Problem Statement of P2P Streaming Protocol (PPSP)

draft-ietf-ppsp-problem-statement-01

Y. Zhang, N. Zong, G.Camarillo, J.seng and R. Yang

IETF-80, Prague, March 28 , 2011

Problems

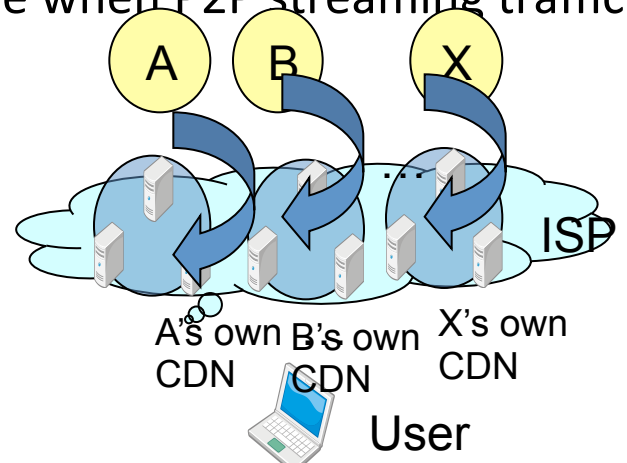
- Hard to share resource with multiple private protocols
  - Memory
  - Storage
  - Bandwidth

  } ISPs, vendors and terminals

- Hard to adapt with new environment current protocols don't address
  - Including mobile and wireless network with a different characteristic in both network and terminals

What's new in the PS(1)

- Difficulties in building open streaming delivery infrastructure with lots of private protocols
  - ISP has the willing to build an open infrastructure for low-cost unified streaming delivery using P2P tech (ISP owned P2Ped CDN)
    - Also current CDN using protocol like HTTP is costly for streaming vendors
  - But private P2P streaming protocols lead to
    - Vendor deploys its own P2Ped CDN network
    - Storage and traffic waste in the ISP for same content as a whole
    - Worse when P2P streaming traffic percentage is increasingly higher



Storage: X times
Traffic in backbone:X times

What's new in the PS(2)

- Terminal physical resource starvation with lots of private protocols
  - iPAD: 256M memory, 16G storage
  - iPhone(X generation): 20M available memory in practice
  - Current P2P Streaming occupation:~100M memory and ~1G storage

  - Concurrent running scenarios
    - PPStream for live streaming and PPVA for helping others (only contributing)

Break down: (

What's new in the PS(3)

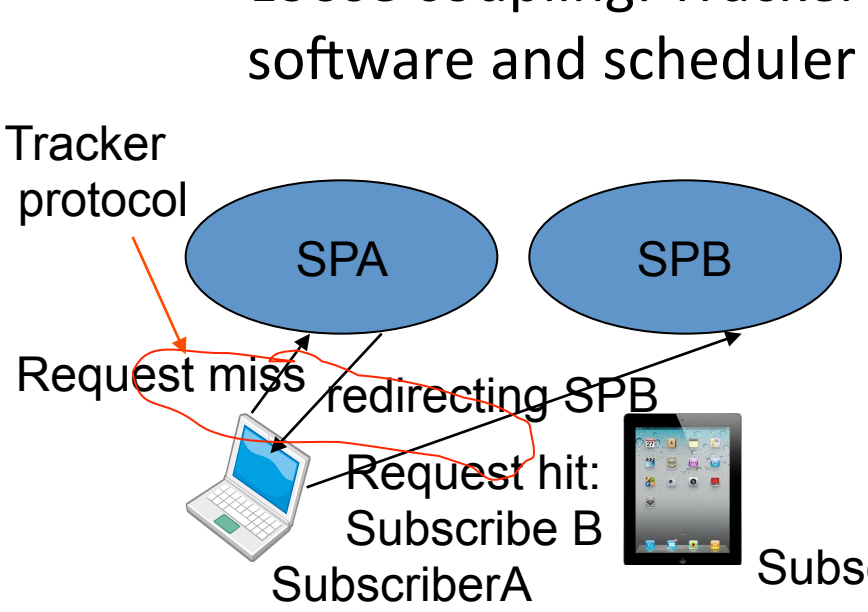
- Difficulties in mobile environment for using current protocols
  - –Any difficulties?
    - Performance degradation
    - Adaptation: what kinds of mobile terminal and network information to carry in tracker and peer protocol for better performance
      - Terminal capability
      - Network dynamics
  - −Question in ML: Is mobile network so *broad* to accommodate P2P streaming?
    - −3G:Already 30% traffic are P2P in some networks
    - −LTE: uplink:50Mbps downlink:100Mbps

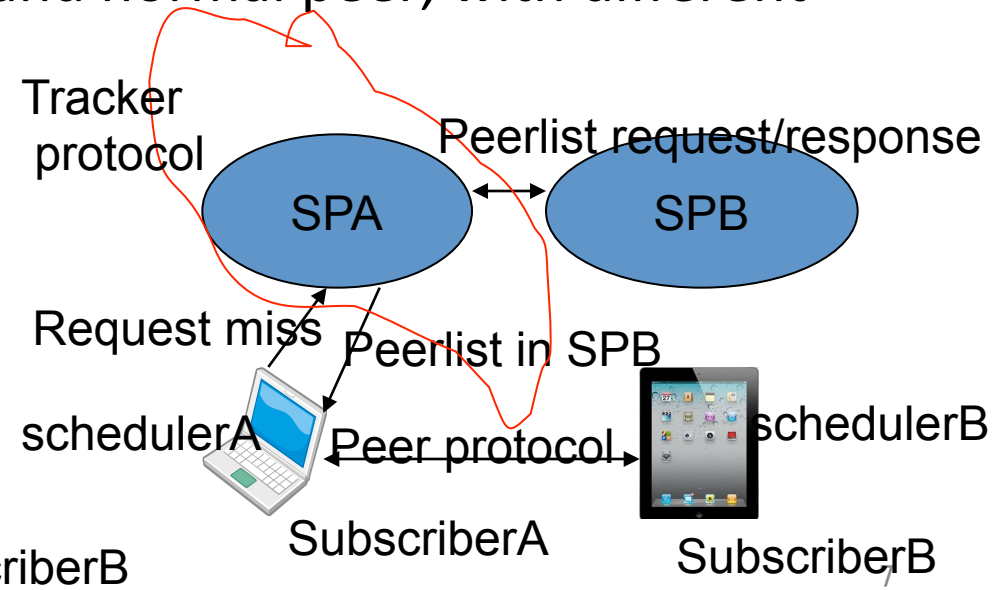
Open tracker and peer protocol enable memory, storage and bandwidth sharing and saving for same content in both terminal and network sides with reduced infrastructure deployment cost among different streaming applications

Open tracker and peer protocol addresses fixed and mobile/wireless converged network environment

Use case updates(1-a)

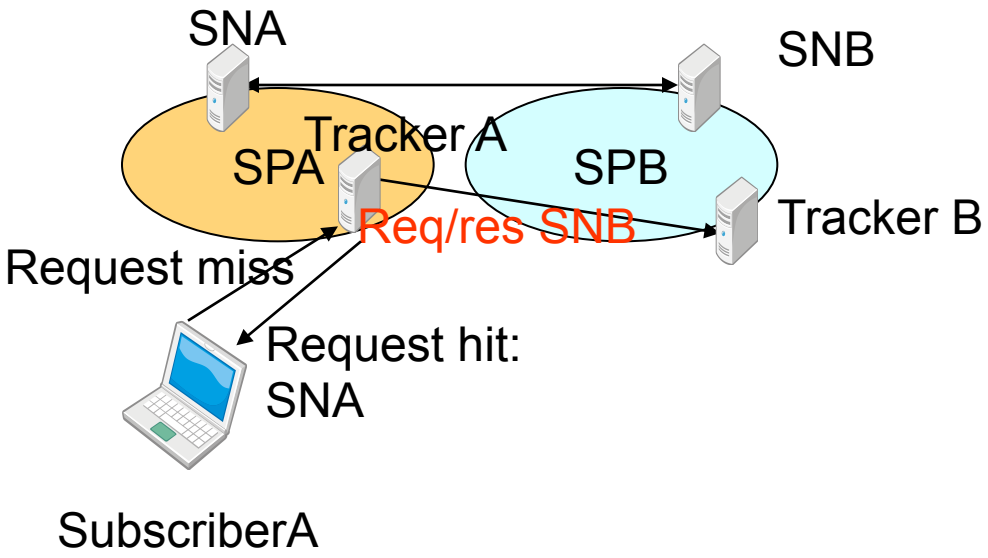
- Interworking between different streaming providers
  - Currently: IP outside certain region cannot access some P2P streaming (by policy) or has a bad performance
    - Limit or wrong knowledge on out of scope IP addresses
  - Cooperation can solve this problem
  - Loose coupling: Tracker and normal peer, with different software and scheduler





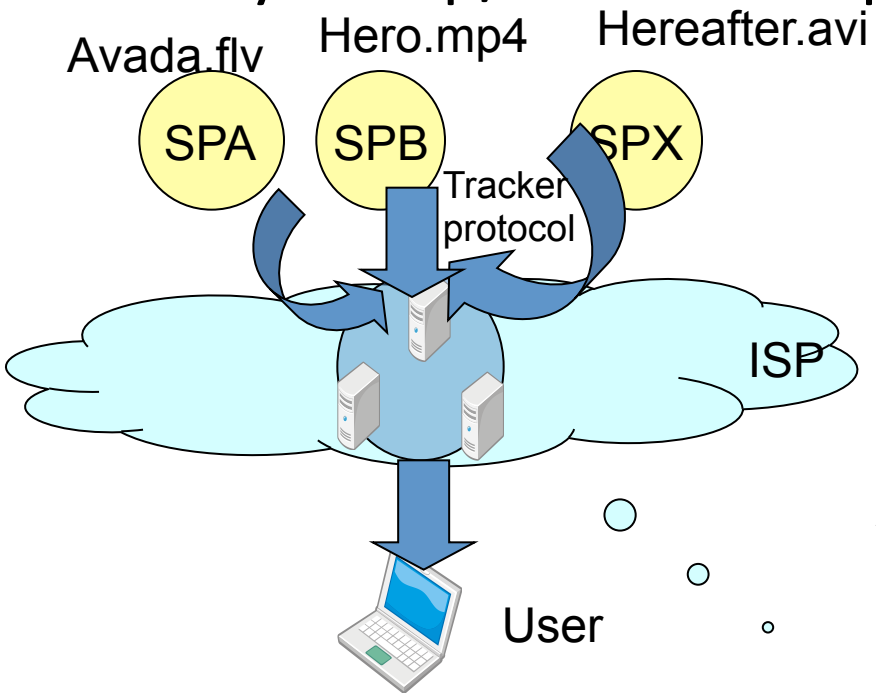
Use case updates(1-b)

- Tight coupling: Tracker and SuperNodes sync



Use case updates(2-a)

- Open ISP's CDN supporting P2P streaming with tracker protocol
  - Edge nodes deployment saving: Some ISPs attract SPs with very cheap/ even free speeding

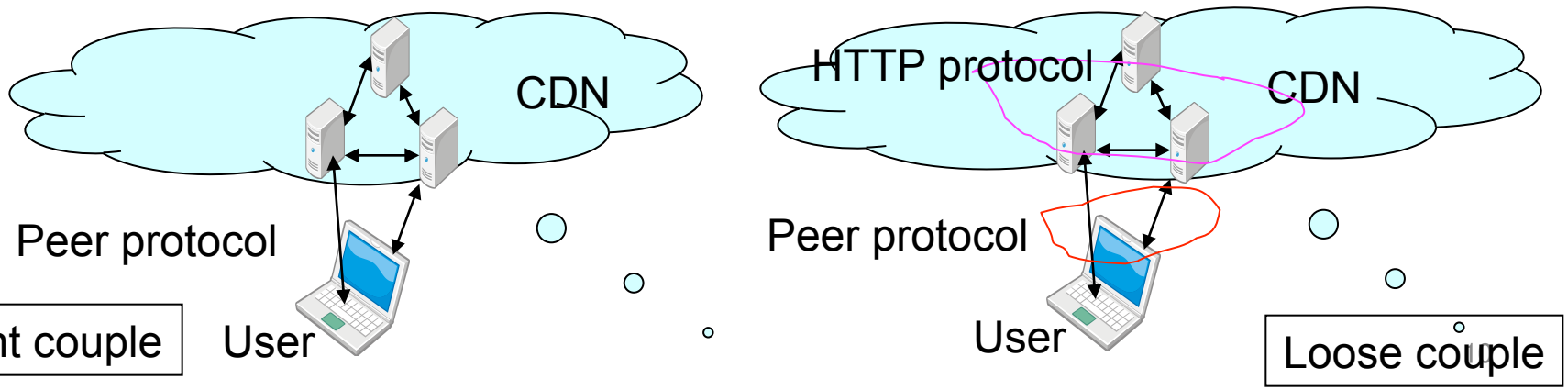


For same content
Deployed Storage: 1 times
Traffic in backbone:1 times

Largely reduce the storage
And traffic waste

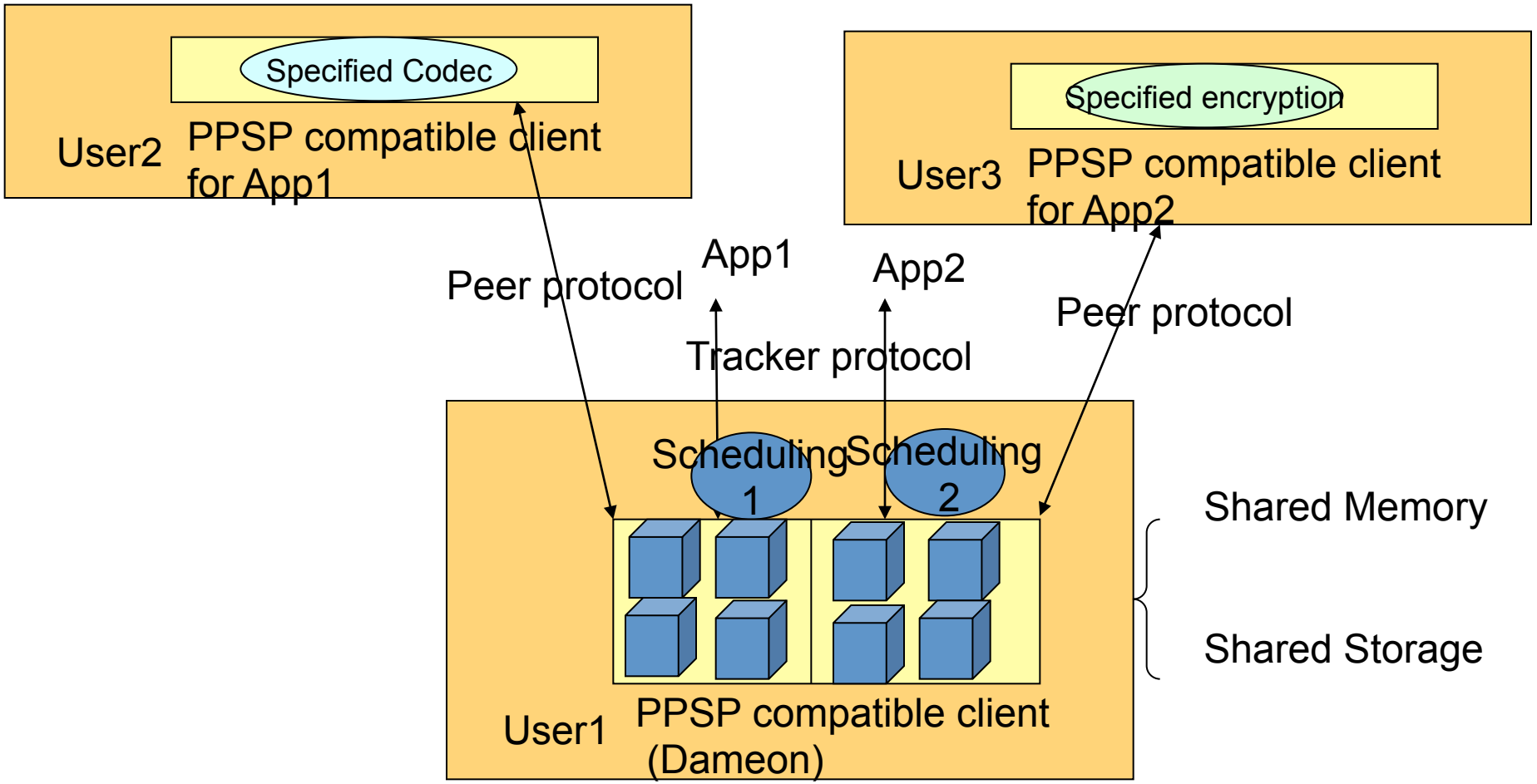
Use case updates(2-b)

- Hybrid CDN-P2P delivery with peer protocol
  - Tight coupling (Newly built CDN):
    - No difference between CDN nodes and peers
    - Trackers can act as the scheduler in the CDN
    - Building CDN network is just the same as building p2p overlay
  - Loose coupling(Existing CDN):
    - Dual stack for http and ppsp in CDN nodes
    - Easily separate the distribution (http based) and delivery (ppsp tracker and peer protocol based)



Use case updates(3)

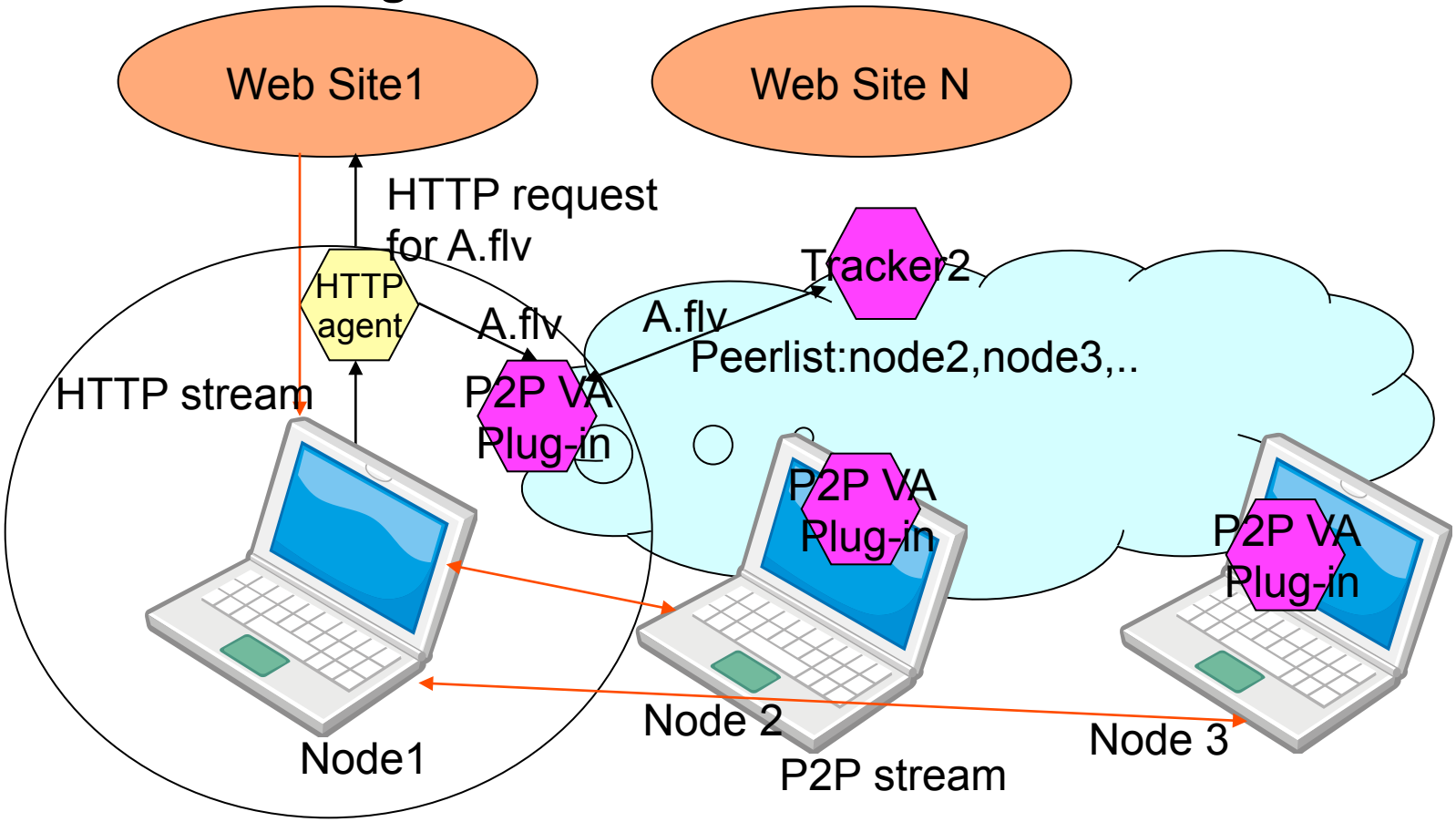
- Single client-base supporting different apps



Use the tracker and peer protocol for necessary information in streaming acquisition and sharing

Use case updates(4)

- Open Video Acceleration (VA) with converged http streaming and PPSP streaming



Security part update

- Adding the consideration on untrusted peers
  - PPSP security considerations involve the security problems related to the introduction of p2p technology (e.g. usage of untrusted peers) and the used PPSP protocols.
    - Malicious peers DDoS attack to tracker by sending fake request
    - Malicious peers may report fake information (e.g.,cheating trackers and other peers by claiming itself owning some unexisting data).
- User authentication and data integrity check for streaming may be necessary for PPSP
- Do we need a draft on this?

Next step

- Modify according to the suggestions and comments
- Ask for WGLC

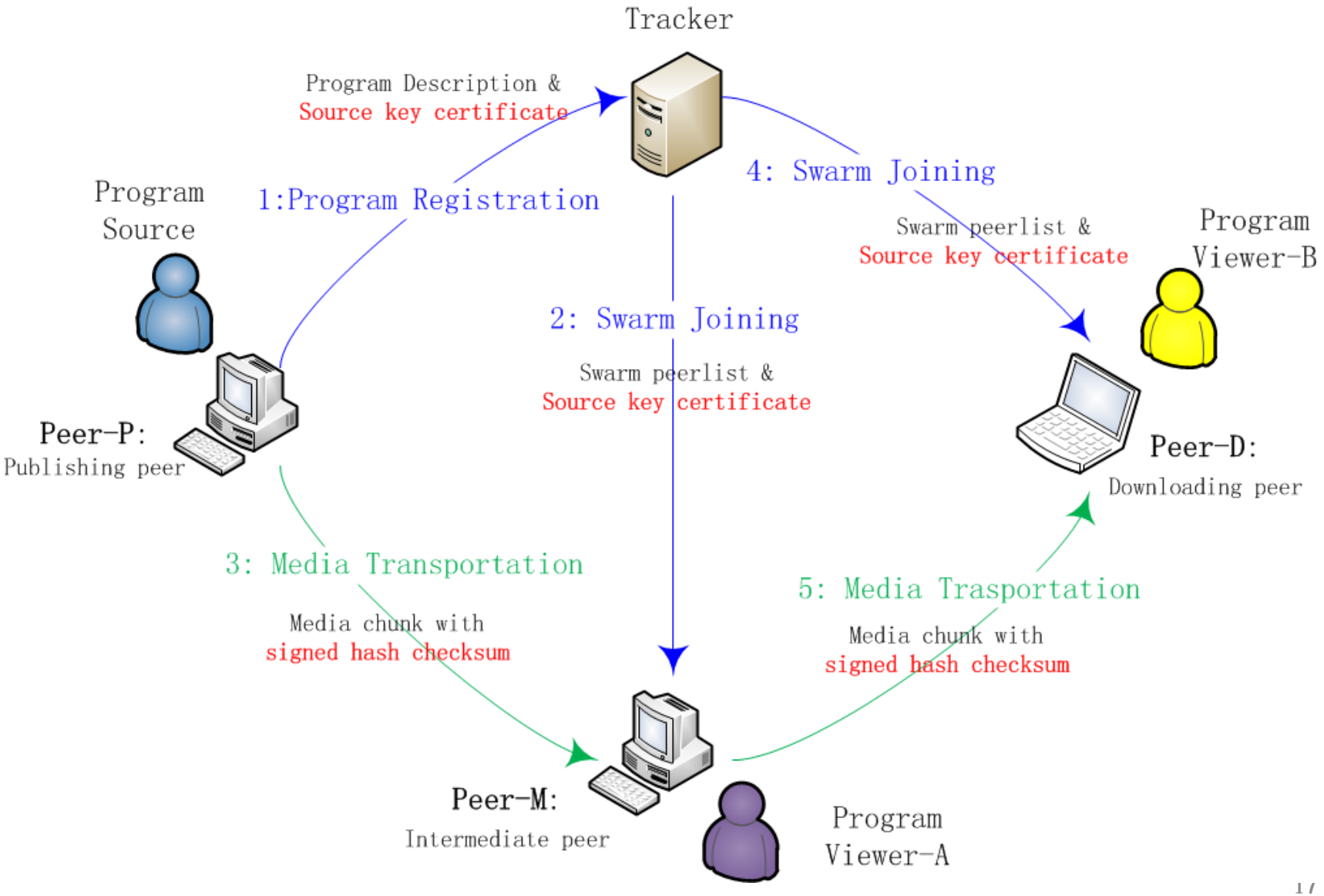
Thanks for your attention!

Q&A?

Motivation

- What does integrity mean in P2P streaming?
  - The media content is exactly the same as published from a certain source and not manipulated by any intermediate party in the network.
- Why do we need to protect media content's integrity?
  - Desirable from the media publisher's point of view
    - Who holds certain reputation/authority/responsibility for the media content's authenticity/validity it provides to the public.
  - Desirable from the downloading peer's point of view
    - To ensure the received media is authentic from a valid source.

Proposal


Tracker
Program Description &
Source key certificate
1:Program Registration
Program
Source
4: Swarm Joining
Swarm peerlist &
Source key certificate
Program
Viewer-B
2: Swarm Joining
Swarm peerlist &
Source key certificate
Peer-P:
Publishing peer
Peer-D:
Downloading peer
3: Media Transportation
Media chunk with
signed hash checksum
5: Media Trasportation
Media chunk with
signed hash checksum
Peer-M:
Intermediate peer
Program
Viewer-A

Open issues

- Which type of certificate should be used?
  - Certificate for the publishing entity, peer, or program?
- Who should be responsible for the certificate distribution?
  - The tracker or the peers?
- Who should issue the certificate?
  - Publishing entity, peer, tracker or a trusted third party?