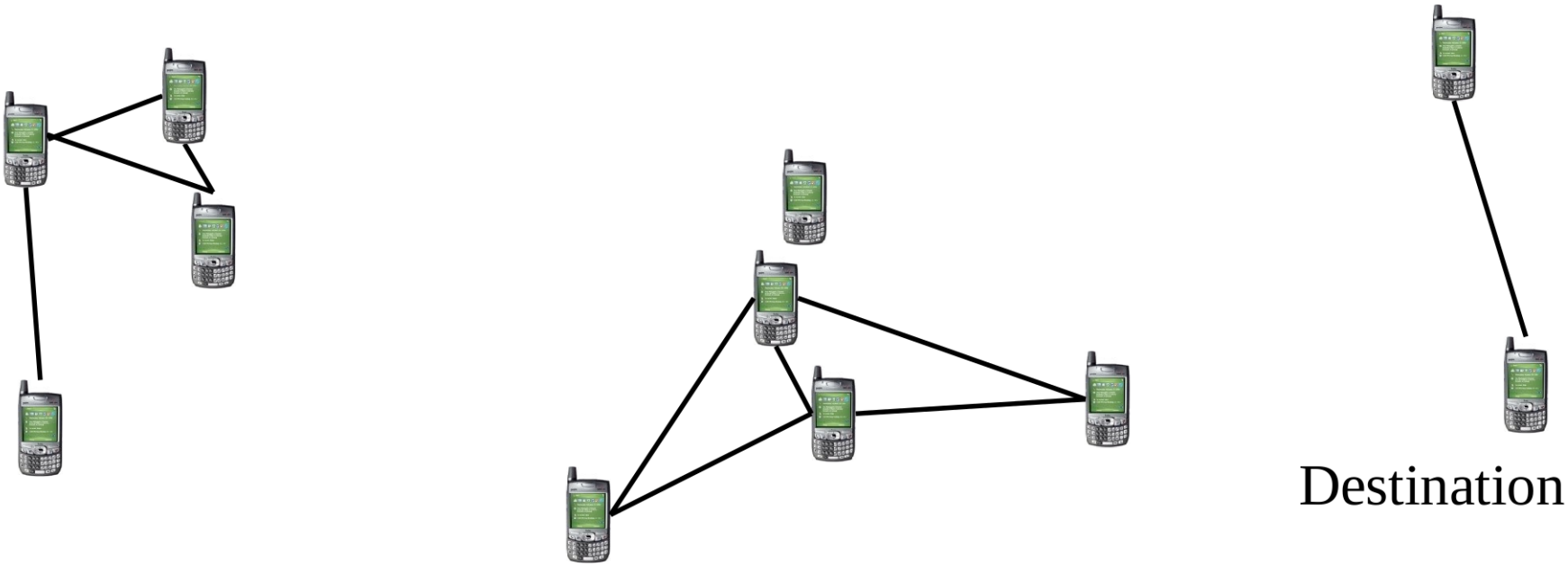
Source



Destination

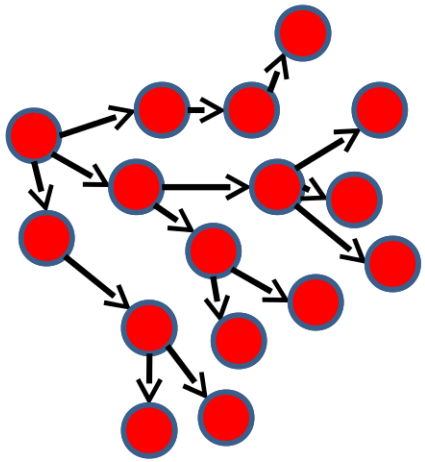
Delay-Tolerant Networks (U)

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



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

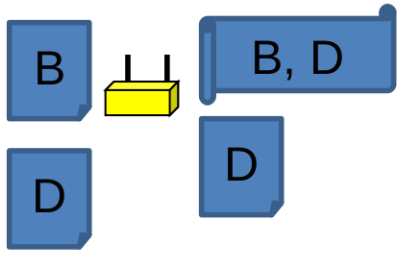
2003: A DTN Architecture for Challenged Internets
Kevin Fall

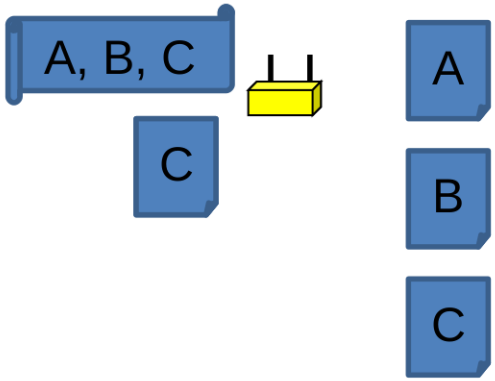
2003: DataMULEs
Shah, Roy, Jain, Brunette

2003: Probabilistic Routing in Intermittently Connected Networks
Lindgren, Doria, Schelen

Beginnings of DTN: Epidemic (U)

- 2000: Epidemic Routing - Vahdat and Becker





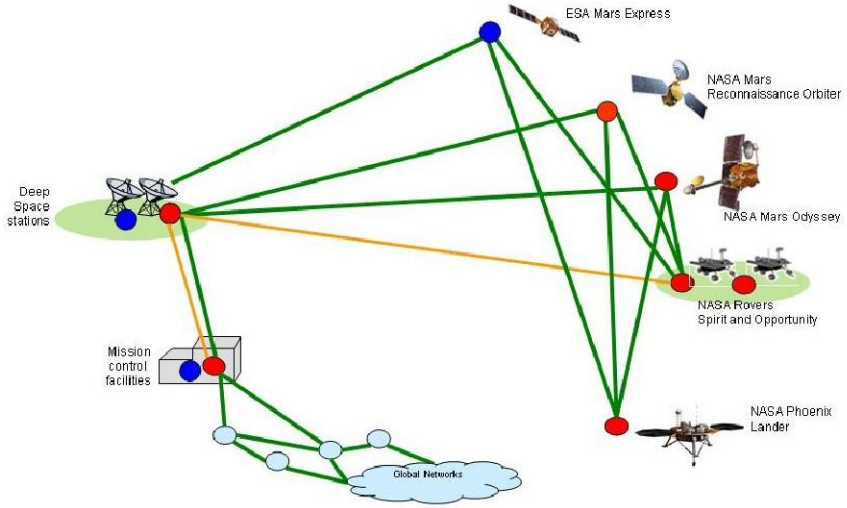
- Nodes exchange "summary vectors"
- Each node sends the data that the other node lacks
- Summary vectors implemented as a Bloom Filter
- Followed by Immunity concept: *Resource and performance tradeoffs in delay-tolerant wireless networks*, 2005; Small and Haas

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)

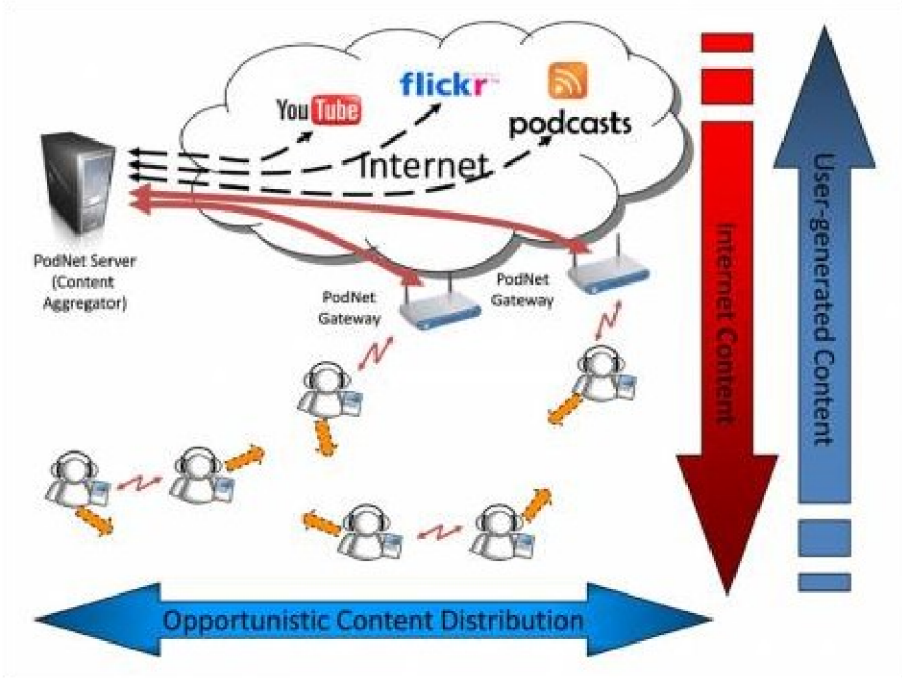
- *Data MULEs: modeling a three-tier architecture for sparse sensor networks*
- 2003 Paper by R. C. Shah, S. Roy, S. Jain, W. Brunette
- Has mobile MULEs relaying data from sensors to well-connected Access Points
- Similar: *A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks*, 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)

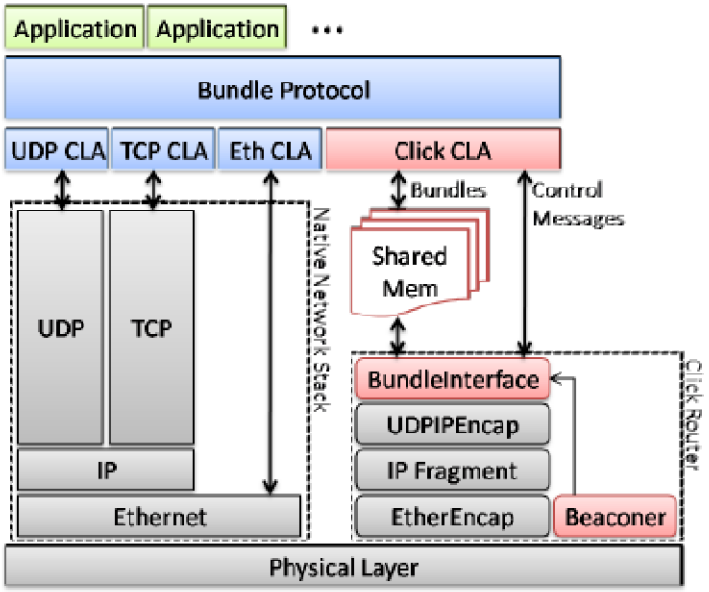
- Content dissemination
  - [*PodNet*, 2006 – Present; Legendre, Lenders, May, Karlsson]
  - Haggle Project
- Social Networking
- Distributed Sotrage
  - [*TierStore*, 2008; Demmer, Du, Brewer]
  - [*DTN-based Content Storage and Retrieval*; Ott, Pitkanen]



- Cellular Traffic Offloading
  - [Cellular Traffic Offloading through Opportunistic Communications: A Case Study, 2010; Han, Hiu et al]

Standardization Activities* (U)

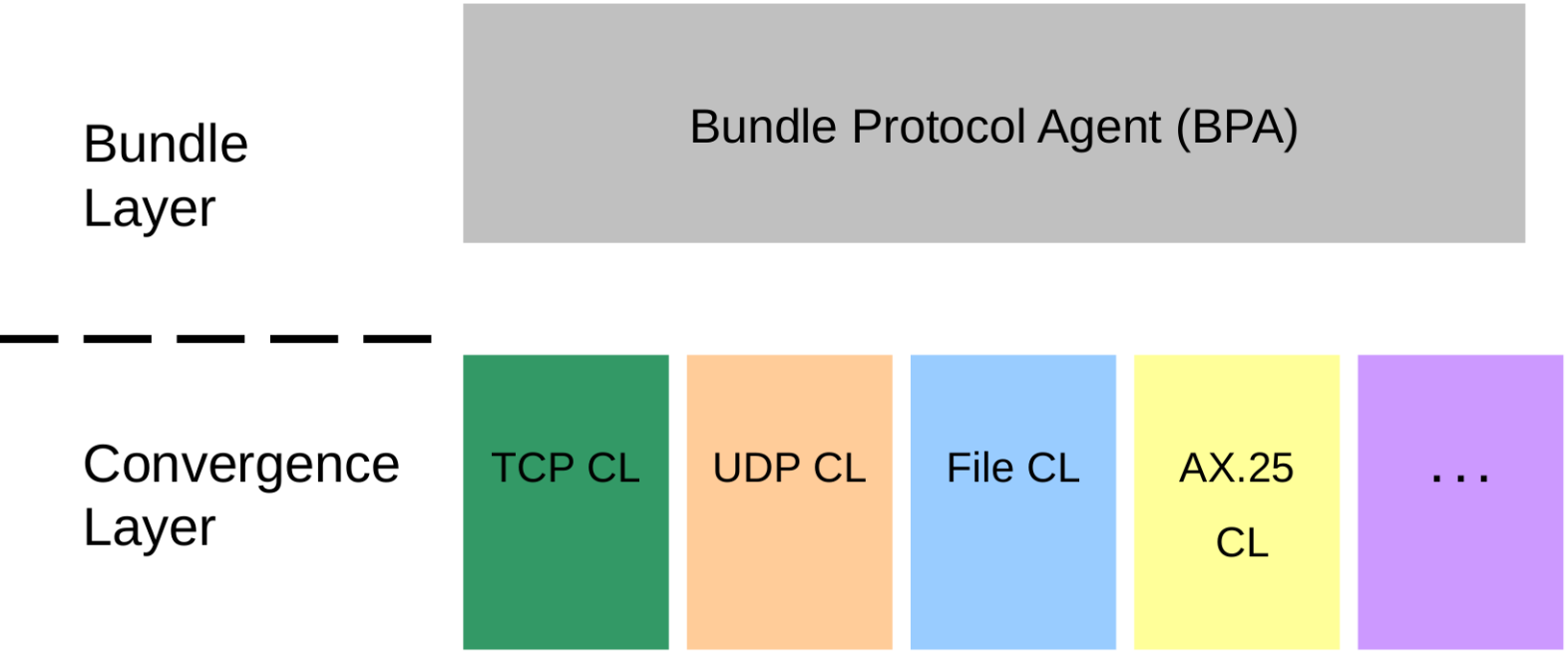
- DTNRG has been part of the IRTF since (at least) 2002
- RFC 5050 defines the Bundle Protocol
- Application-layer overlay that moves “bundles” of data
- Convergence Layers move bundles over different networks



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 Stack Landscape

Vapor

Aalto
Java stack

Cisco
Java stack

GA Tech
C# stack

iPhone
TCPCL

SPINDLE

pydtn

Bytewalla

ION

IBR-DTN

dtns60

DTN2 Reference
Implementation

Real

Bundle Protocol Stack Landscape

Vapor

(TS//SI//REL)
FUZZYLINT
Lightweight
BPA

Aalto
Java stack

Cisco
Java stack

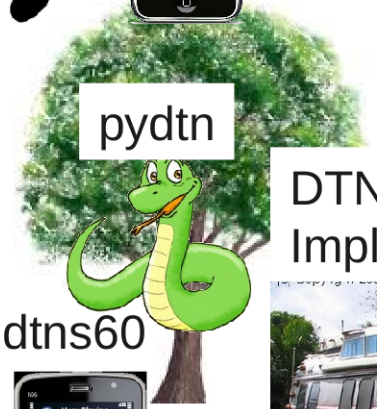
CISCO

GA Tech
C# stack

iPhone
TCPCL

SPINDLE

pydtn



Bytewalla

IBR-DTN

dtns60

DTN2 Reference
Implementation

Real

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.

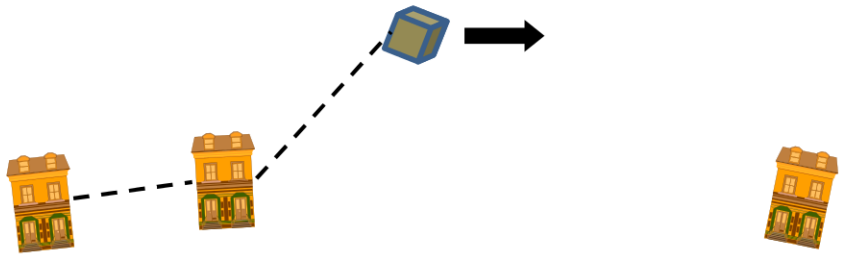
Close Access (TS//SI//REL)

- (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

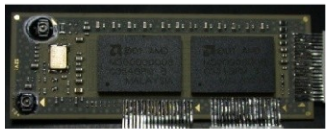


Crowd Sourcing (U)

- (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 RAPTORGALAXY



Summary of IC applications (U//FOUO)

CovComm	Close Access	NRO CubeSat Comms	Crowd-Sourcing	Tagging Tracking & Locating
Unattributable	Data exfiltration from isolated networks and denied areas	Comms between ground stations that only have occasional satellite coverage	Provide data flow in and out of closed nations	Very small hardware
COTS handsets				Record locations and encounters
Open-source	TSV field test	Use inexpensive CubeSat platform	Ambitious BIG idea	
			Proposed CONOP can be done *now*	Use DTN to migrate data back to collection points
			Proposed internally and externally	

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

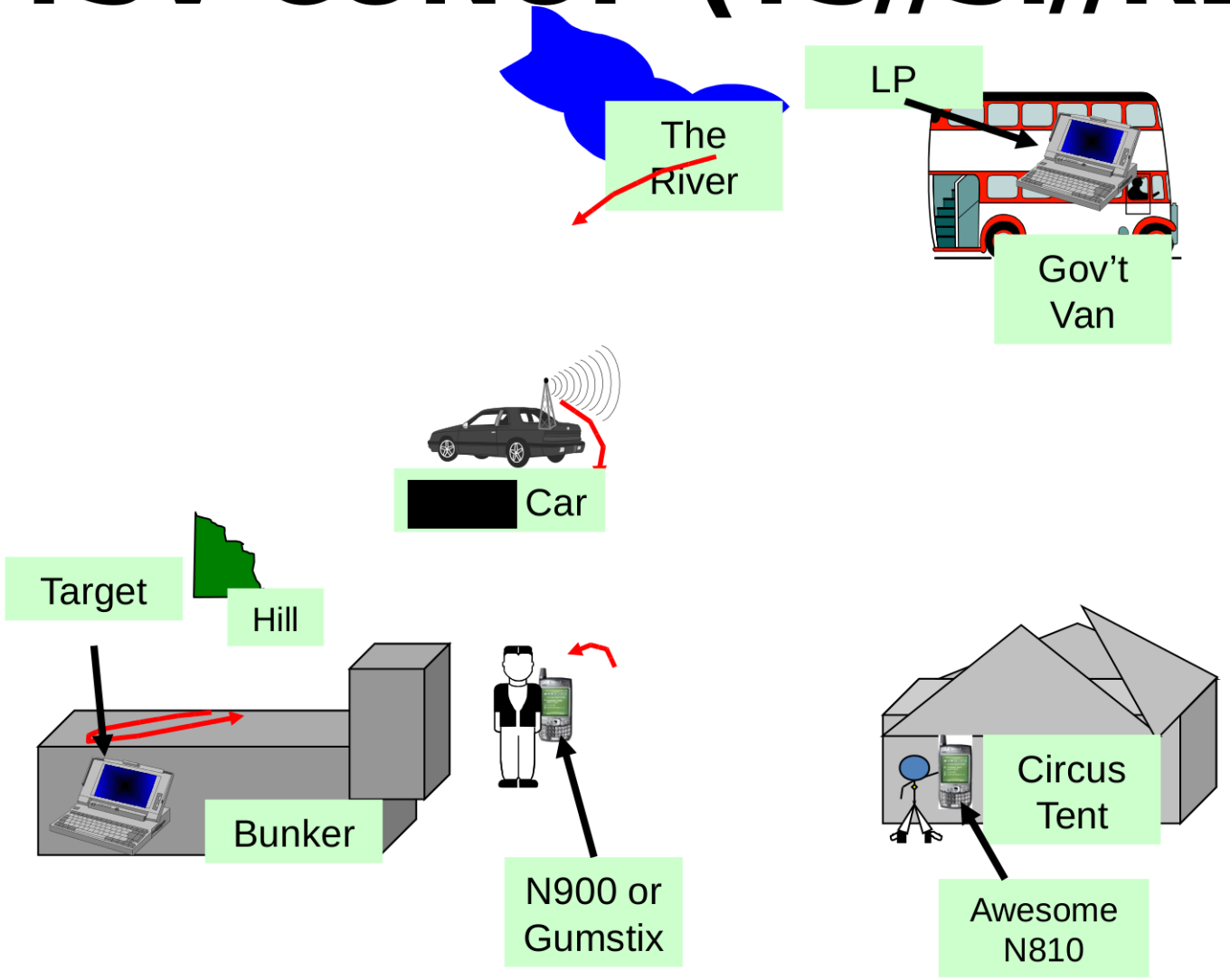
STRAITBIZZARE (U)

- (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

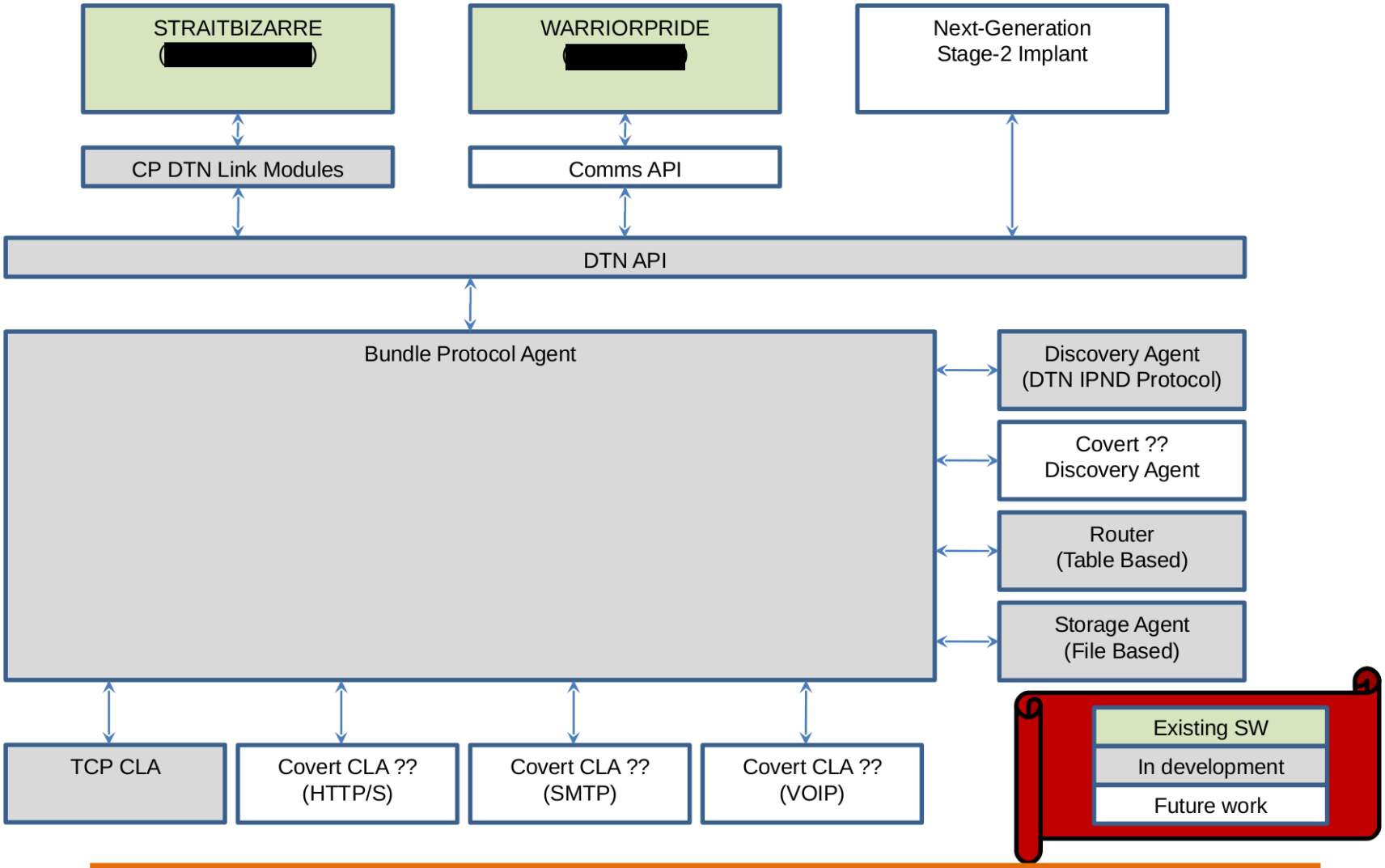
TSV CONOP (TS//SI//REL)



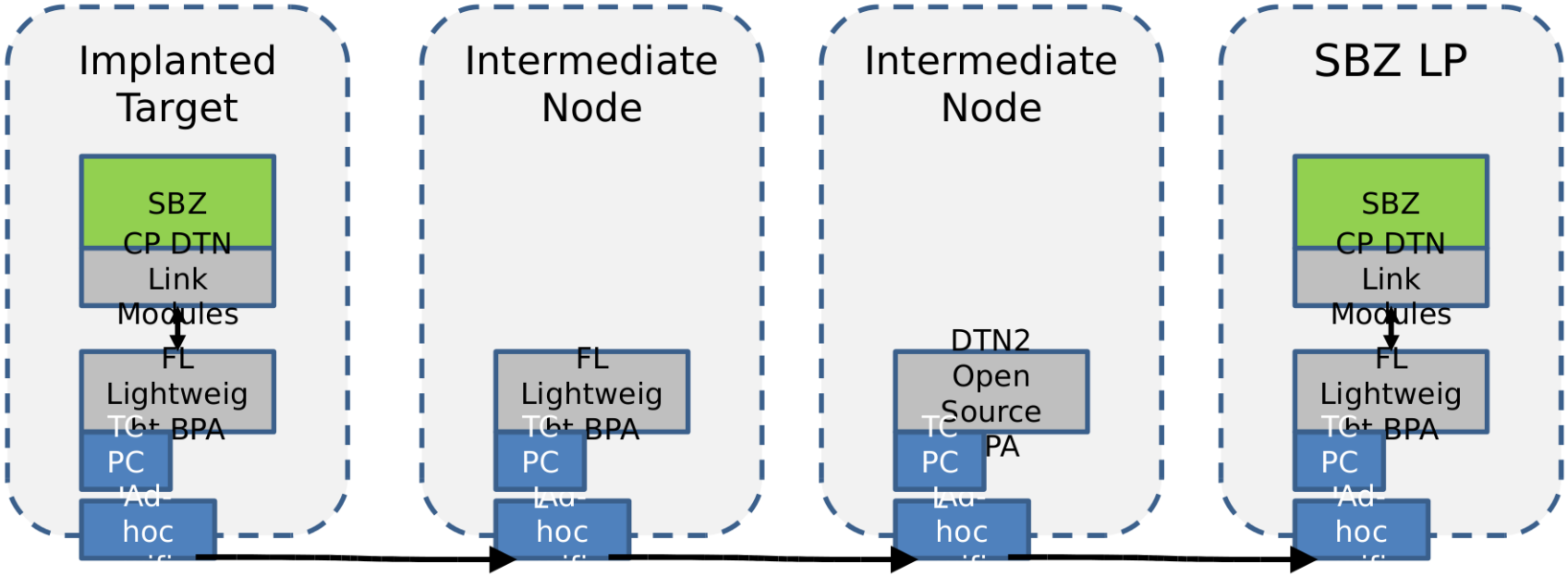
Ultra-lightweight BPA (TS//SI//REL)

- (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

TAO-Specific DTN Stack (TS//SI//REL)



TSV CONOP (TS//SI//REL)



Platforms and Capabilities (TS//SI//REL)

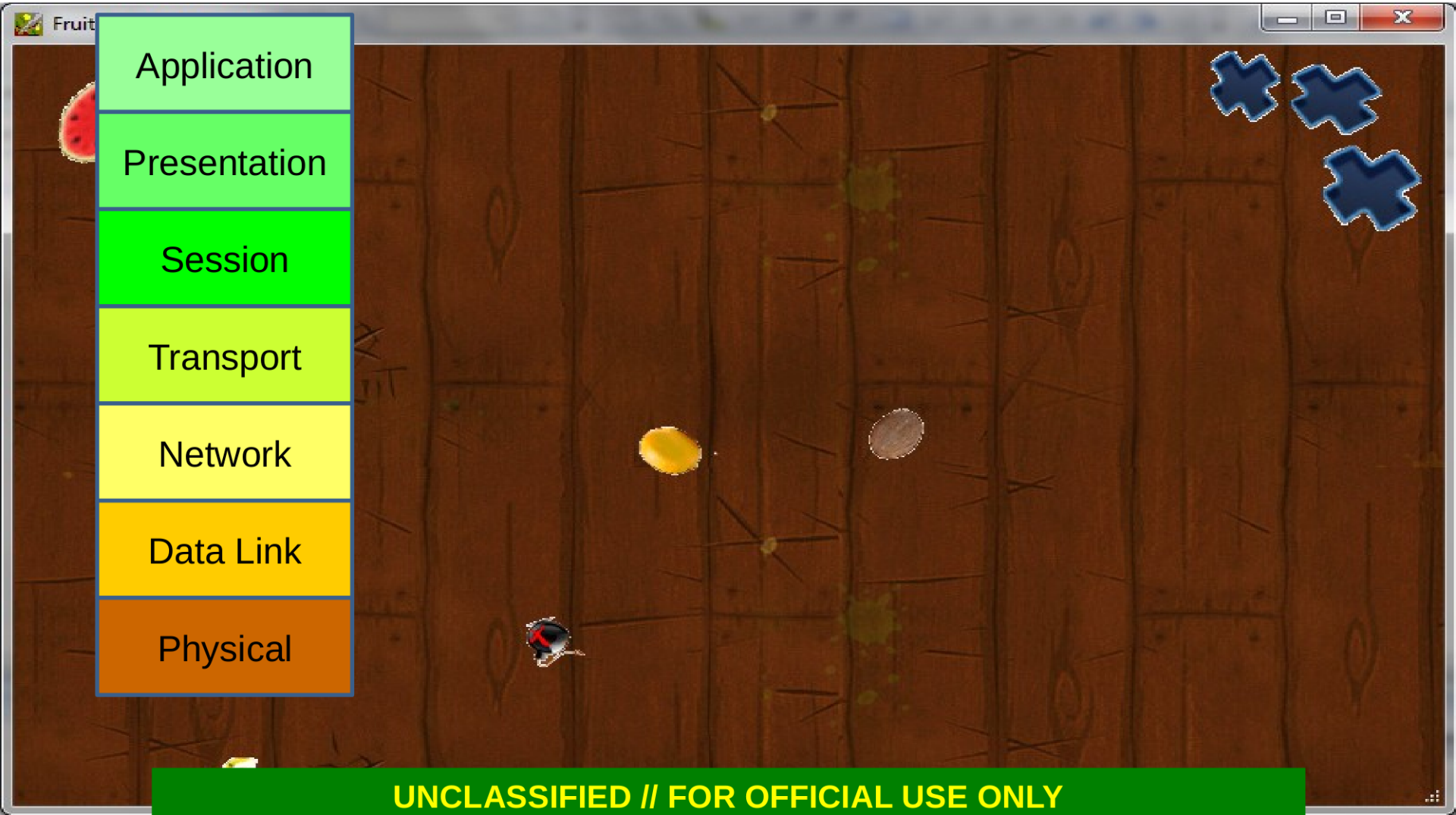
	Linux netbook	Maemo	iPhone	Gumstix	Android	Windows and Java
DTN2						
IBR-DTN						
FUZZYLINT						

Current Effort

Wireless testbeds (U//FOUO)

Reality Ninja (U//FOUO)

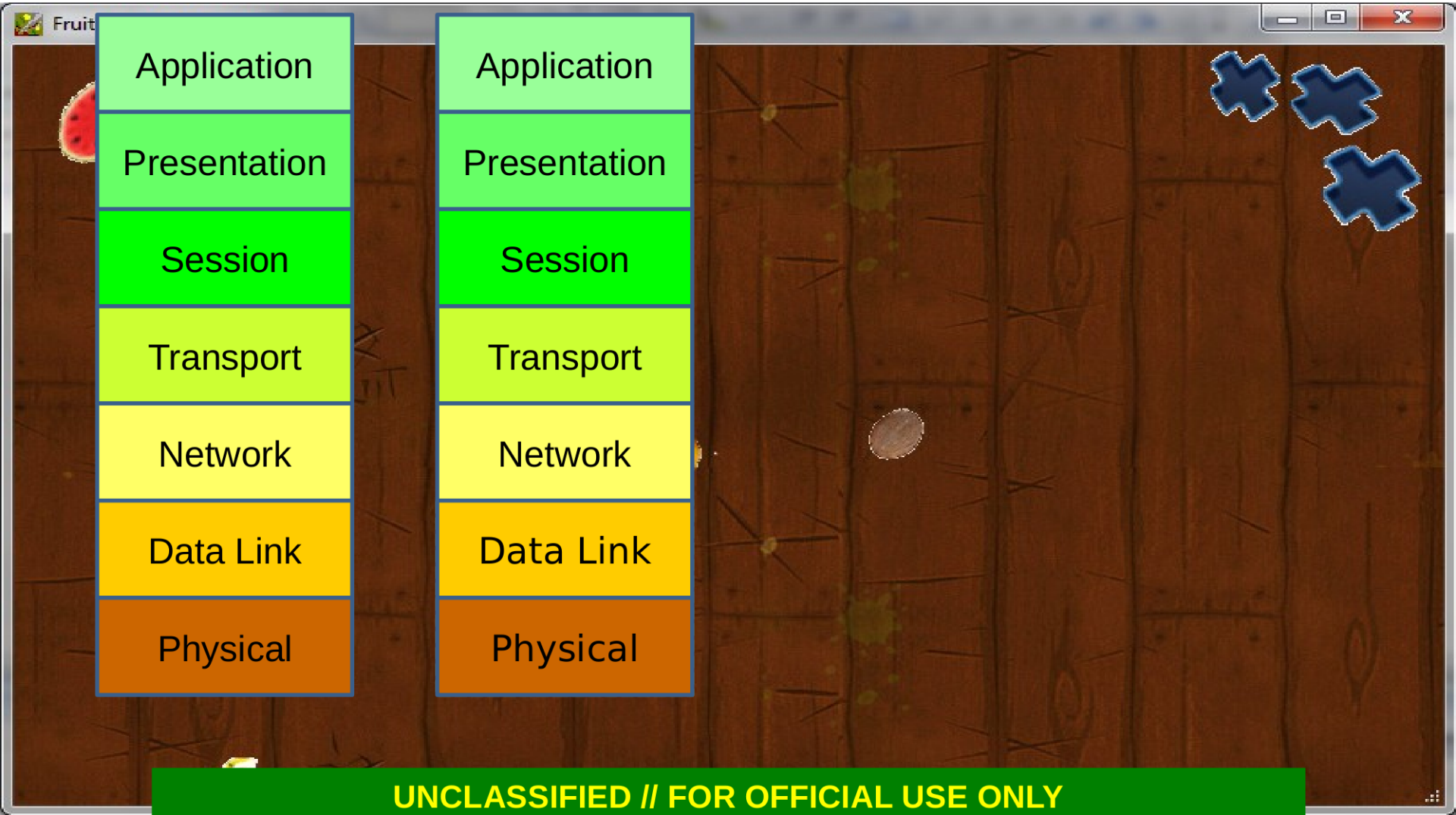
Reality



Reality Ninja (U//FOUO)

Reality

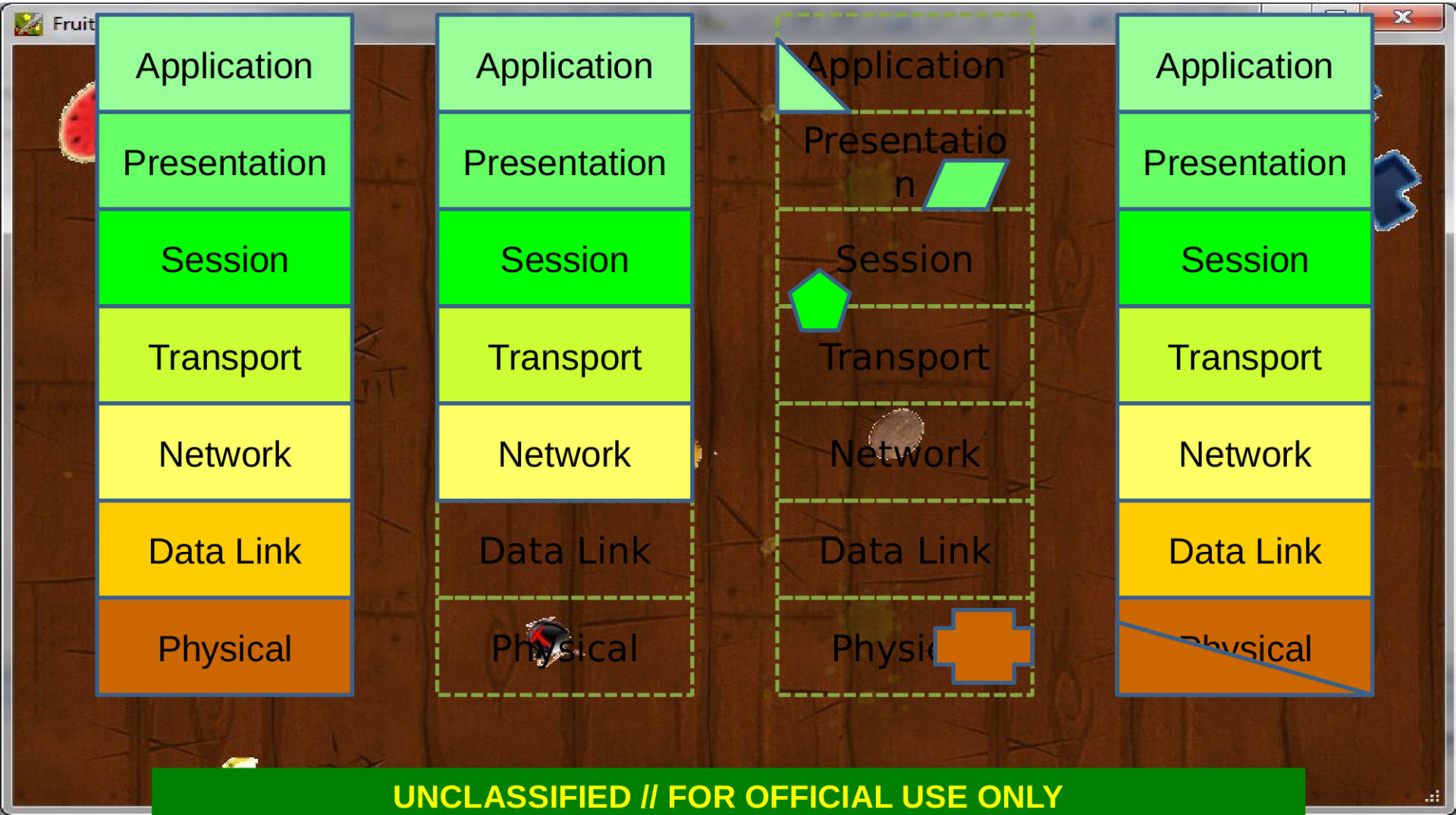
Network Emulators



Reality Ninja (U//FOUO)

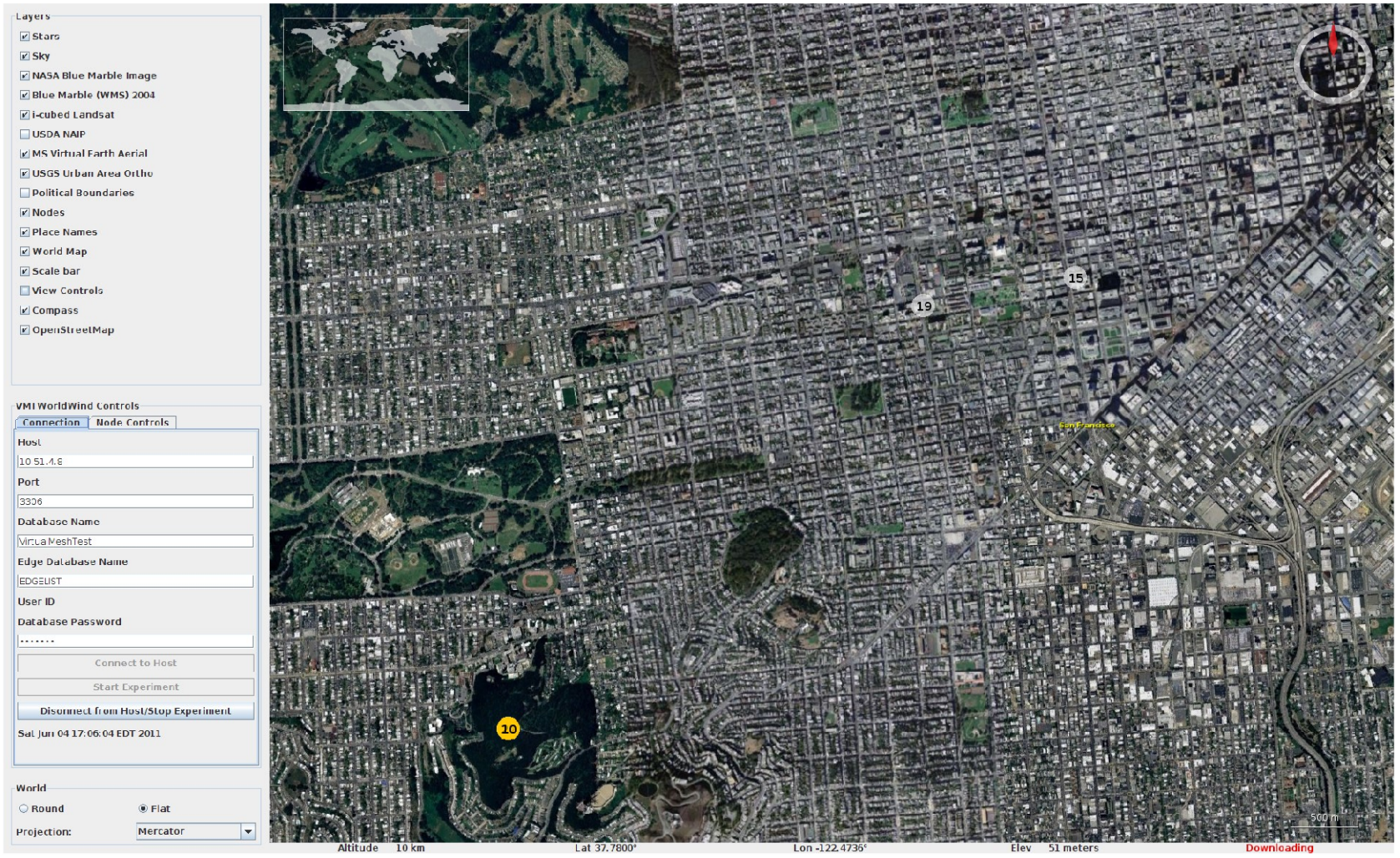
Reality	Network Emulators	Simulation
Application	Application	Application
Presentation	Presentation	Presentation
Session	Session	Session
Transport	Transport	Transport
Network	Network	Network
Data Link	Data Link	Data Link
Physical	Physical	Physical

Reality Ninja (U//FOUO)

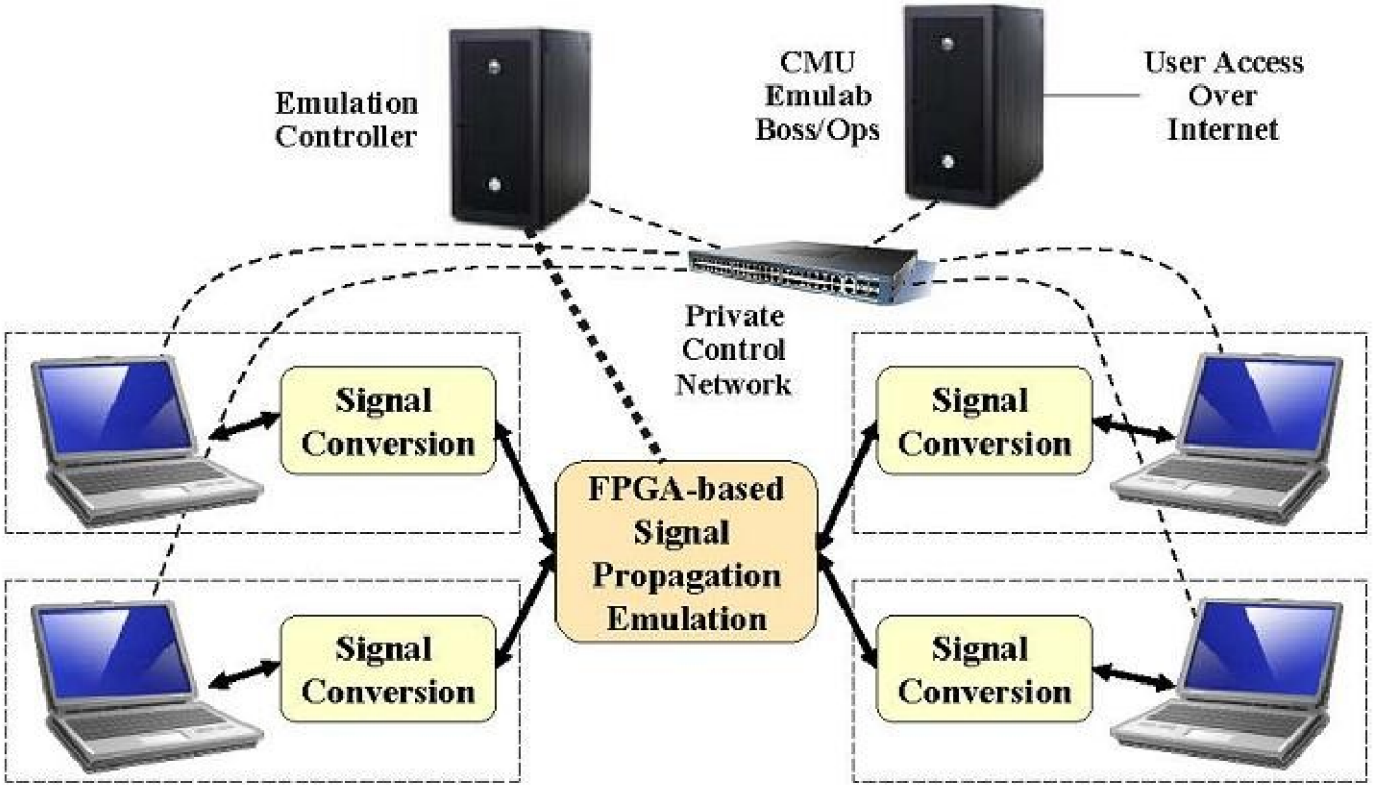


Mobile Wireless Testbed (U//FOUO)

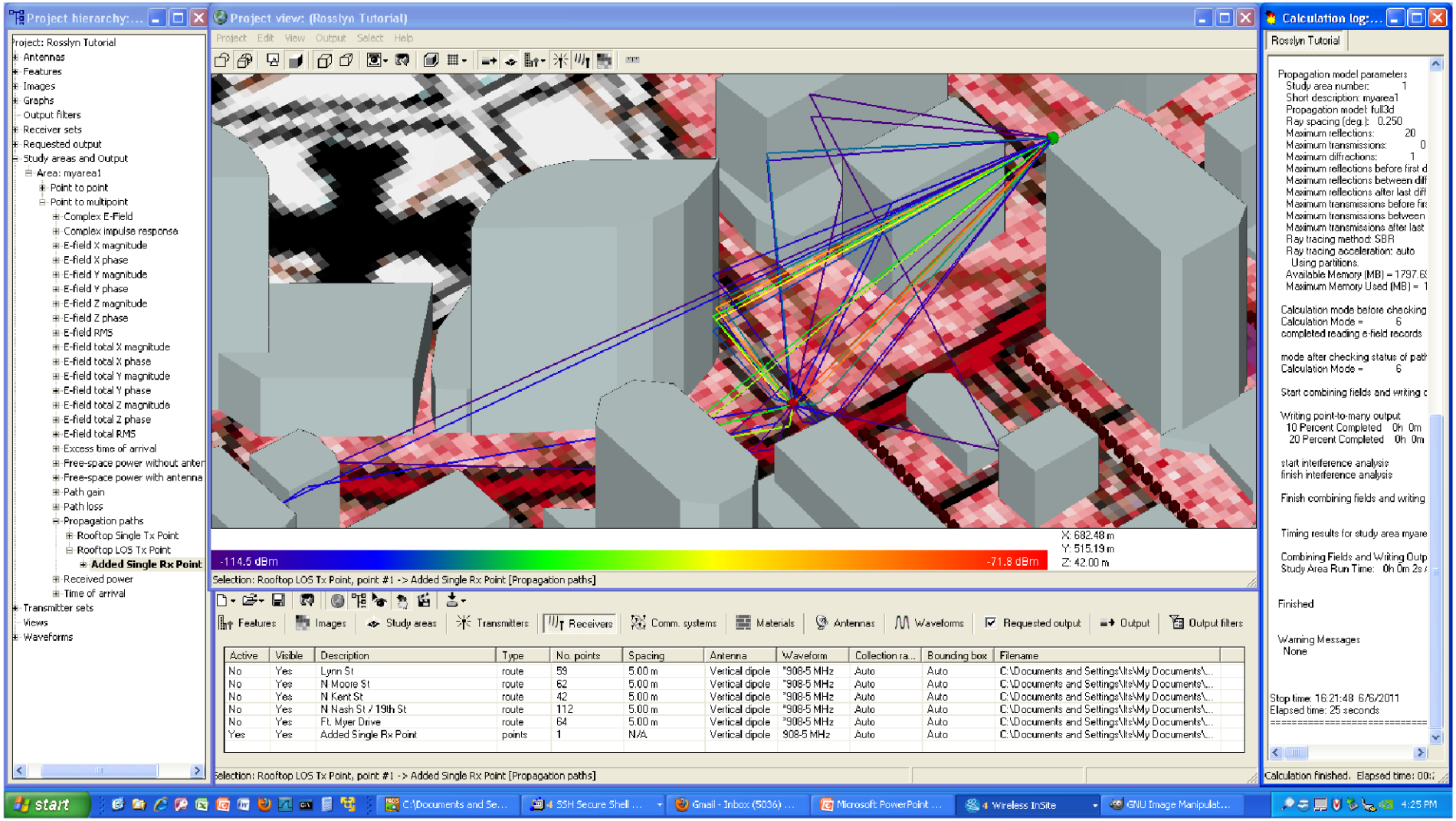
Mobile Wireless Testbed (U//FOUO)



CMU Wireless Emulator (U//FOUO)



Detailed Channel Modeling (U//FOUO)



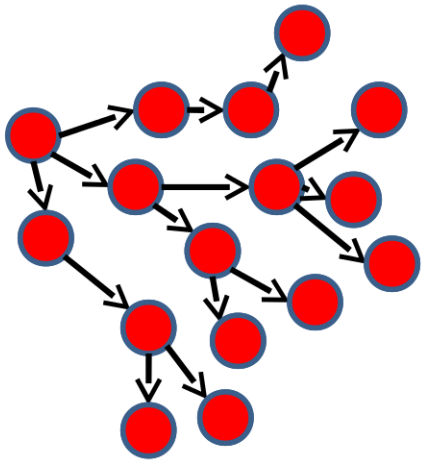
- Routing and Reliability Issues
- Security Issues

Some Interesting Details (U)

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/

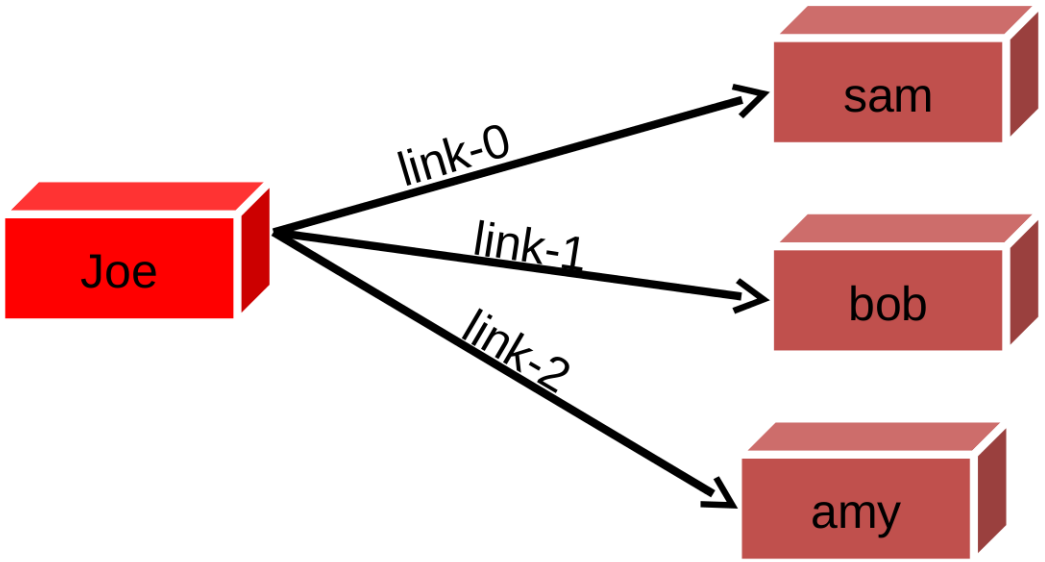
- Convergence Layer connections to neighbors are called “Links”
  - For example a TCP connection to a neighbor is a link

- Each link knows the EID of the neighbor associated with it

Static Routing Tables (U)

One-hop “Direct Delivery”

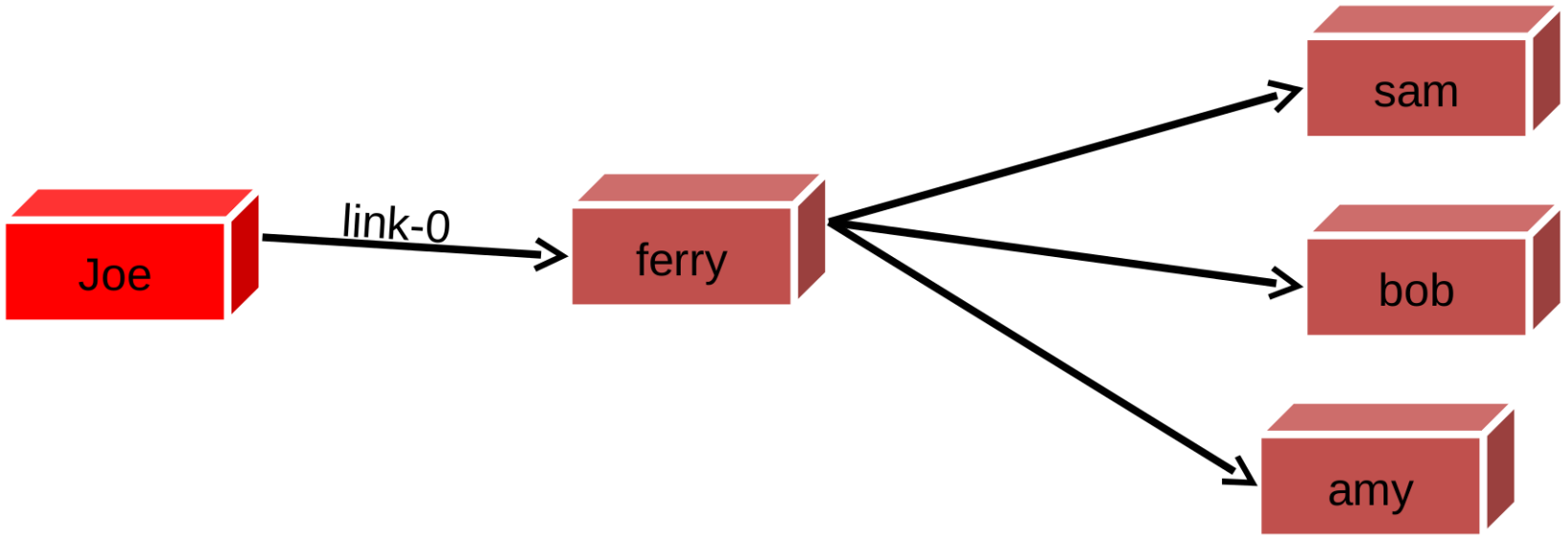
Destination	Next hop	Action
dtn://sam.dtn/	link-0	FWD
dtn://bob.dtn/	link-1	FWD
dtn://amy.dtn/	link-2	FWD



Static Routing Tables (U)

Two-hop “Bundle Ferry”

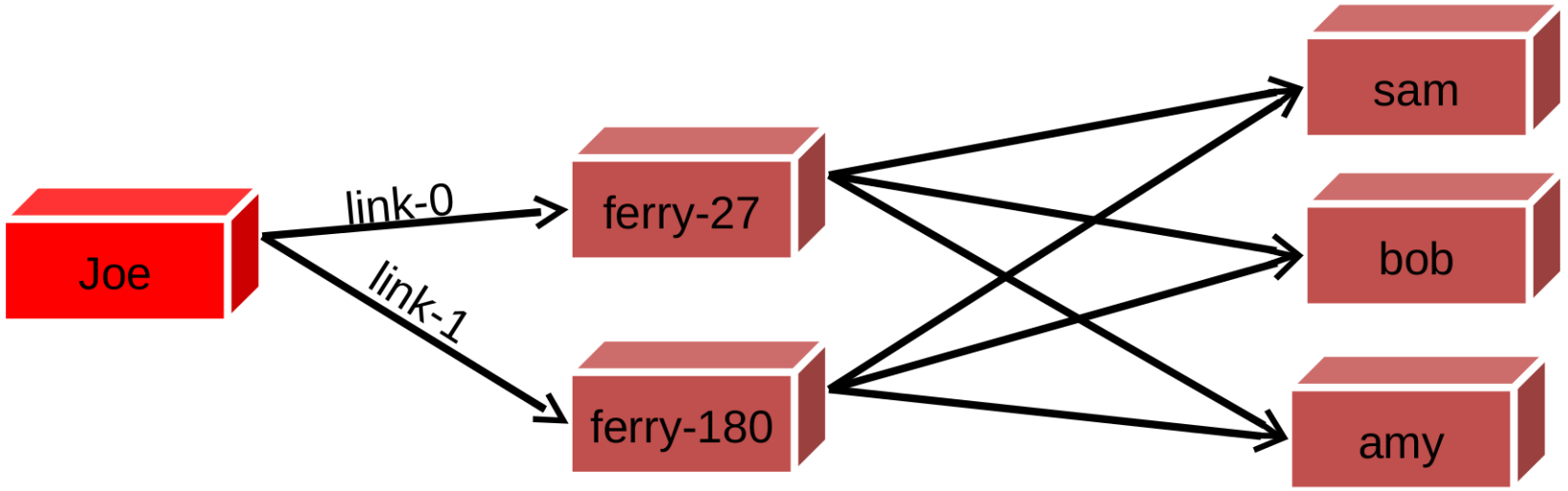
Destination	Next hop	Action
dtn://sam.dtn/	dtn://ferry.dtn/	FWD
dtn://bob.dtn/	dtn://ferry.dtn/	FWD
dtn://amy.dtn/	dtn://ferry.dtn/	FWD
dtn://ferry.dtn/	link-0	FWD



Static Routing Tables (U)

Two-hop “Bundle Ferry” with wildcards

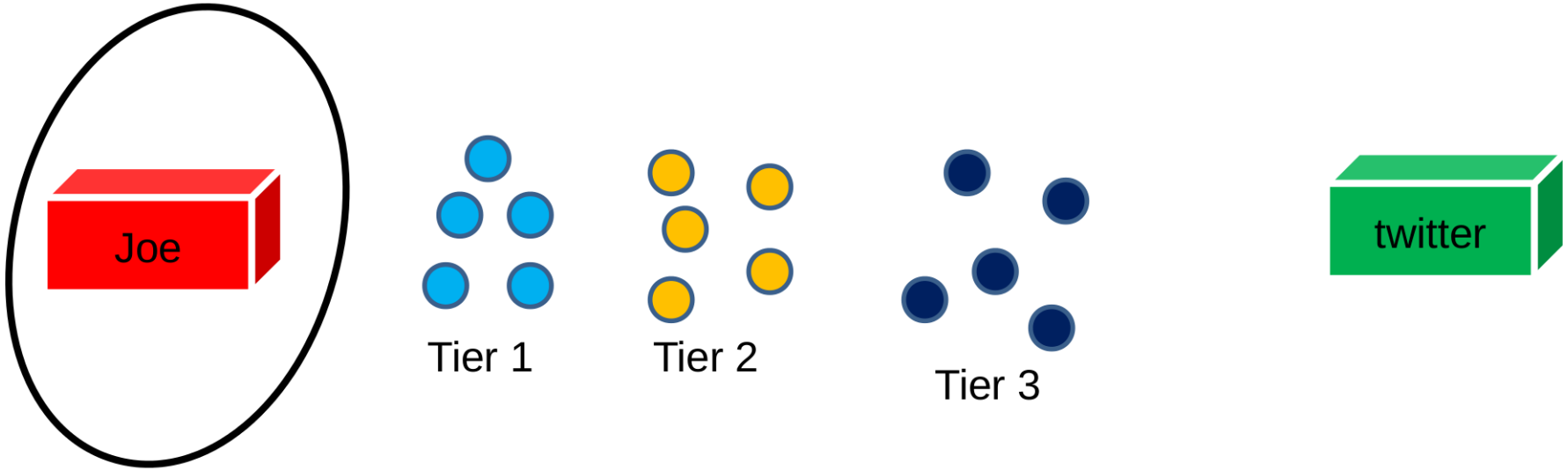
Destination	Next hop	Action
dtn://sam.dtn/	dtn://ferry-*.dtn/	FWD
dtn://bob.dtn/	dtn://ferry-*.dtn/	FWD
dtn://amy.dtn/	dtn://ferry-*.dtn/	FWD
dtn://ferry-27.dtn/	link-0	FWD
dtn://ferry-180.dtn/	link-1	FWD



Static Routing Tables (U)

Multi-hop “Tiered routing”

Destination	Next hop	Action
dtn://twitter.dtn/	dtn://tier1-*.dtn/	FWD
dtn://twitter.dtn/	dtn://tier2-*.dtn/	FWD
dtn://twitter.dtn/	dtn://tier3-*.dtn/	FWD
dtn://twitter.dtn/	link-0	FWD



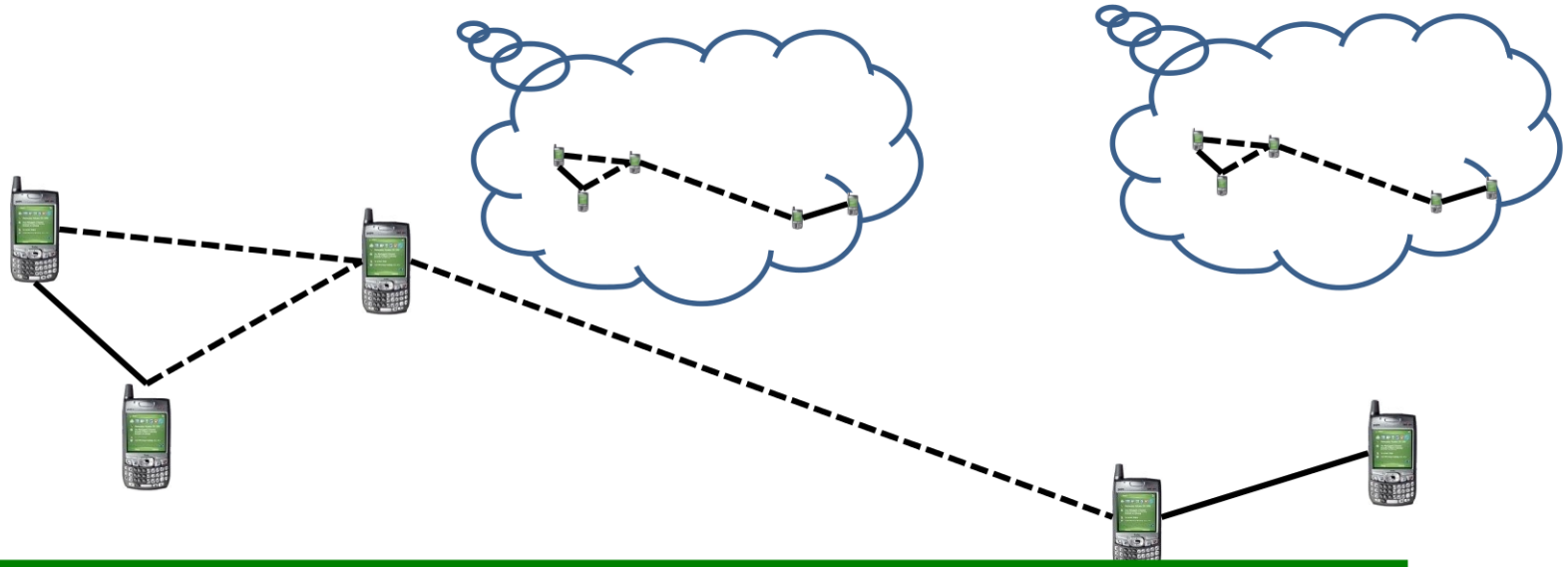
DTN Routing Bonanza (U)

- (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”

Static
Flooding
Static with copy links
Neighborhood
Epidemic
Endemic
Epidemic with Immunity
mphone
TIERStore
DTLSR
Simple Gossiping

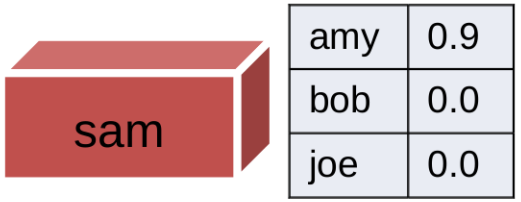
DTLSR (U)

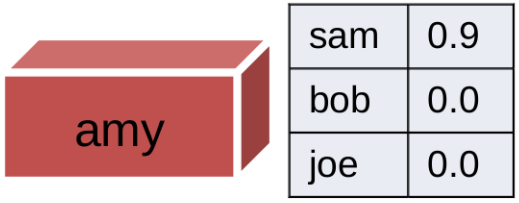
- (U//FOUO) Delay-Tolerant Link State Routing
  - Assumes a mostly stable contact graph
  - Nodes all flood their recent contacts
  - Each node maintains an internal picture of the network, and makes routing decisions based on Dijkstra's alg



"Intelligent" Routing: PRoPHET (U)

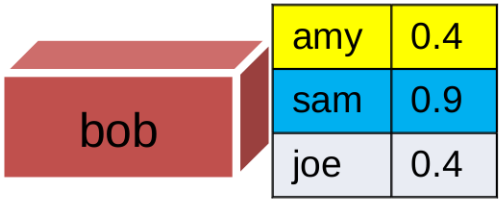
- *Probabilistic routing in intermittently connected networks*, 2003; A. Lindgren, A. Doria, and O. Scheln
- Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET)

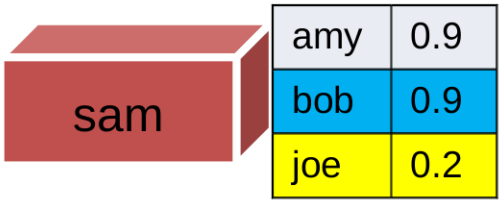


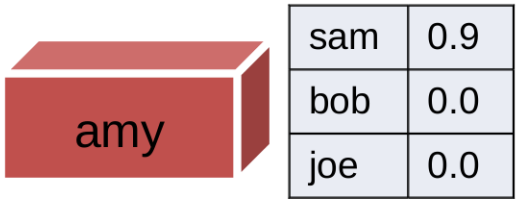


"Intelligent" Routing: PRoPHET (U)

- *Probabilistic routing in intermittently connected networks*, 2003; A. Lindgren, A. Doria, and O. Scheln
- Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET)





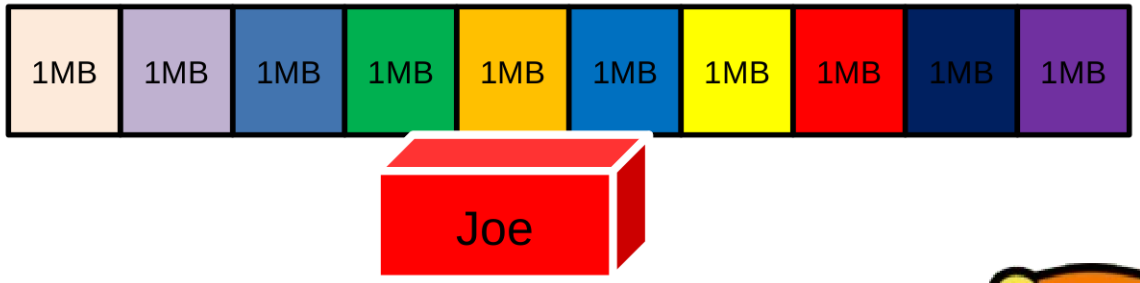


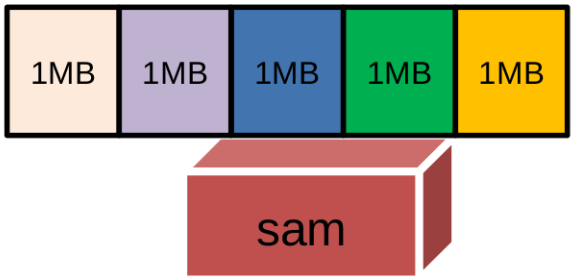
Network-Coding in DTNs (U)

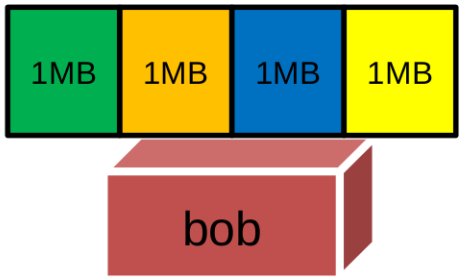
- Imagine trying to distribute a 100MB bundle in a DTN
- Idea:

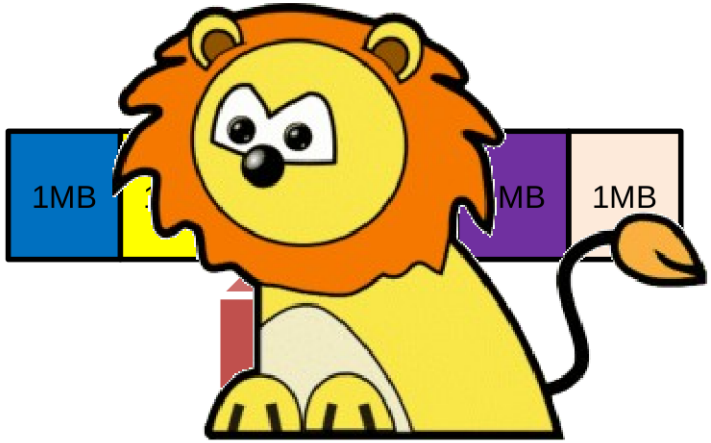
Network-Coding in DTNs (U)

- Imagine trying to distribute a 100MB bundle in a DTN
- Idea: fragment into 1MB pieces



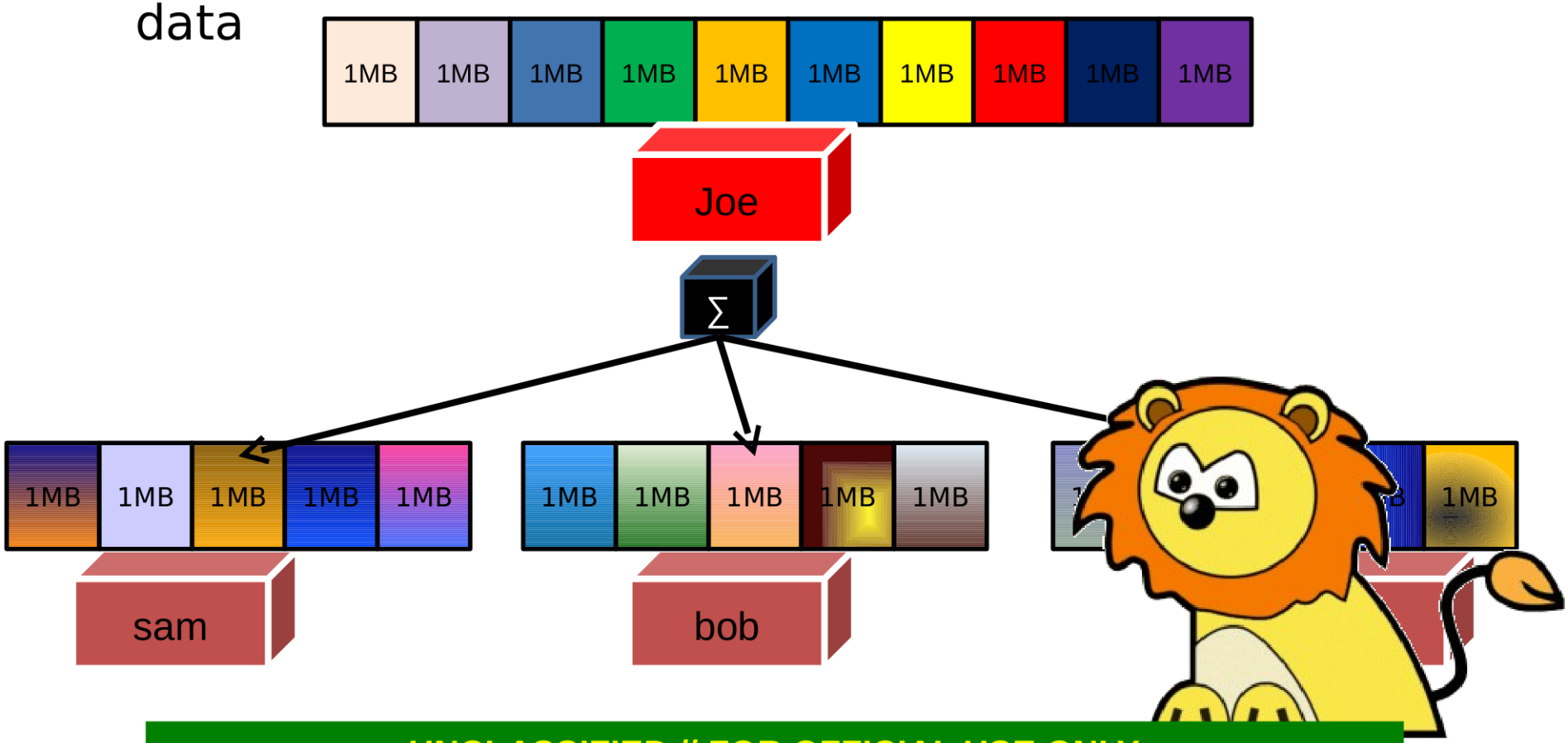






Network-Coding in DTNs (U)

- 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)

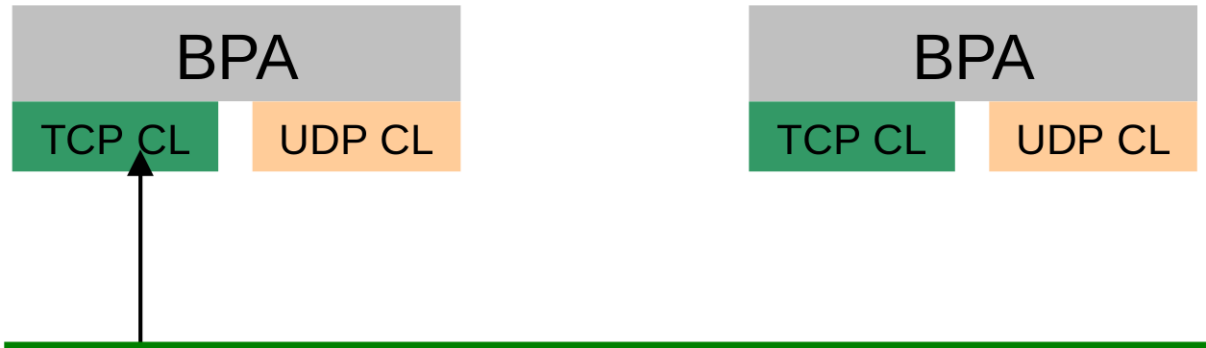
- (U//FOUO) Payload data encrypted with AES in Galois Counter Mode (GCM)
- (U) Provides data integrity
- (U) AES key is encrypted with the destination's RSA public key

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



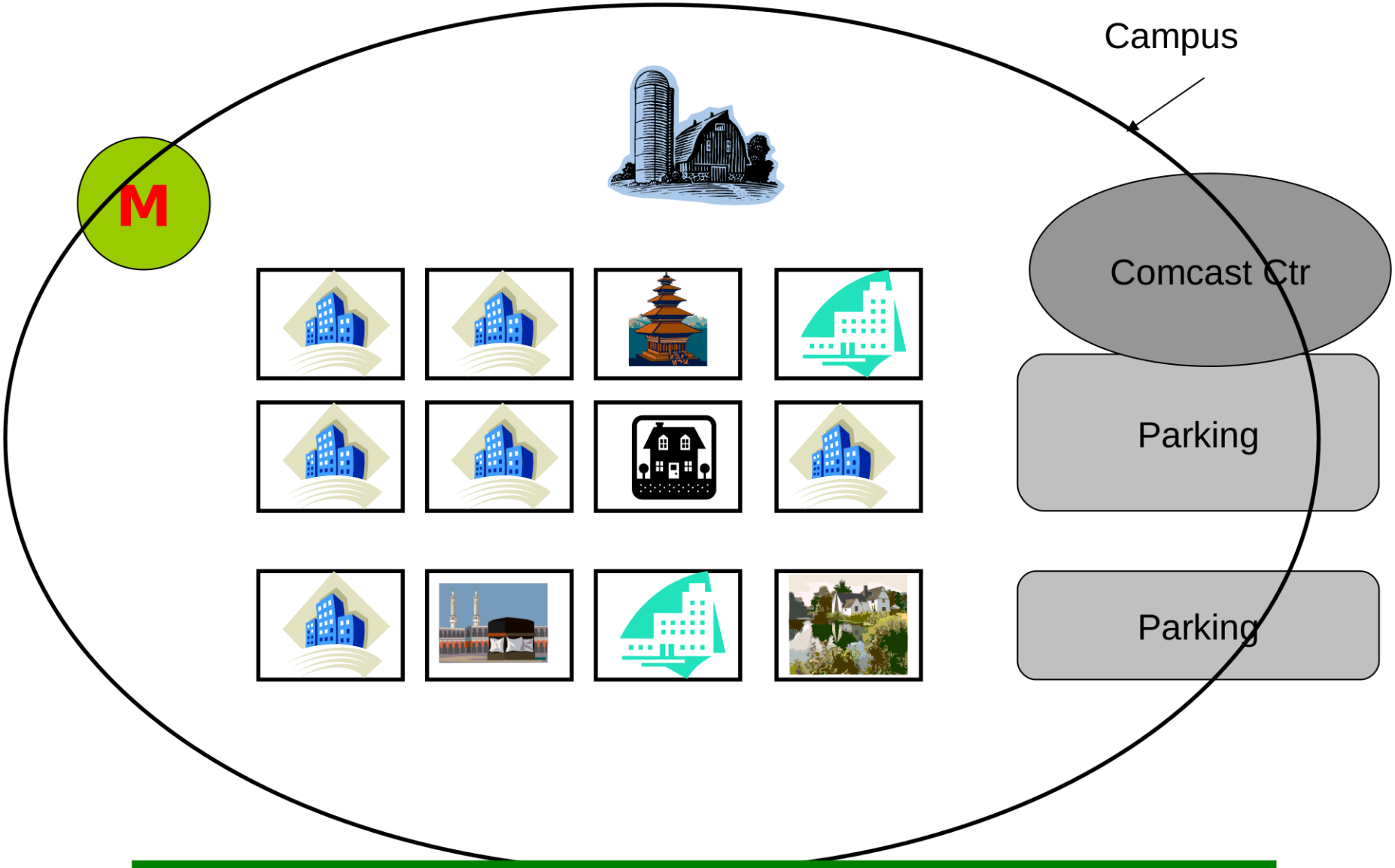
Link-Layer Security (U)

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

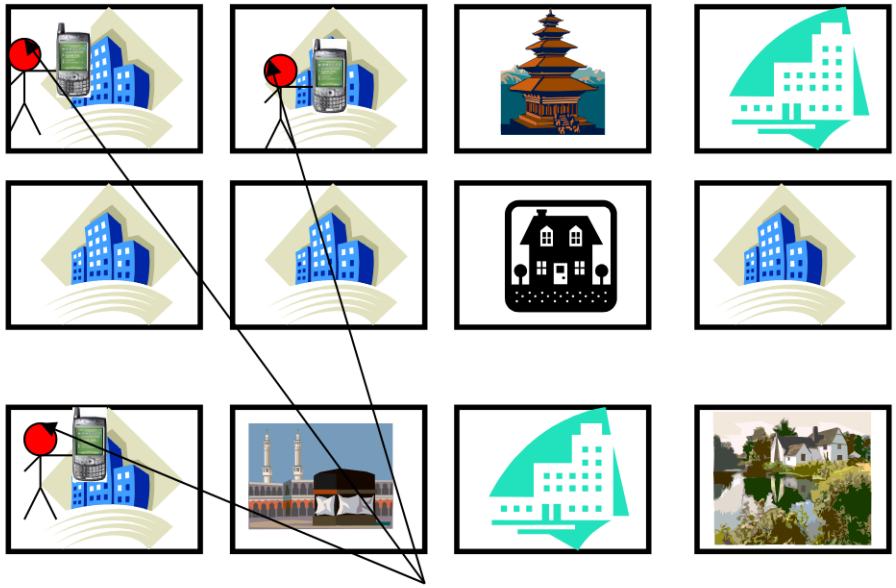
Covert Discovery (S//REL)

- (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)


Campus
M
Comcast Ctr
Parking
Parking

M



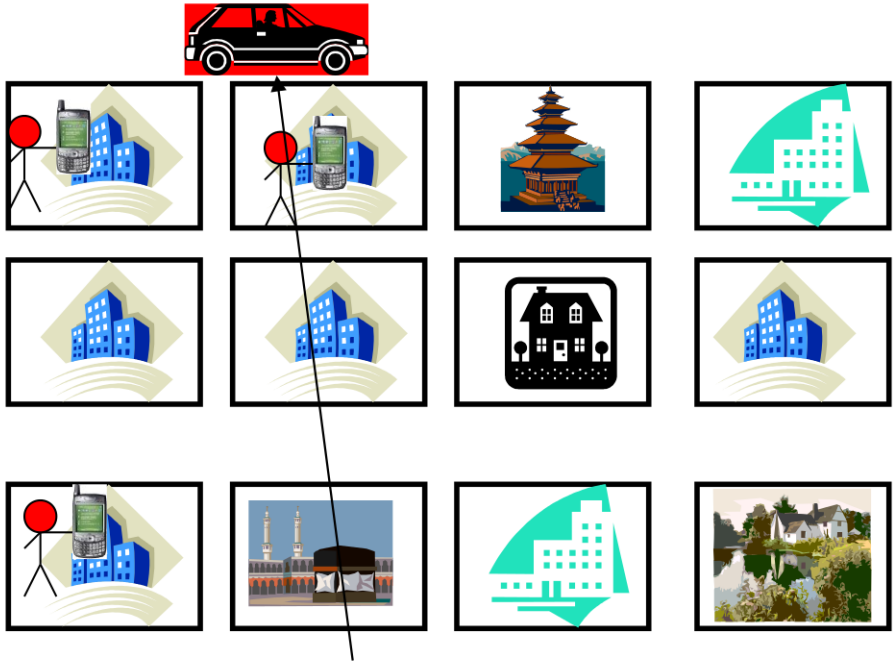
Comcast Ctr

Parking

Parking

Data sources at “secret” locations on campus. Queue up or generate data.

M

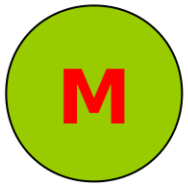


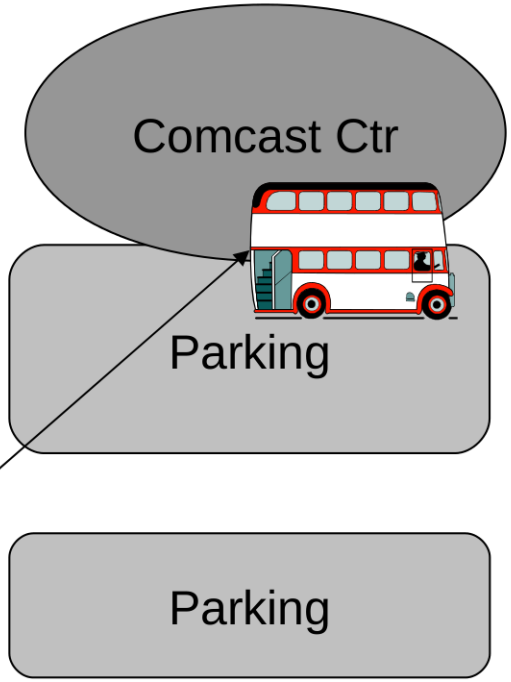
Comcast Ctr

Parking

Parking

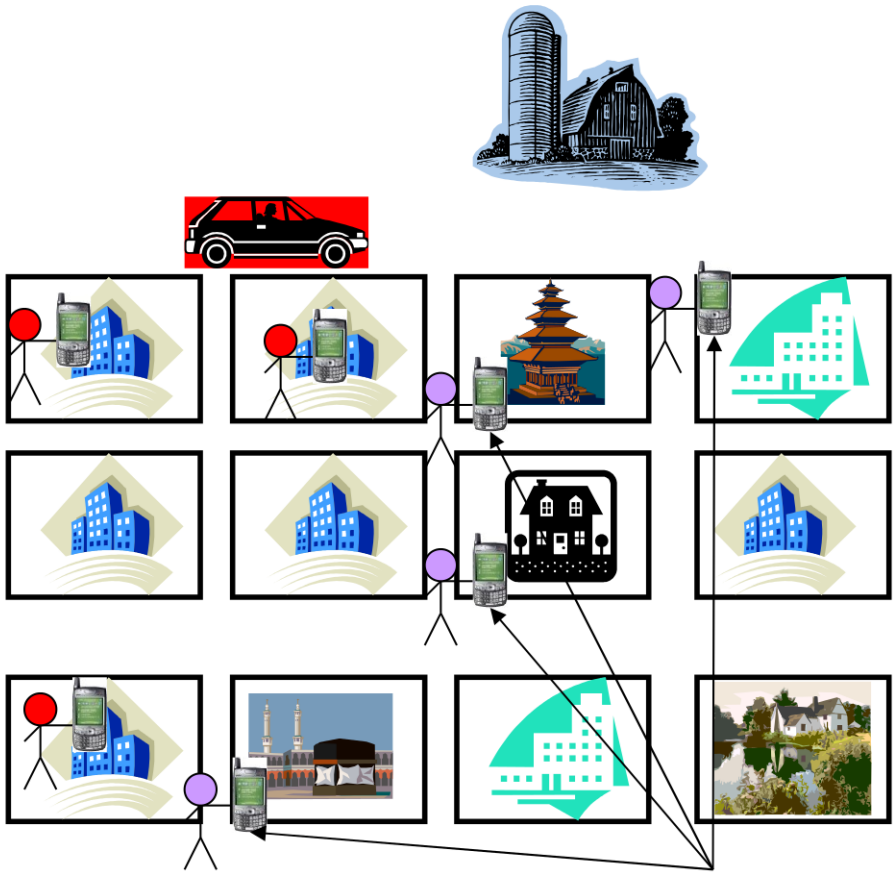
Mobile data generator in a car sending segments of audio





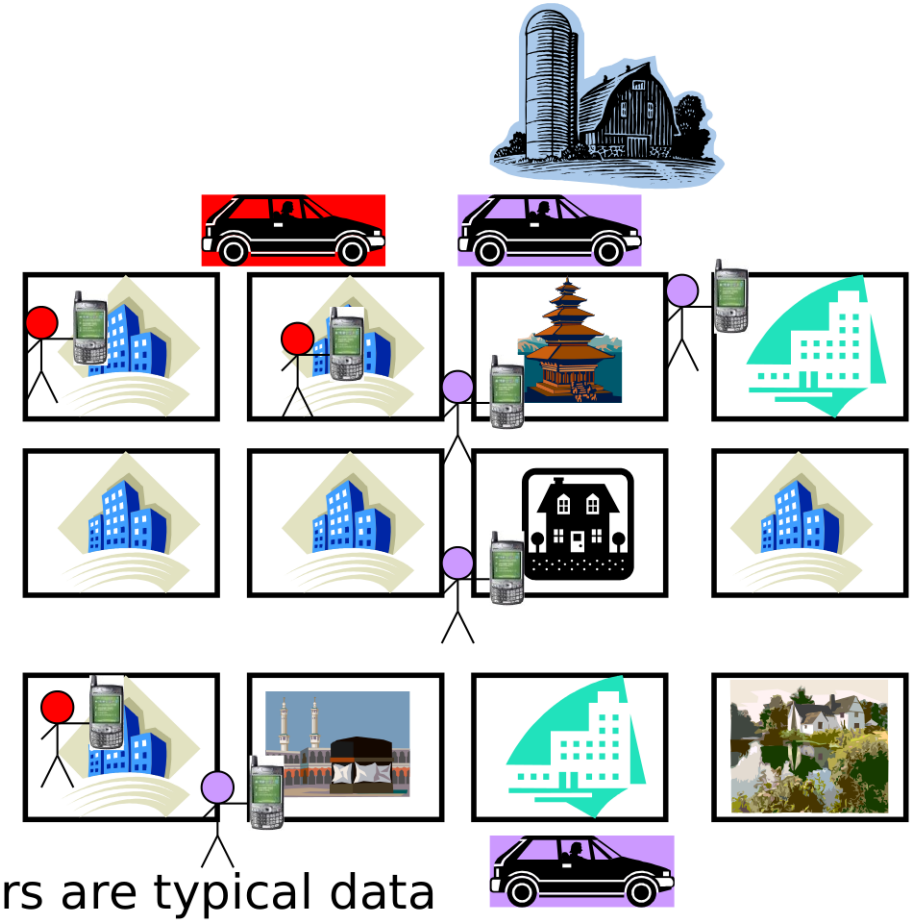
Destination node in parking lot by the Comcast Center

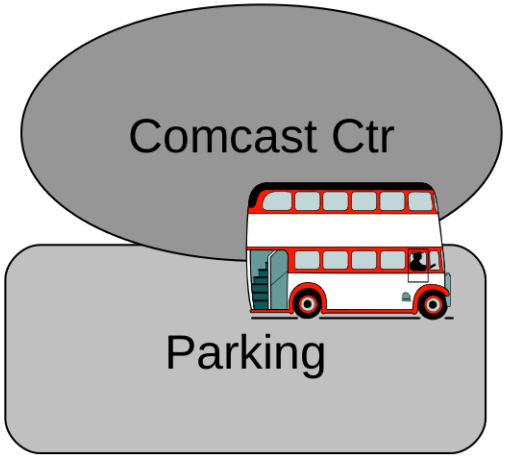
M



Pedestrian relays walk around, and pick up data from source nodes

M





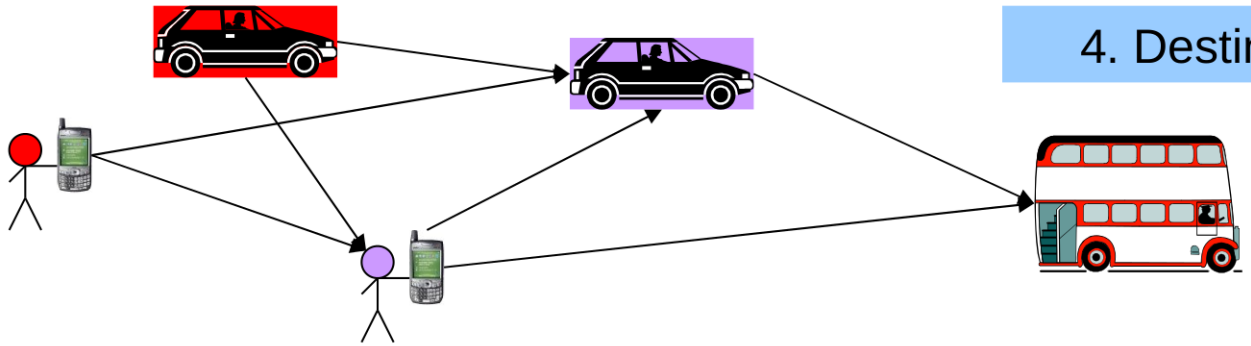
Parking

Car Players are typical data ferries. They relay data to the destination.

1. Sources

3. Relays

4. Destination



2. Relays

Questions?