Delay Tolerant Networking

and

Information Centric Networking

Kevin Fall, PhD

Qualcomm*

Dec 2, 2011 / GFIW2011

*Comments do not necessarily reflect the position of Qualcomm, Incorporated.

Networking Today

- Existing TCP/IP-based Internet
  - Every interface has 32 or 128-bit IP address
  - Identity and location tied together
  - Routing establishes single end-to-end path to host
  - Most traffic uses virtual connection (with TCP) using small best effort transfer unit (datagram)
  - Security of channels between hosts, firewalls
  - Early binding of host name to address
    - Binding security (DNSSEC) just starting

Motivations for Change

- DNS – host table files too big and hard to manage
- CIDR – routing scalability concerns
- IPV6 – running out of IPv4 addresses
- TLS, IPsec, DNSSEC – security
- Delay/Disruption Tolerant Networking
  - Not always connected
  - Not always using same networking stack
- Information/Content Oriented Networking
  - Connections to hosts not of paramount importance
  - Content caching and security are

Firewalls
NATs

ICN: What's Different

- Primary unit of networking is (data) object
- Names (IDs) are location independent
- Routing function is different
  - – Routing toward IDs (content name based)
  - – Mapping between IDs and locators at lower layer
  - – Few/no graph-theoretic scalability results
  - – Caching naturally included in model
- Security on the content (and access to it)

DTN: What's Different

- Primary unit of networking is (data) bundle
- Names (IDs) are flexible and late bound
- Routing function defined outside architecture
    - Routing toward IDs (strings) across protocols
    - (optional) mapping between locators and IDs
    - Caching can be naturally included in model
    - Custody transfer (incremental delivery)
- Security is on content and delivery agents

Bundles / Objects

- Bundle (DTN) is an object useful to application
  - "bundle together" interactions [tolerate big RTT]
  - Unit of retransmission / caching
  - Can be fragmented / encrypted
  - Has origin time and expiration time (and CoS)
- Objects (ICN) = useful content units
  - Unit of retransmission / caching / security
  - Named and found
  - Independent of hosts or immediate connectivity

Naming

- ICN names objects
  - In CCN (NDN), names are hierarchical
  - Receivers express interest, met by data (routing)
  - Opaque to network
- DTN expresses names using URIs
  - And leaves the URI scheme TBD (also opaque)
  - Provides the ability to use multiple schemes
    - E.g. use IP or MAC address if absolutely necessary

Routing and Forwarding

- DTN and ICN route on names (not addresses)
  - No fixed limit on size or # of identifiers
  - No issue (or need for) NAT
  - No major issue of re-binding or multihoming
- DTN routing has a concept of contacts
  - And times/durations they become active
  - Lots of schemes in literature (some have loops)
- ICN (NDN) routing can be naturally multipath
  - With loops avoided by recognizing interests/data
  - Cannot address particular hosts (no prefix hijacking)

Late and Early Binding

- DTN supports early or late binding
  - Early: as with DNS, map name to location
  - Late: forward until mapping required
- ICN supports a form of (very) late binding
- Observations:
  - Early is especially useful for config/debug
  - Late is a tradeoff of flexibility vs latency
  - Binding requires its own security mechanism

Transport

- DTN usually has a DTN and convergence layer
  - – DTN layer- schedules links, proactive fragmentation, replication, subscriptions
  - – CL- adapts bundles for transport on other protocol
  - – Custody transfer keeps forward progress
- ICN (NDN) leaves most transport issues to app
  - – Assumes unreliable transport but caching
  - – Proactive caching keeps forward progress
    - Even if disconnection / disruptions occurs
  - – "Any layer 2"

Security Model

- Today: mostly access and channel security
  - 802.1X, EAP, IPsec, TLS [endpoint mostly host]
- A few exceptions that focus on content
  - DNSSEC [observes sender maybe != author]
- Basic needs for content security [at network]
  - Integrity
  - Authentication
  - Confidentiality
  - Provenance
  - Availability

REGISTERs
FINDs
Content
(in pub/sub systems)

The Basics

- Integrity
  - Can bind content to a name via a hash
- Authentication
  - Stronger than integrity, requires demonstration of key
  - Must cached data (or REGISTERs) be authentic? [policy mgmt]
- Confidentiality
  - Requires usage of key to perform encryption
  - Must cached data (or FINDs) be confidential? [policy mgmt]
  - End-to-end encryption can frustrate in-network processing
- Provenance
  - Can follow chain of modification (with integrity and authentication)
- Availabilituy
  - Resources that can be attacked via DoS
    - Storage, communication channels, computation

(Data) Access Control

- Many people want controlled sharing of their private information
  - – But don't really like DRM [many reasons…]
- Establishing the threat and trust model
  - – Does Bob trust his private content on Alice's system?
    - The DRM problem – usually not safe if software-only
  - – Does Alice trust (anybody's) content on her system?
    - Isolation, sandboxing, taint tracking, IFC

Availability Concerns

- New potential areas for DoS in ICN
  - REGISTERs and FINDs both generate traffic
  - Anonymity already built in if no source ID concept
  - Long ID parsing
  - Fragmentation interaction (e.g. with signatures)
  - Crypto processing
- And in DTN
  - Custody store, registrations, unsolicited traffic, long expirations

Common Research Themes

- Routing / forwarding scalability
  - Objects not constrained by physical topology size
  - Long, variable-length names not like fixed 32 bits
  - Discovery of local nodes/objects/attributes
- In-network storage management
  - Cache eviction, custody, DoS resistance, priority
  - Multicast operations over time
- Security and privacy
  - Scalability, revocation, resource exhaustion
  - Content/policy-enforcing gateways

Conclusion

- DTN originally designed for two things
  - Dealing with radical heterogeneity in networks
  - Tolerating delay and disruption
- ICN designed for the efficient dissemination of information and content
- Several features in common
  - Long term storage in routers, incremental delivery, routing on names, security on objects
- DTN can serve as the underlying transport
  - Possibly the other way as well
  - But must ultimately travel on *some* network not defined by either DTN or ICN

Thanks

www.dtnrg.org

kfall@qualcomm.com