Analysis of Streaming Services and Security Issues in Peer-to-Peer Network

R.Geetha M.E, Nithya B.E (M.E)

Department of Computer science and Engineering. S.A. Engineering College Anna University of Technology
Department of P.G. Studies S.A. Engineering College Anna University of Technology

Abstract
A P2P network is a special type of computer network that exhibits self-organization, symmetric communication, and distributed control. P2P streaming systems can be classified into P2P live streaming systems and P2P VoD systems. P2P live streaming systems can be categorized into tree-based P2P live streaming systems and mesh-based P2P live streaming systems. VoD services allow users to watch any point of video at any time. Depending on the forwarding approaches, P2P VoD systems can be categorized into: 1) buffer-forwarding systems, 2) storage-forwarding systems, and 3) hybrid-forwarding systems. Next, we examine different ways that P2P networks are often attacked, including denying services, contaminating the network, and compromising personal information of the peers. Finally, we analysis the security issues that occur in the underlying p2p routing protocols, as well as trust issues in p2p applications.

Key Terms
Peer-to-Peer (P2P) Video On Demand(VoD), Live Streaming , Tree based streaming , Mesh Based Streaming , Throughput maximization.

I. Introduction

Recently, there has been significant interest in the use of peer-to-peer technologies for live video multicast over the Internet. Peer-to-Peer system has emerged as a promising technology to provide video-on-demand service. Video-on-demand (VoD) streaming is one such service where videos are delivered to asynchronous users with minimal delay and free interactivity. Compared to P2P live streaming, P2P-VoD system supports user interactivity such as VCR operations, which changes user viewing location.

II. P2P Live Streaming System

P2P live streaming system classified into two major types: Tree based live streaming system; Mesh based live streaming system.

A.Tree based structure
In this the group members self-organize into a tree structure, based on which group management and data delivery is performed. Such structure and push-based content delivery have small maintenance cost and good scalability and low delay in retrieving the content and can be easily implemented.

In tree based live streaming to deliver the video streams, a single application layer tree or multiple application layer trees are constructed. Peer may join or leave a live streaming session at any time. Figure 1 shows the tree based live streaming network construction.

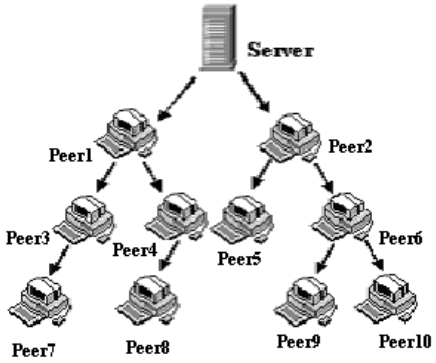

Fig.1 Tree based live streaming

Single Tree Based Structure

In a single-tree based P2P live streaming system, users participating in a live video streaming session can form a tree at the application layer. The root of the tree is the server. Each user joins the tree at a certain level. It receives the video from its parent peer at the level above and forwards the received video to its child peers at the level below.

There are two major drawbacks for single-tree based P2P live streaming systems [10]. First, the departure of a peer causes the isolation of all of its descendants from the video source. Second, all the leaf nodes do not contribute their uploading bandwidths, which degrades the efficiency of the peer bandwidth utilization. A remedy to those drawbacks is a multiple-tree based P2P streaming system.

Multiple-Tree based structure

To improve the resiliency of the tree and the bandwidth utilization of the peers, multiple-tree based approaches

Manuscript received April 5, 2013
Manuscript revised April 20, 2013

have been proposed. There are two key advantages for the multiple-tree solution. First, if a peer fails or leaves, all its descendants lose the sub-stream delivered from that peer, but they still receive the sub-streams delivered over the other trees.
Therefore, all its descendants can receive a coarse video quality in case of a loss of a sub-stream. Second, a peer has different roles in different trees. It might be an internal node in one tree and a leaf node in another tree [10]. When a peer is an internal node in a tree, its upload bandwidth will be utilized to upload the sub-stream delivered over that tree. To achieve high bandwidth utilization, a peer with a high upload bandwidth can supply sub-streams in more trees.

B. Mesh-Based Structure

In contrast to tree-based structure a mesh uses multiple links between any two nodes. Thus, the reliability of data transmission is relatively high. Besides, multiple links results in high bandwidth usage. Mesh forms an overlay network by selecting a number of neighbors while tree structure is formed by selecting parent and children. In fact, Neighbors or Parent-Child selection is considered a topic to be studied. A P2P system can selects neighbors/Parent-Child by comparing bandwidth, packet delay, round time trip, ranking and other kinds of selection. Each peer can receive data from multiple supplying peers in mesh-based streaming systems, instead of a single parent in single-tree based streaming systems. The major challenges in mesh-based P2P live streaming systems are neighborhood formation and data scheduling.

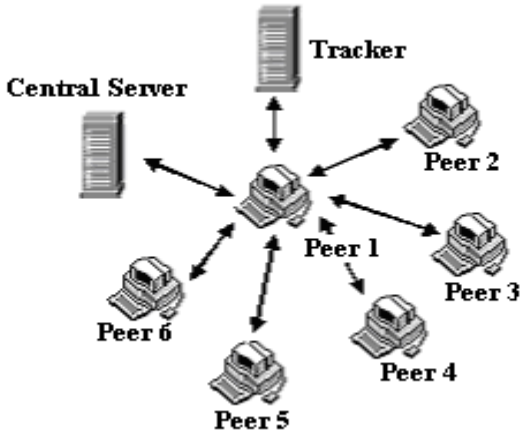

Fig.2 Mesh based P2P Live Streaming

III. P2P VoD Systems

P2P-based video-on-demand (P2P-VoD) is a new challenge for the P2P technology. Unlike streaming live content, P2P-VoD has less synchrony in the users sharing video content, therefore it is much more difficult to alleviate the server loading and at the same time maintaining the streaming performance[3]. VoD service allows users to watch any point of video at any time. VoD provides more flexibility and interactivity to users, thus attracting more users recently. Depending on the forwarding approach, the existing P2P VoD systems can be classified into three categories: buffer-forwarding P2P VoD systems, storage-forwarding P2P VoD systems and hybrid forwarding P2P VoD systems.

A. Buffer forwarding P2P VoD System

In buffer-forwarding architectures, each peer buffers the recently received content, and forwards it to the child peers. The participating peers can be organized into a tree-structure [3]. In addition, by adjusting the priority weight at each peer, we can implement the differentiated throughput among different users within a video session in the buffer-forwarding architecture.

B. Storage-forwarding P2P VoD systems

In storage-forwarding systems, the blocks of the video are disseminated over the storage of peers.When a peer wants to watch a video; it first looks for the supplying peers who are storing the content and then requests the content from them [7]. In the storage-forwarding approach, each peer stores one or multiple segments in its storage, and contributes the stored segments to other peers who are requesting them.

C. Hybrid forwarding P2P VoD systems

P2P VoD architecture which integrates both the buffer-forwarding approach and the storage-forwarding approach is called hybrid forwarding P2P VoD systems propose a hybrid-forwarding P2P VoD architecture to improve the throughput by combining the buffer-forwarding approach with the storage-forwarding approach [9]. The total upload capacity is still limited in the buffer-forwarding systems. To further improve the throughput, we propose a hybrid-forwarding.

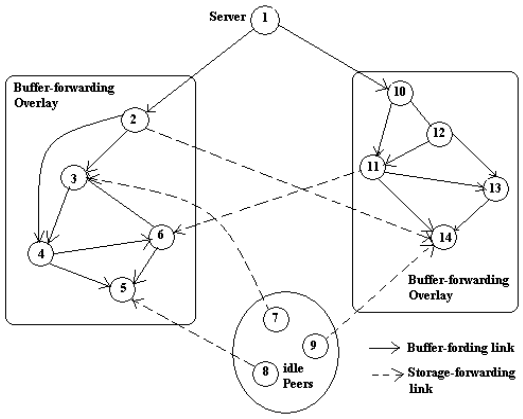

Fig.3 Hybrid Forwording System

D. Exprimental Results

The buffer-forwarding architecture has a limitation in total upload capacity. The throughput maximization problem in the hybrid-forwarding architecture is also solved using a fully distributed algorithm.

We demonstrate that the proposed hybrid-forwarding architecture greatly improves the throughput compared to the buffer-forwarding architecture.

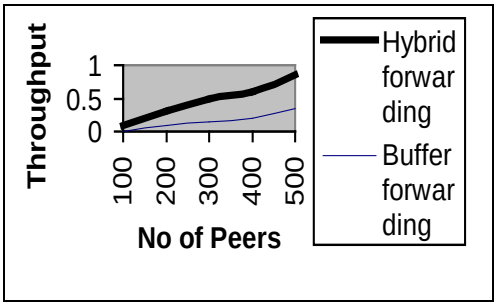

Fig.4 Performance comparison in buffer-forwarding and hybrid forwarding with different network sizes

IV. Security issues in p2p network

A p2p network provides a scalable and fault-tolerant mechanism to locate nodes anywhere on a network without maintaining a large amount of routing state. This allows for a variety of applications beyond simple file sharing. Examples include multicast systems, anonymous communications systems, and web caches. [1]

A. Attacks on P2P Networks

Since P2P systems inherently rely on the dependence of peers with each other, security implications arise from abusing the trust between peers [1]. In a traditional client-server model, internal data need not be exposed to the client, but with P2P, some internals must be exposed to fellow peers in the name of distributing the workload.

Some of the Attacks of P2P networks are:

- Distributed Denial-of-Service
- Poisoning the Network
- Privacy and Identity
- Fairness in Sharing
- Blocking of P2P Traffic

In a traditional denial-of-service (DoS) attack, a server is usually the target of massive connections, rendering the server inoperable. Another approach towards attacking a P2P network is to inject useless data (poison) into the system. Since P2P networks must implement a lookup service in some way, whether it is a centralized directory or a DHT, an attacker can inject large amounts of useless lookup key-value pairs into the index.

Poisoning can be accomplished in two ways, by index poisoning or route table poisoning. In index poisoning, fake records are inserted into the index pointing to a target IP and port number. . In route table poisoning, the attack leverages the fact that almost all P2P clients need to maintain some kind of routing state of the current peers with which it is connected.

B. Trust Management

A peer-to-peer (P2P) network is a computer network that does not have fixed clients and servers but a number of peer nodes that function as both clients and servers to the other nodes in the network [11]. P2P File sharing system provides an open, unrestricted environment for content sharing. However, this openness also makes it an ideal environment for attackers to spread malicious content. In order to be a reliable source of information, the responses to be used in trust evaluation must be authenticated.

Trust Models

Peer-to-peer online communities are commonly perceived as an environment offering both opportunities and threats. Peer-to-peer online communities can be seen as truly distributed computing applications in which peers communicate directly with one another to exchange information, distribute tasks, or execute transactions [12].

Most of the security threats presented in P2P information sharing environments are due to two main features of the P2P design as Unknown P2P communication and shared information.

The following are some of trust models:

- Secured Trust
- SF Trust
- FC Trust

- Reco-Trust
- User-Trust
- MAS-Trust
- Peer- Trust

Typical issues in implementing a P2P trust model such as Peer Trust in a decentralized P2P network include decentralized and secure trust data management [12]. Figure 5 shows the comparing the trust models in terms of computational time.

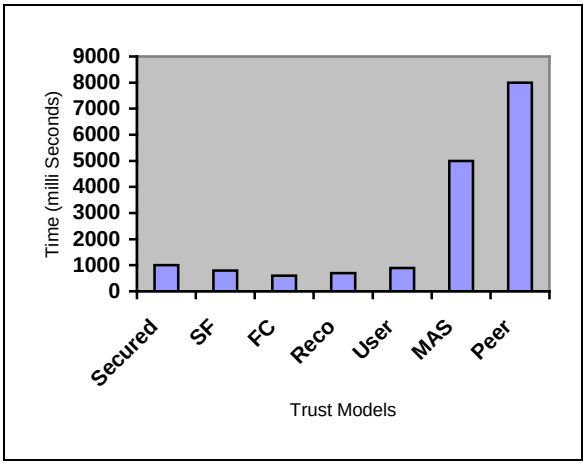

Fig.5 Performance comparison of different Trust Models

C. P2P protocols

In the peer-to-peer environment there are different categorizations of this technology that range from completely centralized to completely decentralize. Peer to Peer enable messaging clients to communicate with each other directly, eliminating the requirement to route message through an external message broker. The protocols and topologies of the centralized peer-to-peer technologies are simple. The distributed architectures are very interesting and quite often complex topologies and protocols.

Following list shows some of the P2P protocols:

- Ares
- Bittorrent
- Direct Connect
- Fasttrack
- eDonkey
- Freenet
- Gnutell
- OverNet

FastTrack is a proprietary protocol, but attempts at cracking the FastTrack protocol have been made but has failed to break the encryption between supernodes. Gnutella was a decentralized protocol for distributed search on a flat topology of peers. Gnutella like FastTrack doesn't have any centralized control point. In Gnutella network nodes are classified as leaf nodes and higher level nodes as ultrapeers, which are high capacity nodes that act as proxies for lower capacity nodes [15].

eDonkey2000 (ED2K) is a semi-centralized network developed by MetaMachine. There are loosely connected, separate index-servers, but there is no single centralized server.

BitTorrent is a P2P system that uses a central location to manage users' downloads. The central location is a tracker that is contacted when you launch a torrent for file downloading. The tracker keeps track of all the users who have the file and connects users to each other for downloading and uploading [15].

Overnet is a fully decentralized network based on Kademlia. Each peer on Overnet gets a NodeID from the 128-bit key space. Key, value pairs are stored on peers with IDs close to the key, closeness is defined by the XOR-metric.

V. CONCLUSIONS

In this paper, we study the different streaming services in p2p environment and also different forwording mechanisms. We analyzed the hybrid-forwarding architecture greatly improves the throughput, and also analyzed security issues and trust models.

ACKNOWLEDGMENT

I must thank my Internal Guide Mrs.R.Geetha M.E Associate Professor, Department of computer science and engineering, without whose guidance and patience, this dissertation would not be possible. I wish to record my thanks to Mrs.Umarani Srikanth M.E., (Ph.D) Head of the Department, Department of Computer Science and Engineering project panel members, Professors of the Department of Computer Science and Engineering for their consistent encouragement and ideas.

REFERENCES

[1] "A Survey of Peer-to-Peer Security Issues " Dan S. Wallach ,Rice University, Houston, TX 77005, USA.
[2] Chi, H., Zhang, Q., Jia, J., Shen, X.: Efficient search and scheduling in P2Pbased media-on-demand streaming service. IEEE Journal on Selected Areas in Communications 3, 1467–1472 (2006)
[3] "Distributed Throughput Maximization in P2P VoD Applications "Yifeng He, Member, IEEE, Ivan Lee, Senior Member, IEEE, and Ling Guan, Fellow, IEEE.
[4] http://dl.acm.org/citation.cfm
[5] http://en.wikipedia.org/wiki/List_of_P2P _protocols
[6] http://www.streamerp2p.com/fourm/viewtopic.php

[7] I. Lee and L. Guan, “Centralized peer-to-peer streaming with layered video,” in Proc. IEEE ICME, Jul. 2003, vol. 1, pp. 513–516.
[8] K. A. Hua, Y. Cai, L. Guanai, and S. Sheu, “Patching: A multicast technique for true video-on-demand services,” in Proc. ACMMM, Sep. 1998, pp. 191–200.
[9] Lee, I., Guan, L.: Centralized peer-to-peer streaming with layered video. In: Proc. of IEEE ICME, vol. 1, pp. 513–516 (2003
[10] “Peer-to-Peer Streaming Systems “Yifeng He and Ling Guan Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, M5B 2K3 Canada
[11] Peer Trust: Supporting Reputation – Based Trust for Peer–to– Peer Electronic communities, Li Xiong and Ling Liu.
[12] SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multi-Agent Systems, Anupam Das and M. Mahfuzul Islam, Member, IEEE,
[13] http://fusesource.com/docs/broker/5.5/connectivity_guide/FMBConnectP2P.html
[14] http://ntrg.cs.tcd.ie/undergrad/4ba2.02/p2p/index.html
[15] http://delco.cs.tut.fi/doc/other/p2p_analysis_v01.pdf