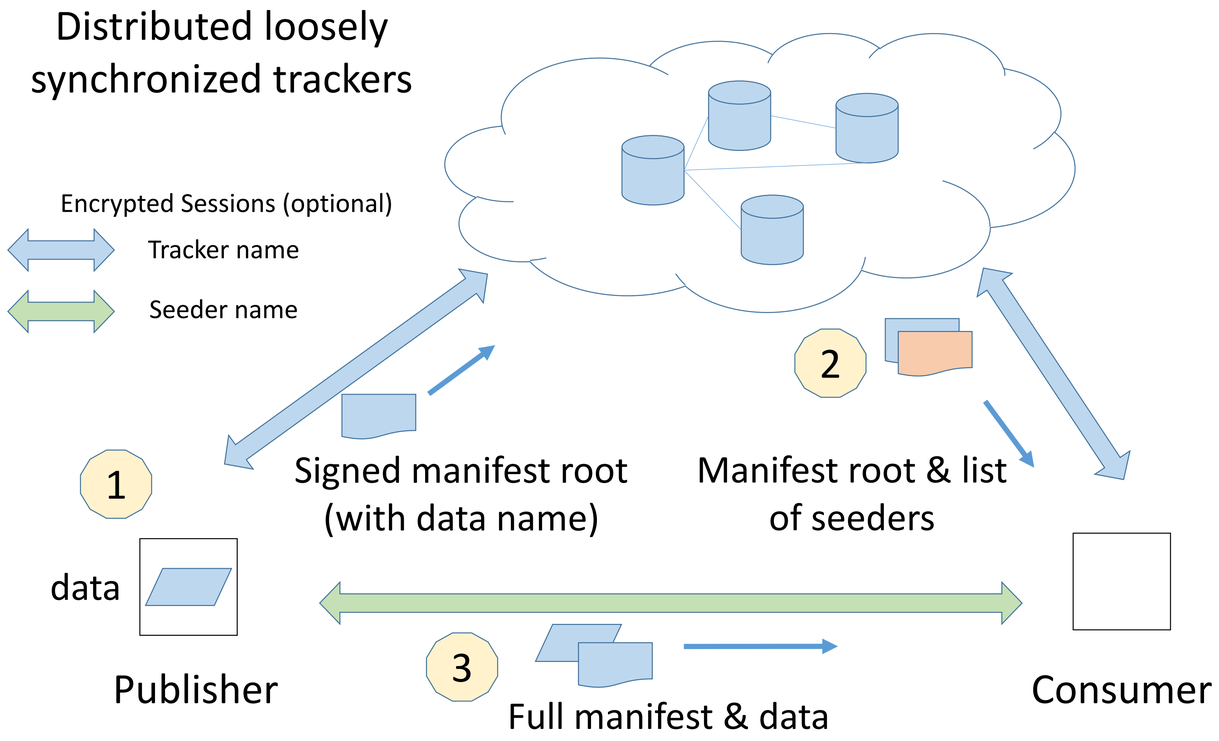
Project Origin: A distributed peer-to-peer object store for CCN

Marc Mosko, Palo Alto Research Center (May 29, 2016)



Nameless Objects

- Content Object does not have name
- Interest has name (for routing) and Hash Restriction
- Match only on SHA-256 hash of Content Object

Use

- Root manifest has a name, no other objects in manifest tree
- A seeding node co-signs root manifest with its own name
- Tracker distributes original root manifest and list of co-signed seeder names
- Consumer then asks for hashes (from original manifest) under seeder namespaces
- If using encrypted tunnels, may use names + encapsulation instead of nameless objects.

Protocol Overview

- Better than BitTorrent using CCNx
  Manifest hierarchical, trackers sync small amount of data
- Publisher transfers signed root manifest to tracker (~ 1KB)
  Uses publisher's routable namespace (/pub) (or encap)
- Trackers synchronize list of seeders, co-signed root manifests
- Consumers request original manifest name, get back original root manifest plus list of seeders (e.g. co-signed manifests)
- Consumers transfer from seeders (e.g. /seedc namespace)
  Verify seeder based on co-signed root manifest
  Consumer-seeder protocol exchanges which manifest branches seeder has, does not need all data
- Variation: Trackers transfer initial data for on-line repo
- Variation: Trackers support push notifications to consumers

Encrypted Sessions

- Uses CCNxKE protocol
- Derived from TLS 1.3
- Allows 1-way and 2-way authentication
- Allows authentication namespace separate from data namespace
- Only "server" side needs routable name
- Create forward-secure ephemeral keys for AES-GCM
- Uses Interests and Content Objects (both inner and outer)
- Outer namespace names encrypted session
- Inner namespace for data transfer
- Use of encrypted tunnels (encapsulation) means use of Nameless Objects not required