Volume 3, Issue 1, January 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Collusive Piracy Prevention in P2P Network

Mrs. Vidya Waykule*
Department of Computer Engineering,
AISSMS's College of Engineering, Pune,
Maharashtra, India-411001

Abhishek S. Naswale
Department of Computer Engineering,
AISSMS's College of Engineering, Pune,
Maharashtra, India-411001

Rahul S. Gaikwad
Department of Computer Engineering,
AISSMS's College of Engineering, Pune,
Maharashtra, India-411001

Mandar M. Mahadeokar
Department of Computer Engineering,
AISSMS's College of Engineering, Pune,
Maharashtra, India-411001

Abhijit R. Jain
Department of Computer Engineering,
AISSMS's College of Engineering, Pune,
Maharashtra, India-411001

Abstract— The primary cause of violation to intellectual property law is collusive piracy. Unpaid clients may get copyright contents from colluders illegally. Such kind of piracy causes to damage to content delivery in P2P network. We propose a system which prevents colluders from pirating the copyright contents in P2P.The firm idea to implement the system is to provide 4 level security mechanism with identity based signature(IBS).The proposed system helps to decrease the piracy without disturbing paid clients by sending unnecessary data i.e. poisonous chunks to violators. We propose Client Authorization Protocol (Cap) to differentiate unpaid client form paid ones. We are assigning time stamp to copyright content file which can be downloaded by paid clients exclusively. Based on simulation results, we find 90 percent prevention rate in Gnutella .We aim to achieve 70 to 80% of prevention rate on eMule. The system is found to be less effective in protecting some poison resilient network like Bittorrent and Azureus.

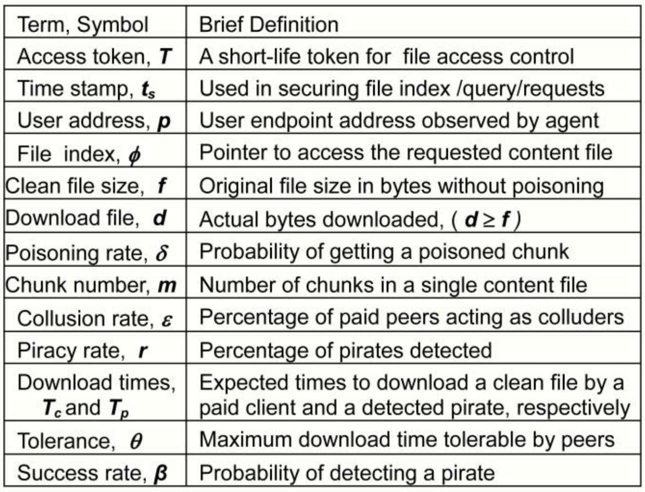
Keywords— *P2P Network, Peer Identification, Copyright Content Poisoning, Legitimate User Authorization Protocol (LUAP)*

1. Introduction

Peer-to-Peer (P2P) networks are networks where there are no client and no server i.e. all the workstations are considered as client as well as server depending upon the operation. Also P2P is most cost-effective in delivering large size files to maximum number of users. Unfortunately, today's P2P networks are abused by illegal distributions of music, games, video streams, and popular software which causes piracy. All of these have not resulted in heavy financial loss in media and content industry, but also restrict the legal commercial use of P2P technology. The main sources of illegal file sharing are peers or the clients who ignore copyright laws and help the pirates. To solve such a kind of collusion problem, we propose a copyright-compliant system for legal P2P content delivery which does not allow pirates in any how in the network. Our goal is to stop collusive piracy within the boundary of a P2P content delivery network without disturbing the existing paid clients. In particular, our scheme force to protect large-scale valuable contents that diminish in value as time elapses. Traditional content delivery networks (CDNs) use a large number of content servers over many globally distributed among the WANs. The content distributors need to replicate or cache contents on many servers. Due to this the bandwidth demand and resources needed to maintain these CDNs are very expensive which give poor performance over CDNs.This drawback of CDN's network is overcome in P2P network. A P2P content network significantly reduces the distribution cost since many content servers are eliminated and open networks are used due to this maximum bandwidth demand of the clients can be fulfill. P2P networks improve the content availability, content security as any peer can serve as a content copyrighted files, even in the presence of colluding peers or the pirators. We use a reputation scheme to detect these colluders.

A copyright-protected P2P network should benefit both media industry and Internet user communities in a large extent. Our work leads to the development of a new generation of CDNs based on P2P technology which reduces piracy in large extent. Table 1 lists important symbols and notations used to benefit our readers. These terms are used to secure file indexes, generate access tokens, quantify poisoning effects, collusion prevention, and define the performance metrics.

We focus on finding solution of collusive piracy within the scope of a P2P network. Inter network piracy between unprotected networks is a much more complex security problem. Our main purpose is to stop colluders from releasing content files freely and provide less effort for the paid clients for clean chunks. Here are many other forms of online or offline piracy that are beyond the scope of this study that are the future scope of our paper. For example, our protection scheme does not work on a private or enclosed network formed by pirate hosts exclusively. As they privately own their own network .We did not solve the piracy problems using email along with attachments, FTP download directly between different colluders, or replicated CDs or DVDs. At present, these direct point-to-point copyright violation problems are mostly handled by digital rights management (DRM) techniques. Though it can handle by DRM but even the protection results are not considered satisfactory as many hackers have post DRM-cracks on internet which causes piracy.



Term, Symbol	Brief Definition
Access token, ***T***	A short-life token for file access control
Time stamp, t_s	Used in securing file index /query/requests
User address, ***p***	User endpoint address observed by agent
File index, ϕ	Pointer to access the requested content file
Clean file size, ***f***	Original file size in bytes without poisoning
Download file, ***d***	Actual bytes downloaded, ($d \geq f$)
Poisoning rate, δ	Probability of getting a poisoned chunk
Chunk number, ***m***	Number of chunks in a single content file
Collusion rate, ε	Percentage of paid peers acting as colluders
Piracy rate, ***r***	Percentage of pirates detected
Download times, T_c and T_p	Expected times to download a clean file by a paid client and a detected pirate, respectively
Tolerance, θ	Maximum download time tolerable by peers
Success rate, β	Probability of detecting a pirate

2. Legitimate User Authorization Protocol (LUAP):

In P2P content delivery every connected peer in the network doesn't know each other's identity (like IP address). Revealing a user's identity to other peers assualts his or her privacy. Every peer gets logged into the network using user ID/password combo, which is verified by content owner only, other users are unaware about that. We proposed a Legitimate User Authorization Protocol to overcome this problem. There are three states in this protocol as follws

1) Secure file indexing using IBS
2) File level Token generation
3) LUAP protocol

2.1 Applying IBS to secure file indexing

To differentiate pirates from paid clients, we proposed to update file index with three strongly connected components an authorization token, a time stamp, a peer signature. File indexing is useful for mapping File ID and peer end point address in P2P network before updating. When a peer wants to download any file, it first sends requests the indexes that matches given file ID. Then the peer who wants to download downloads from currently available peers pointed by indexes.

Bootstrap agent assigns a valid token to it's Legitimate client. Validity of token is depends on the time measure which is stored in time stamp component. After this time client has to get renew his token by distribution agent only. This token is important for protecting copyright of that file against colluders. Cost of refreshing tokens by the distribution agent of client has its boundries limited. The peer signature is the form of digital signature which is containes PKG generated private key, which authenticate peers.

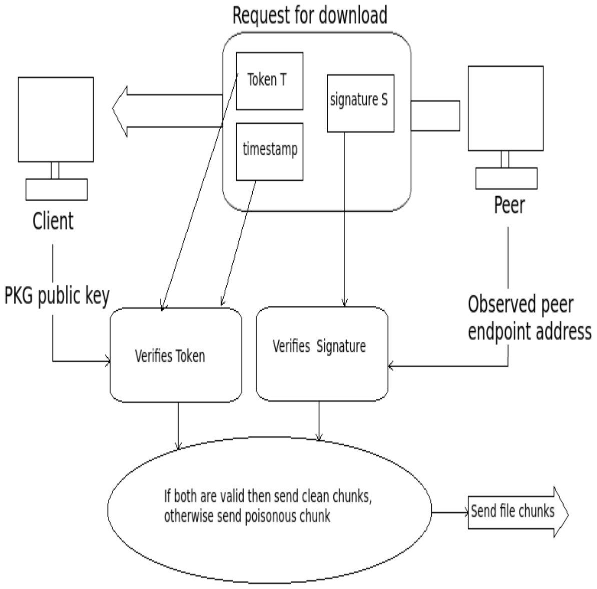
2.2 Generation of token for file:

Trusted components in P2P network are transaction server and the public key generator (PKG) whose public keys are known to all peers. In LUAP protocol, we are going to consider two parts as generation of token and verification of peer. To join P2P network every peer needs to send a request to *bootstrap agent* which verifies the peer. Communication of peer and its bootstrap agent takes place through encrypted messeges (these messeges are encrypted using session key assigned by transaction server at the time of purchasing).

For generation of token for a specified file we use alogithm called *token generation algorithm*. A token is a collection of 3 tuples file ID, peer endpoint ,timestamp. Also we can say that token is a digital signature signed by private key of content owner. In this algorithm, we are passing digital receipt as input. Transaction server sends digital receipt, generated at the time of purchasing of file to bootstrap agent. As peer is also sending same digital receipt to bootstrap agent, bootstrap agent matched that key with the copy of digital receipt sent by transaction server. If digital receipt is valid then token is generated for respective file and peer, otherwise it will deny the request.

2.3 The Legitimate User Authorization Protocol

In LUAP, as shown in above figure a client, who could be legitimate or pirate, requests to download a file with three parameter token, timestamp and signature. All these fields are impotant and must for download file. Token and timestamp are used to verify token is valid or invalid. Signature is also get verified. If any one of the two, token or signature is invalid then poisoning chunks have been sent to requestor, otherwise clean file chunks are get sent.



Firstly, if invalid token is detected then that token could be of legitimate client and might be expired or it could be of pirate. Second one, if signature is invalid then fake end point of requestor is detected. Either of the two cases downloading of requested file will be stopped.

2.4 Adversery and Security Analysis

Hacker can attack on this protocol to crack the system. These attacks are given below with their solution that why thsese types of attacks will get failed against the LUAP protocol. This ensures that our protocol is secured for implementation.

2.4.1 If pirate tries to poison legitimate client

Our system uses file indexing format which contains token and signature. Every client checks the valid signature through file indexes. It can only get connected to other legitimate clients. Though pirate wants to send poisoned chunks to legitimate clients, it couldn't send

2.4.2 If pirate steals private keys

Pirate can get private keys by hacking into the legitimate client system or colluders may share it with pirate. LUAP protocol does not depends totally on private key it also needs peer end point as public key. This public key is obtained by other peers in the network by using observe () procedure .So Stolen private keys are useless for pirates.

2.4.3 If pirate steals token

As explained above tokens are used to verify legitimate clients within peers. This token is generated using three tuple as *file ID, peer endpoint, timestamp*. And *peer endpoint* is different for different peer. That’s the reason peer endpoint is added in token. So, stolen tokens are also useless for pirates.

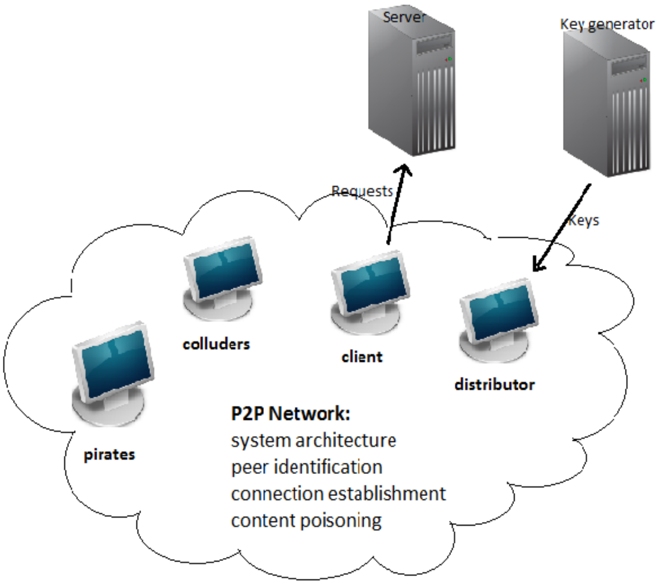
3. P2P Network

A **P2P** computer network is one in which each computer in the network can act as a client or server for the other computers in the network, allowing shared access to various resources such as files, peripherals, and sensors without the need for a central server. Here, conceptual architecture, peer identification, establishment of connection, copyright content poisoning are explained in this section.

3.1 Proposed System Architecture:

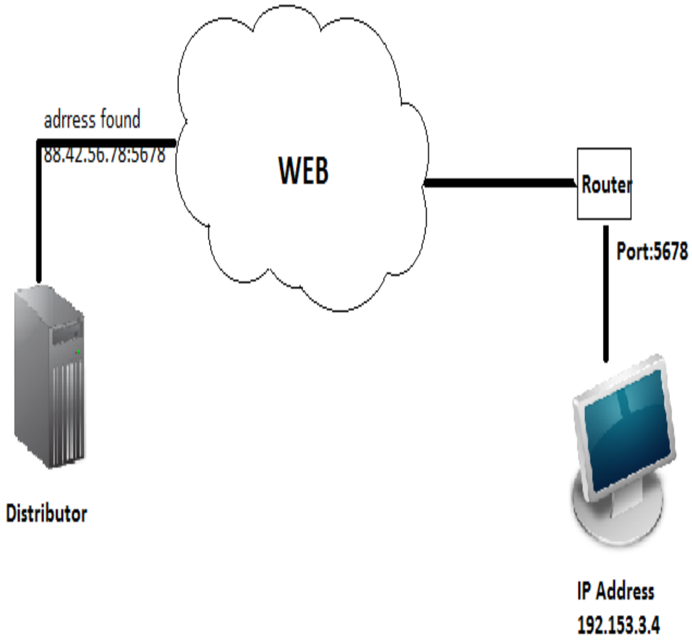
Architecture of our system is shown in figure. Proposed system contains the LUAP(Legitimate User Authorization Protocol) server which handles the user’s transactions. The network contains different types of peers like clients(legal peers), paid client(peers sharing contents with other), intruders/pirates(peers which uses file illegally). One more component is installed to generate the private key for peers i.e. private key generator(PKG).

To get connected to network, peer requests the LUAP server which completes the purchasing process and transactions. On completion of the transaction private key is assigned to peer by PKG. That key is used to communicate among peers in the network. For better service, another type of peer is introduced in the system i.e. distributor. It authorizes the peer to download & prevent s the unpaid clients from getting same contents.



3.2 Peer Identification

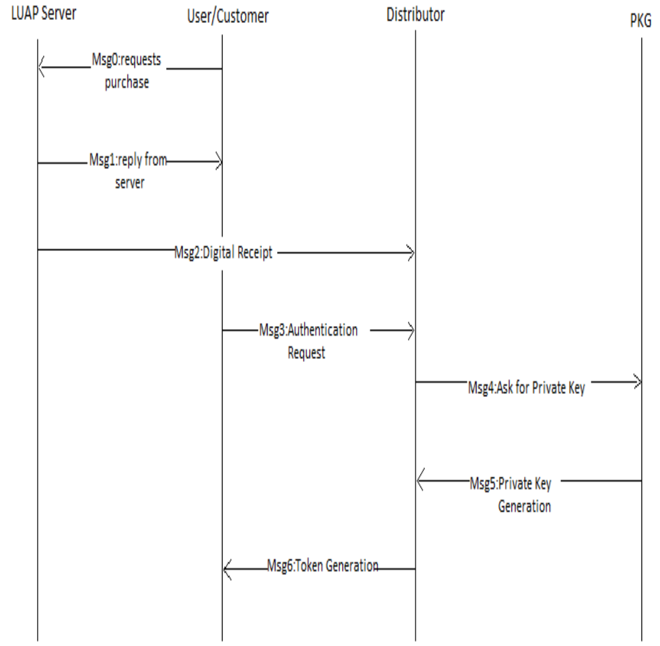
In P2P network, all the peers (clients, colluders, intruders) are all mixed up. It is important to distinguish them. For that each peer is assigned with distributor. Distributor has it's unique port address while peer has it's unique IP address. Combining these two addresses, peer is identified. In home network environment, it is necessary to configure NAT device to forward the incoming port to peer node statically. The constraint occurs when large numbers of peers are behind the single NAT device.



Example: Peer is having IP address 45.67.89.23 and it is listening to the port number 5678 of the distributor. So the peer is identified by 45.67.89.23:5678

3.3 Connection Establishment

The client or peer requests to LUAP server for any copyrighted content. LUAP server makes transactions and replies with address of distributor, digital receipt and session key. Session key is useful for communication for particular session only. Distributor decrypts digital signature and authenticates peer. Then it requests PKG for private key. On getting private key, distributor generates authorization token.



Msg0: Purchase request
Msg1: Reply from server
Msg2: Digital Receipt to distributor
Msg3: Authentication Request from user.
Msg4: Request for private key generation.
Msg5: Reply from PKG with private key.
Msg6: Generation of token.

3.4 Copyright Content Poisoning:

Copyright contents are made bulky by adding poisonous chunks to them. LUAP authorizes legal download privilege to clients. Content poisoning is done to disrupt illegal file distribution to pirates. If pirates make request to client or distributor, it will get only poisonous chunks. Exactly opposite if it makes request to paid client(colluder), It will receive clean chunks. And if it request to other pirate, it will receive mixed contents i.e. clean + poisonous chunks. For file to be useful it should get downloaded fully and if pirate keep downloading poisonous chunks, it will give up attempt out of frustration.

4. Protection Performance Analysis:

Here, the performance of the P2P copyright protection system is take place. Initially, we put the terms to protect the file index . Further , we evaluate the poisoning rate P of arriving poisoned chunk in concern to a pirate's download request. Lastly, we surmise the average file download span T by payable customer and detected pirates for comparison. β is the protection success rate which measures the percentile of pirates that unable to download the requestedfile within a given tolerance threshold.

4.1 Secure File Indexes

File index $\phi(\lambda,p)$ in present P2P networks relates file identifier λ with a station endpoint address p. In LUAP, we replace this index style with a four-tuple style:

$$\Phi=\{\phi(\lambda,p), T,ts, S\}.$$

Where T, S : collision free signatures

Such enhanced index format cannot be copied. Token or signature via brutal-force attack cannot be generated by pirates its own. Thus, self fake index cannot be created by pirate's itself. If pirate want to alter or modify the single bit of four tuple index then should fail in token or signature verification or both. Thus, this enhanced index is strongly secured. There exist a 1:1 mapping of Φ and customer digital receipt This special mapping is the basic of our LUAP protocol as it ensures scattered or distributed pirate searching at every client. Securing the digital receipt is not our aim. Nevertheless PKI service, IBS is used due to concern of overhead in PKI services. Each peer may need to contact all n -1 peers In a P2P network with n peers. By using the IBS despite of PKI overhead to CA communication get reduce to O(n) from O(n^2).

4.2 Chunk Poisoning Rate

An integral function has been used to randomly detect colluders, in our proposed system. Such effect could not be precise. There might be possibility that some unauthorized outsiders will escape the detection. Thus the original sources of copyright violations are these undetected colluders.

5. CONCLUSION

From the above proposal it can be conclude that, the new concept for file indexing using three tuples *file ID , peer end point address & Digital Signature* and poisoning method are useful for preventing collusive piracy.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their valuable comments.

REFERENCES

[1] Xiaosong Lou and Kai Hwang, “Collusive Piracy Prevention in P2P Content Delivery Network,” IEEE Trans computers, vol. 58, no. 7 J 2009.

[2] Y.Kulbak and D.Bickson,”The eMule Protocol Specification,” Technical Report TR-2005-03, Hebrew Univ.Jan 2005

[3] J. Franklin and T. Pepper, “The Gnuttela Protocol Spec. v0.4” Revision1.2,http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf,2000

[4] BitTorrent.org, “BitTorrent Protocol Specification,” http:// www.bittorrent.org/protocol.html, 2006.

[5] S Androutsellis-Theotkis and D. Spinellis, “A Survey of Peer-to-Peer Content Distributio Technologies,” ACM Computing Surveys, vol. 36, pp. 335-371, 2004.

[6] B. Gedik and L. Liu, “A Scalable P2P Architecture for Distributed Information Monitoring Applications,” IEEE Trans. Computers, vol. 56, No. 6, pp 767-782, June 2005