CERIAS

the center for education and research in information assurance and security

A Design for Securing Data Delivery in Mesh-Based Peer-to-Peer Streaming

Jeff Seibert, Xin Sun, Cristina Nita-Rotaru and Sanjay Rao
Department of Computer Science, Electrical and Computer Engineering and CERIAS, Purdue University

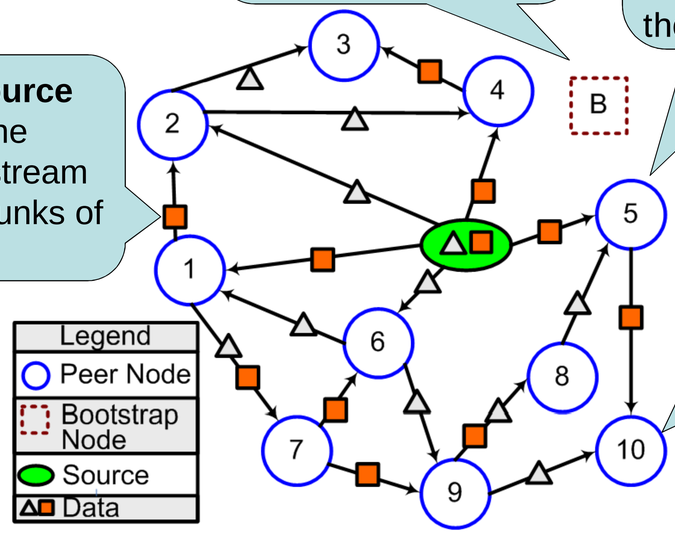
What is Mesh-based Peer-to-Peer Streaming?

The **bootstrap node** introduces new peers into the system by referring already joined peers.

Each node connects to only a small subset of peers (i.e. *neighbors*) and requests the most recent chunks from them.

The **source** splits the video stream into chunks of data.

Each node relies on its neighbors to deliver chunks to it. It is supposed to forward these to its neighbors as well.



Insider attacks on P2P streaming

- Malicious nodes want to disrupt the video playback of benign nodes.
  - An unfair business competitor can target the streaming service with the goal of discouraging users from using the system.
- **Our goal: Limit the amount of damage malicious nodes can cause.**

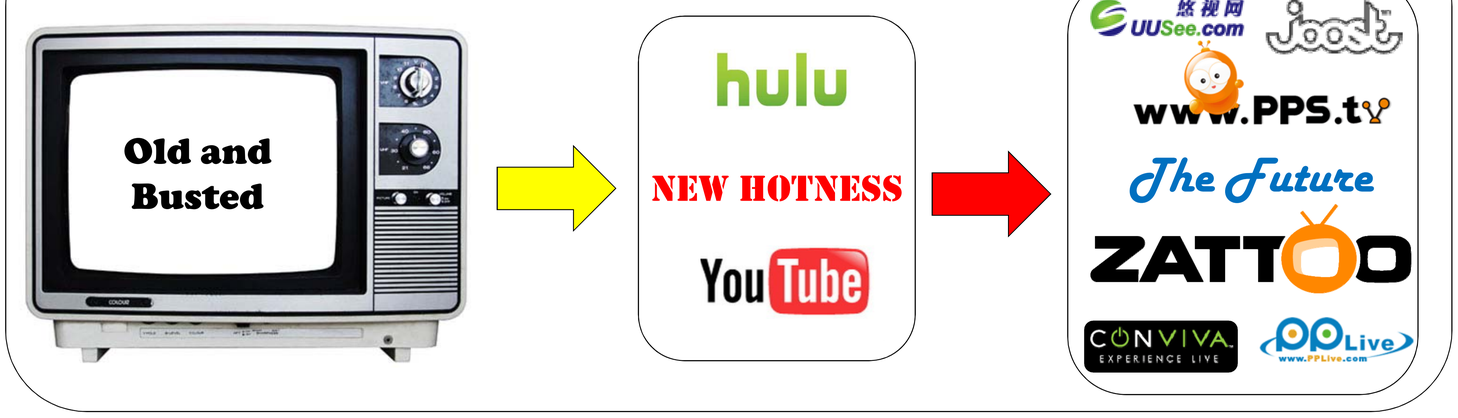
How do malicious nodes attack the system?

- Malicious nodes want to become *neighbors* of many nodes.
- They then drop the video data that they are supposed to deliver to their *neighbors.*
- They can receive data from the source, but never give it to others.
- They can also pollute the bootstrap node's list of peers with malicious nodes.

Peer-to-peer systems are a scalable way to deliver video to users.

They can be used to offset the bandwidth costs of servers and to overcome bottleneck links in the Internet.

The Evolution of Video



These systems assume peers will be honest and cooperative.

How to secure P2P streaming from malicious nodes is an important question.

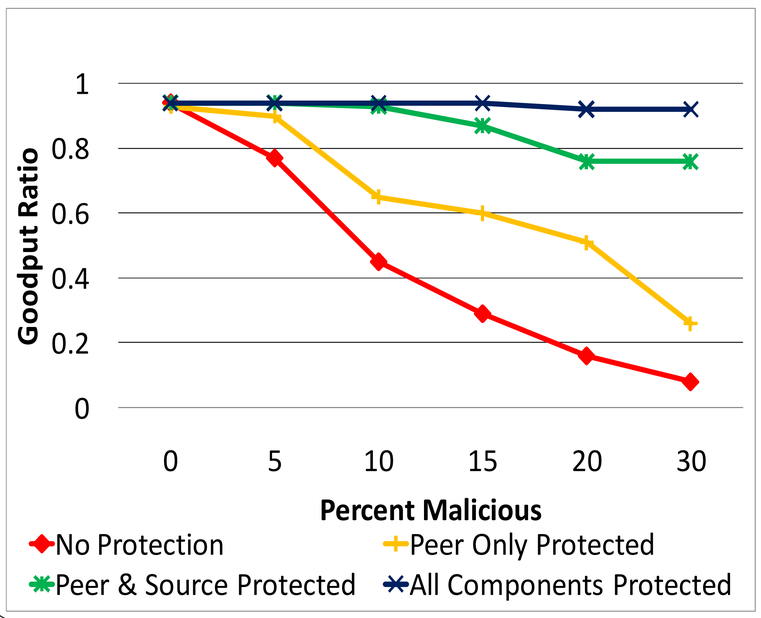
Securing the Data Delivery

The **bootstrap node** will keep track of who has contacted it recently and rate limits the effect that they can have on who is in its referral list.

The **source** will periodically drop those who it is giving data to and try new nodes, so that malicious nodes cannot have a monopoly on the chunks in the stream.

The **peers** will maintain reputation for all other nodes that they come into contact with. They will use this reputation to decide who to keep as *neighbors* and who to allow as *neighbors*.

Peers build reputations for their *neighbors* by evaluating how much data they give and how connected they are to other nodes.



Goodput ratio on PlanetLab for an overlay of 300 nodes when malicious nodes conduct all described attacks.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center