

## Survey on Copyright Protection in Peer To Peer Network

P.Kretthika, Vinutha Yadav D<sup>1</sup>, Dr.Ashwini K<sup>2</sup>

<sup>1</sup>Department of Information Science New Horizon College of Engineering Bangalore, India

<sup>2</sup>Sr.Assistant Professor Department of Information Science New Horizon College of Engineering Bangalore, India

### ABSTRACT

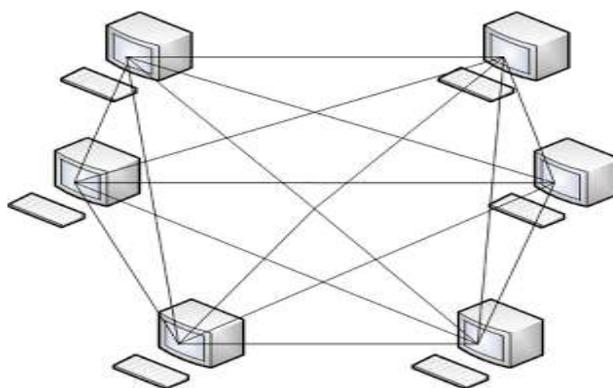
Recently, P2P technology has become so popular that a large number of files are being exchanged by millions of users concurrently. However, due to the significant growth of P2P file sharing, even copyrighted files are also actively exchanged so copyright infringement has become a serious issue. In particular, P2P file sharing is recognized as a killer application for the P2P technology, and several P2P file sharing systems have been used by many users from the late 90's to the present, including Napster, Gnutella, Kazaa and Bit Torrent. However, the popularization of such P2P file sharing causes several undesired issues in recent years, such as the illegal sharing of copyrighted contents violating the copyright law and the act as a hotbed of cyber-crimes such as phishing scams and leaks of personal information. In this work, we propose a solution to ensure copy right violation in P2P systems. Our framework includes DRM, pollution attack, index poisoning, water marking and fingerprinting.

**Keywords:** Peer to Peer systems, copyright infringement, file sharing, digital rights management, pollution attack, index poisoning, watermarking and fingerprinting.

### I. INTRODUCTION

Currently there are a lot of P2P file-sharing networks in existence, and many of them have millions of on-line users and millions of bytes of data shared. In this type of networks, what a user really wants is to find the file he/she is looking for to download it. P2P networks have been typically used for file sharing applications, which enable peers to share digitized content such as general documents, audio, video, electronic books, by using P2P file-sharing application; each peer can upload or

download files freely and share files efficiently. Although Peer-to-peer (P2P) file-sharing networks significantly reduce the cost for large scale Internet content delivery, they have not been explored much in commercial content-delivery applications for lack of protection on intellectual copyrights. This paper attempts to provide an integrated approach to solve this long-awaited open problem. We aim at enabling P2P file-sharing networks as a legitimate channel for legally distribution of copyrighted digital contents such as music and video over the internet.



A peer-to-peer network.

Peer to peer is a type of architecture in which nodes are interconnected with each other and share resources without the central controlling server. P2P system allows us to construct such a distributed system or an application in which all resources and data is contributed by the hosts over the network.

P2P system allows us sharing of data at a very large scale without the use of any server whose job is to manage scaling. P2P is used in file sharing, web caching and providing information to the users; Bit Torrent is an example which uses P2P architecture. The models of P2P architecture include purely decentralized systems, centralized system and hybrid system. Purely decentralized models are which there no central server is; all nodes are acting as both client and server. All nodes are getting and sending data to each other and no server is managing them. One of the examples of this model is Gnutella 0.4. One of the disadvantages of this model is that we can't administrate the network.

Centralized P2P model has a central server whose job is to maintain all the records of files at each node. When a node needs a file it requests the server database and redirects the requesting node to the node which has files. Decentralized P2Ps are classified into structured P2Ps and unstructured P2Ps. Structured P2Ps such as Chord and CAN search files rapidly. However, in order to construct structured topologies, peers in structured P2Ps exchange additional data, and peers are dependent on each other. On the other hand, in unstructured P2Ps, peers are connected randomly and the data placement is largely unconstrained. The system needs low cost to form the topology and low latency to maintain the connection. Prominent examples of unstructured P2P networks are Gnutella and Free net. Hybrid model is a type of model which is introduced to take advantage of both centralized and decentralized system; this model does not use the server hence scalability issue got resolved. One of the examples of hybrid models is Gnutella v0.6. Few issues of this model are loss of distribution and more centralized control.

## **II. ADVANTAGES AND LIMITATIONS OF P2P NETWORKING**

One of the major advantages to a P2P network is that each time a new node is connected to the network the total capacity of the system increases. This point differs from the client-server model standpoint since the addition of new nodes to a network that connects to a set number of servers could

possibly slow data transfers for all of the connected users. Another advantage in regards to a pure P2P network is that there is no single point of failure in the network. One of the weaknesses of P2P networks is that of security. Generally speaking P2P networks are more susceptible to security problems. Security is hard enough in traditional networks that depend on central servers. It's harder still in P2P networks, particularly when you want to authenticate your communication partners and exchange data only with people you trust. One way to combat these security problems in P2P networks is that of a reputation system. Another disadvantage of P2P networks is the high bandwidth usage required. This high bandwidth usage has led to internet service providers starting to throttle or limit P2P traffic.

## **III. APPLICATIONS**

Some of the general applications for P2P networks include the ever popular file sharing, streaming media, grid computing, instant messaging and voice over internet protocol. The most popular P2P file sharing networks that are still active today include G2, fast track, and Gnutella. The application of sharing files over P2P networks is what first popularized the use of P2P technology. Peer-to-Peer (P2P) networks are extensively used for large-scale file sharing. As more information flows through these networks, people are becoming increasingly concerned about their privacy. The reasons behind the privacy concerns may be various such as avoiding user profiling, tracking and data mining, engaging in legal content sharing that may be deplorable from a political, religious or social point-of-view, or engaging in illegal or incriminating content sharing. Traditional P2P file sharing systems are designed for performance and scalability. These systems take advantage of the large number of interconnected peers<sup>1</sup>, and their idle resources, to more efficiently distribute contents at the cost of requiring peers to publicly advertise what they download. Given that peers form interest-based communities [6], every single connection presents an opportunity for a malicious peer to passively obtain additional information that may enable user's content interests' identification.

Copy right is a right given by the law to the creators of literary, dramatic, musical and artist works

and producers of cinematograph films and sound recordings. P2P file sharing of copyrighted works without the permission of the copyright holder is called copyright infringement, the copyright act 1957, governs the laws and applicable rules related to the subjects of copyrights in India. Peer-to-peer file sharing intermediaries have been denied access to safe harbor provisions in relation to copyright infringement. These types of intermediaries do not host or transmit infringing content themselves, but may be regarded in some courts as encouraging, enabling or facilitating infringement by users. These intermediaries may include the author, publishers and marketers of peer-to-peer networking software, and the websites that allow users to download such software.

#### IV. PREVIOUS TECHNOLOGIES

P2P file-sharing networks have been categorized as the latest generation of Internet content delivery systems. However, lack of copyright protection mechanisms in current P2P applications prevented them from being considered as a viable platform to distribute copyrighted contents. The proposed copyrighted P2P content distribution framework supports P2P networks, either structured or unstructured. In this paper, we propose a *copyrighted P2P* (CP2P) content distribution framework for copyright protection in P2P content delivery.

1. **DRM (Digital Rights Management)** encodes contents using a specific encoding technique so that it could be decoded merely by using specific software and/or hardware. But content can be copied and distributed, making this approach in effective [1].
2. **Pollution attack** is aimed to prevent users from conducting an illegal sharing of copyrighted contents in Fast-track (a P2P file sharing system). It is very specific to Fast-track and cannot work for commercial systems [2].
3. **Index poisoning** scheme for **winy networks**, which is a P2P file sharing system widely used in Japan. This scheme involves a mechanism which removes a copy of the index of illegal files immediately after overwriting the correct copy. The cost of replacing index is high [3].
4. **Index poisoning** is a technique which alters the index of illegal files so that they could not be reached by any peer which wishes to access them through the P2P. The index updating cost is high [4].
5. **Watermarking** is a technique which will encrypt copyright information to the content or otherwise restrict or even block access to the digital content

through the internet and the P2P infrastructure which is digital watermarking technique. This technique produces the correspondent watermarking keys distributed within P2P environment [5].

6. **Fingerprinting** scheme is suitable for P2P network which has a basic idea that distributor divides the media content into two parts. Each user gets the same encrypted digital copy from the P2P network and gets a unique decryption key from the content provider. The decryption key is generated from the node's ID that is derived from anti-collusion code. After decryption, the ID is left into the decrypted digital copy, which can be used to trace the traitors. It will protect multimedia data from illegal redistribution [6].
7. A system to stop pirated content propagation by utilizing **several attacks to Bit Torrent**. We design a copyright protection system that can delay the propagation of piracy contents in Bit Torrent without modifying the existing system and protocols [7].
8. A new **P2P authorization protocol** (PAP) is developed to distinguish pirates from legitimate clients. A proactive content poisoning scheme is proposed which stops collusive piracy [8].

#### V. CONCLUSION

Peer-to-peer networks use a decentralized model in which each machine, referred to as a peer, functions as a client with its own layer of server functionality. First section introduces a concept of peer to peer network and classification based on their architecture and structure of network. Then the second section presents the advantages and disadvantages of peer to peer systems. Third section includes the application based analysis of peer to peer systems. Then we propose a *copyrighted P2P* content distribution framework for copyright protection in P2P content delivery.

#### REFERENCES

- [1]. Jungsoo Lee, 'P2P Based Private Broadcasting DRM System', 'supported by the IT R&D program of Ministry of Knowledge Economy / IITA (Institute of Information Technology Advancement) (2007-S-017-01, Development of user-centric contents protection and Distribution technology).
- [2]. J. Liang, R. Kumar, Y. Xi, and K. W. Ross. "Pollution in P2P File Sharing Systems." In Proc. the 24th IEEE International Conference on Computer Communications (INFOCOM), 2005, pages 1174–1185.

- [3]. M. Yoshida, S. Ohzahata, A. Nakao, and K. Kawashima. "Controlling File Distribution in Winny Network through Index Poisoning." In Proc. International Conference on Information Networking (ICOIN 2009), 2009, pages 1–5.
- [4]. J. Liang, N. Naoumov, and K. W, Ross. "The Index Poisoning Attack in P2P File Sharing Systems." In Proc. the 25th IEEE International Conference on Computer Communications (INFOCOM), 2006, pages 1–12.
- [5]. DimitriosTsolis, EleftheriosGeorgatos& Spyros Sioutas, 'The Use of Peer-to-Peer Networks in Copyright Protection', '2009 13th Panhellenic Conference on Informatics'.
- [6]. HaiboGao, WenjuanZeng and Zhen Chen, 'Fingerprinting For Copyright Protection in P2P Context', '2010 International Symposium on Intelligence Information Processing and Trusted Computing'.
- [7]. Hongli Zhang, Lin Ye, Jiantao Shi, Xiaojiang Du, and Hsiao-Hwa Chen, 'Preventing Piracy Content Propagation in Peer-to-Peer Networks', 'IEEE journal on selected areas in Communications/Supplement, vol. 31, no. 9, September 2013'.
- [8]. Xiaosong Lou, and Kai Hwang, 'Collusive Piracy Prevention in P2P Content Delivery Networks', 'IEEE transactions on computers, vol. 58, no. 7, July 2009'.
- [9]. LanQuan, Kyung Geun Lee, Timothy Mark Pinkston, 'Performance Analysis of Unstructured Peer-to-Peer Schemes In Integrated Wired and Wireless Network Environments', 'Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05) IEEE'.
- [10]. Hiroki Ushikubo, Sonoko Takeda, Hiroshi Shigeno, 'A Reputation Aggregation Method considering File Request Distribution and Peer Behavior in Unstructured P2P Networks', '2013 16th International Conference on Network-Based Information Systems'.
- [11]. Xiaosong Lou, Kai Hwang, and Yue Hu, 'Accountable File Indexing against DDoS Attacks in Peer-to-Peer Networks', 'IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings'.
- [12]. Hyunggon Park, RafitIzhakRatzin and Mihaela van der Schaar, 'Peer-to-Peer Networks – Protocols, Cooperation and Competition'.