Behavioral Analysis of a Proposed Reputation System for Peer-to-Peer Network

Sunaina Bagga, Chetan Jain, Kaushik Adhikary
Deptt. Of IT, RIMT-MAEC, India

ABSTRACT

Peer-to-Peer (P2P) networking technologies have gained popularity as a mechanism for users to share files without the need for centralized servers. 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. The increasing availability of high bandwidth Internet connections and low-cost, commodity computers in people's homes has stimulated the use of resource sharing peer- to-peer networks. These systems employ scalable mechanisms that allow anyone to offer content and services to other system users. This allows for a variety of applications beyond simple file sharing. Examples include multicast systems, anonymous communications systems, and web caches.In this paper we propose a reputation system for peer-to-peer network with free rider sensitivity.

Keywords

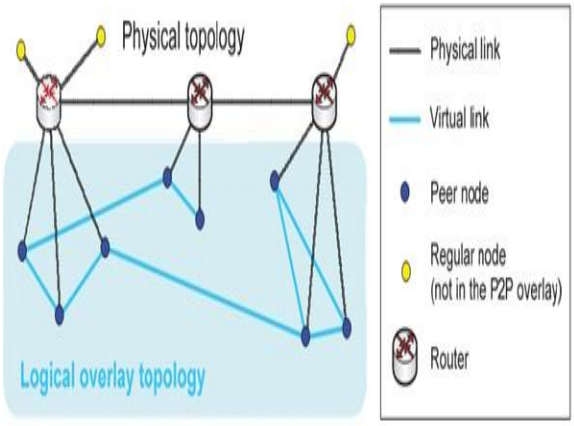
Peer-to-Peer network, reputation system, free rider

1. INTRODUCTION

Peer-to-Peer (P2P) networks are overlay networks on top of the IP network topology. The topology of an overlay is logical, so the underlying physical topology is usually different from the overlay topology. Each peer node maintains a set of virtual links to other peers that become its neighbors, and these links form the overlay network. Every peer knows the location of at least one another node in the P2P overlay. An overlay network is formed by some protocol that uses some specific algorithm to manage the virtual links of the overlay. The protocol also determines the lookup mechanism of the P2P overlay, as the resources have to be found somehow in the absence of a centralized entity. The protocols for network maintenance and search operation can also be separate, like in Gnutella [1].

The absence of a centralized entity also presents the problem of how to join some P2P overlay. The process of finding some node of a P2P overlay is called bootstrapping. There are different ways to locate a bootstrap node, such as multicasting, cached addresses and pre-configuration.

The network architecture of Peer-to-Peer overlay is essentially different when compared to the conventional CS architecture. The main goal of P2P overlay networks is to share the resources such as bandwidth, storage, computation power of participating peers. Thus, taking advantage of this distributed resource network, the usage of centralized servers can be avoided. However, even though good scalability is possible with P2P systems, P2P systems with poor scalability also exist. There are different lookup mechanisms and they also depend on how their overlay topologies are arranged and managed. There are thus many different ways to implement a P2P overlay network, and many different protocols with their algorithms have been developed for P2P systems. P2P overlay networks can be divided into two subgroups, unstructured and structured overlay networks depending on how the peers are connected with each other. The fundamental problem of decentralization is resource discovery, e.g. finding a particular node, service or file. This is done differently in unstructured and structured networks. Today, structured overlay networks are more common among the P2P systems [2].



2. FACTORS THAT AFFECT SECURITY IN P2P NETWORKS

There are many factors affecting the security of any given P2P system. This section will focus mainly on the P2P software. Open P2P networks are often insecure since users can join without any authentication of their identity or proof that the data they are sharing is not malicious software. It is a known fact that P2P networks are used by malicious users to spread viruses, Trojans and other malicious programs. In this system several computers in the network will disseminate information about probable security attacks to each other; this will ensure a rapid spread of information regarding new attacks between the cooperating nodes. Each node will be responsible for:

1. Detecting whether a virus or worm is propagating through the network and possibly causing an epidemic.

2. To automatically send out warnings and information to other peers connected to the network.

3. Take precautions for protecting its host. This can be done by a stricter security policy during the time span of the suspected epidemic.

The hope is that by gathering this information the nodes will be able to estimate when a new wave of attacks are about to happen, and take appropriate countermeasures without the intervention of the user [3, 4].

This method can provide protection against the spread of viruses and Trojans, but will not be able to protect an application against attacks that rely on the actions of the user. It would therefore be important to find ways to protect the

user from performing actions that would result in an increased chance of exposure to attack.

One such method is to make a trust based system available in P2P networks. This goes for both P2P applications by themselves and the data shared on P2P networks. Today there are few ways to confirm the integrity and authenticity of P2P programs; these are programs that usually require full access and privileges on the host computer to operate in a satisfactory way. Since it is nearly impossible to control that the P2P software itself is secure, it is necessary to have architecture to safely run un-trusted code on. When it comes to protecting the host computer from malicious nodes, there are some methods that can be implemented. When users share their data with others, there is a chance that they accidentally share more data than they know. Windows XP users can reduce the chance of malicious users gaining access to sensitive data by using the built in file-sharing features. They can then designate data as either shared or private. Private data can only be accessed by the machine's owner. User should not depend on the built in protection of the P2P software as it can easily be bypassed by an experienced hacker [3, 5].

Backdoor attacks are also a common form of attack, not only on P2P networks, but throughout the Internet. As much as 45% of files downloaded from P2P networks have been shown to contain some form of malicious code. Malicious users can disguise viruses and Trojans in well-known file formats; this is done with software commonly known as "Wrappers". The most efficient way to defend against such attacks is by having up to date antivirus software. This software will analyze any suspicious files and alert users when it detects malicious code. This means that unknown variations of such malicious code will go undetected [3, 5].

3. Pre reputation evaluation algorithm

Input: recommendation received in current period and reputation table

Output: updating new reputation values and reputation levels in reputation table

Procedure:

Group manager s exchange recommendation records in the current period with each other

for each peer p in the group

prep=Rp

for all recommendation about peer p

if reputation repoerter has highest reputation level

then Rp=Rp*(1-α*preq) + Score p,q*α*preq+r

else Rp=Rp*(1-α*preq) + Score p,q*α*preq

endif

endfor

else

if peer p has no recommendation

Rp=prep*β or prep-γ /*degrading reputations*/

if (Rp<0.5 and prep>=0.5)

Rp=0.5

endif

endif

if Rp>=0.8

reputation level of peer p is 5

elseif Rp>=0.7 &&Rp<0.8

reputation level of peer p is 4

elseif Rp>=0.6 &&Rp<0.7

reputation level of peer p is 3

elseif Rp>=0.5 &&Rp<0.6

reputation level of peer p is 2

else

reputation level of peer p is 1

endfor

4. BEHAVIOR ANALYSIS

I have done the implementation of our proposed model for reputation system in Peer-To-Peer network over ns-2 and it is analyzed that said model gives best results.

Following are sample screenshots for the simulation results with this research work which are showing the detailed representation of such mechanisms.

As per Fig 3 shows the simulation (implementation) of our model consists of 25 nodes. The circles inside the simulation represent the groups in Peer-to-Peer network. There is more than one group manager in a group and services are delivered in terms of packet in the group and between the groups.

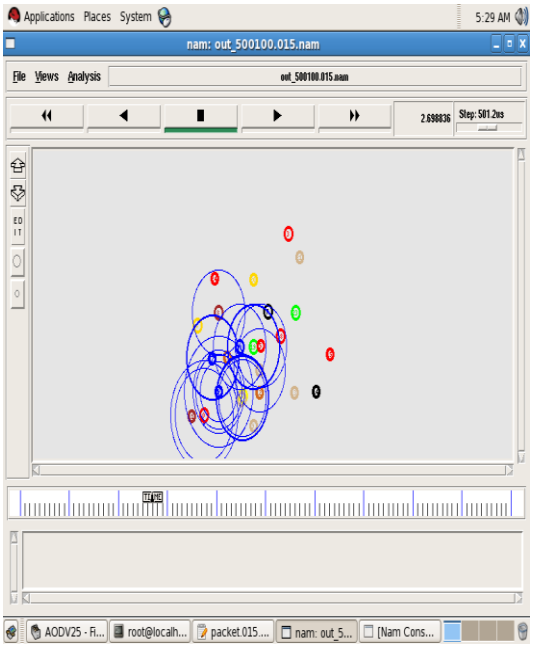


Fig 3: Simulation of the Proposed System

From the Fig.4 it is analyzed that as soon as full network is established number of groups increases to balance load between the groups. In this way maximum services are provides to the network. Surely it will be a flexible and robust model for Peer-to-Peer network.

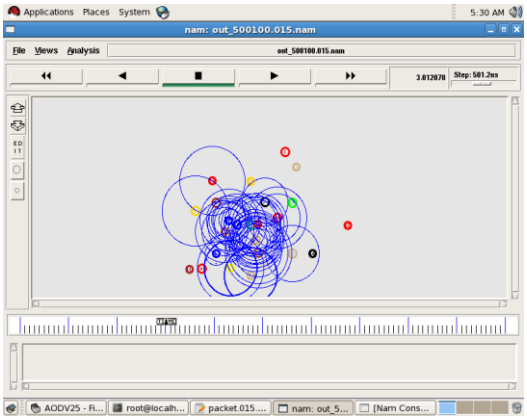


Fig 4: Example of delivery of Services behaviors of the proposed sytem

Fig. 5 shows that groups are communicated for the services. It is not always possible that services are available in to a peer node in the same group so group manager extends the search to another group. So groups need to be communicating other groups for better services. If any malicious node is detected then services are not proved to that node. In simulation packet drops represent that malicious node is eliminated from the network by note giving any service to that node based on their reputation in the network.

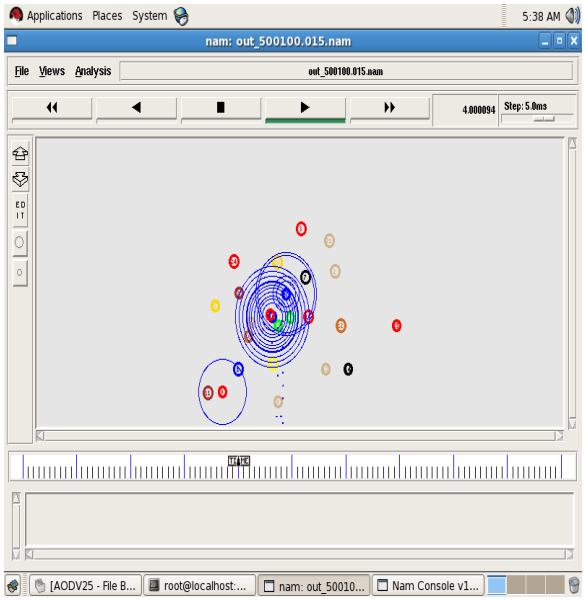


Fig 5 : Example of Packet drops

5. CONCLUSIONS

In this paper a free-rider sensitive and contribution-oriented reputation system including two transaction protocols is presented which is aiming to degrade the willing of free riders and resist malicious file spreading. It uses a semi-decentralized P2P network to decrease network traffic for peer reputation computation. This system stops figuring out all peers in unstructured P2P network by creating group, so each peer figures out all peers that are very difficult in unstructured P2P networks. This system can control the number of exchanges reputation data.

Our reputation management scheme is simple, proactive and has minimal overhead in terms of computation, infrastructure, storage and message complexity. Further more, it does not require any synchronization among peers. This system provides an easy way to find a good file and avoids malicious file spreading in the P2P file-sharing networks. In additions, peers have incentive to share their files to other peers in order to get good services from other peers in the future. It is believed that free riders will be reduced because he cannot download files with high authorized levels if they do not share files to increase their reputation levels.

Performance evaluations show that this system is able to detect and isolate malicious peers from the system, hence providing higher peer satisfaction and better network resource utilization.

6. REFERENCES

[1] Chazapis, A. Tsoukalas, G. Verigakis, G. Kourtis, K. Sotiropoulos, A. Koziris, N. "Global-scale peer-to-peer file services with DFS" 978-1-4244-1560-1 IEEE2007, pp. 251-260

[2] Lua E. K., Crowcroft J., Pias M., Sharma R. and Lim S., "A Survey and Comparison of Peer-to-Peer Overlay Network Schemes", Communications Surveys & Tutorials, IEEE, vol. 7, issue 2, pp. 72-93, 2005.

[3] Rowstron A. and Druschel P., "Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems", in Proceedings of IFIP/ACM Middleware, 2001.

[4] Schafer, J. Malinka, K. "Security in Peer-to-Peer Networks: Empiric Model of File Diffusion in BitTorrent" 978-1-4244-3839-6 IEEE 2009. pp. 9-13

[5] Balfe, S., Lakhani, A.D., Paterson, K.G "Trusted computing: providing security for peer-to-peer networks" 0-7695-2376-5 IEEE 2005 pp.117 - 124