Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 652 – 659

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Resolving Problems Based on Peer to Peer Network Security Issue's

Pravin Wararkar[a]*, Naman Kapil[b], Vyom Rehani[b], Yash Mehra[b], Yashi Bhatnagar[b]

[a]*Department of Electronics & Telecommunication Engineering (Assistant Professor), SVKM's NMIMS (Deemed-to-be-University), Mukesh Patel School of Technology Management & Engineering, Shirpur-425405, India*

[b]*Department of Information Technology (Student), SVKM's NMIMS (Deemed-to-be-University), Mukesh Patel School of Technology Management & Engineering, Shirpur-425405, India*

Abstract

A peer to Peer network, which is a part of highly distributed systems, contains a diverse number of nodes to form a network. These nodes are used to exchange content containing audio, video, data and various kinds of files without the use of a single server as in Client server architecture. Such type of files makes the network highly vulnerable. In the area of peer to peer security, there are five goals - Anonymity, Availability, File authentication, Access Control and fair trading. This paper identifies the security problems and proposes some of the solutions to these threats.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Peer; Anonymity; Fair Trading

1. Introduction

Today BitTorrent is the most widely used file sharing client, people use it for downloading audio, video and various other content using internet. BitTorrent has been working on Peer to Peer Network for almost a decade after P2P network was introduced in 90s.

Securing the P2P Network has been an issue due to the lack of trusted managing authority and instability and further using it doesn't use Client Server Model so it requires more security features. In P2P Network all the peers have equivalent authority and responsibility unlike the Client server architecture. In Client Server architecture, the bandwidth usage of the main server keeps on increasing with the increase in number of clients. More the usage of bandwidth, lower will be the speed provided to the individual clients.

* Corresponding author. Tel .: +91-9960948042

*E-mail address:*pwararkar@gmail.com

Peer-review under responsibility of organizing committee of the ICISP2015

doi:10.1016/j.procs.2016.02.113

Whereas in P2P, more the number of clients higher the download speed and less will be the usage of bandwidth as some part of bandwidth of each individual client is used.

2. Peer To Peer Networks

Peer to Peer networks is organized in a flat structure as a result direct exchange of information takes place between the clients. Taking Bit Torrent as an example, while downloading a file, we are uploading some parts of file while others are being received from different peers simultaneously who may have already downloaded or are downloading the file. This increases the downloading speed.

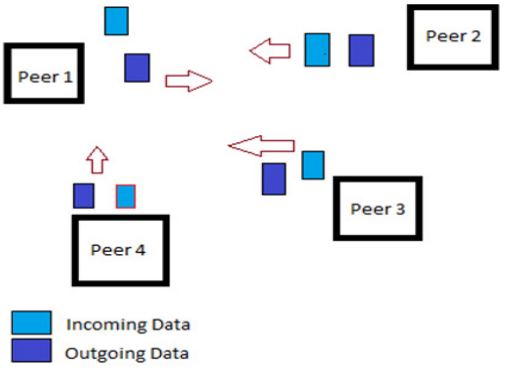

Fig.1 Peers sending and receiving data simultaneously

A peer acts as both server as well as a clientsimultaneously. It is a self-organized and dynamically adjusted structure as the number of nodes may increase and decrease in number anytime. The respective Peer is responsible for finding the appropriate information. If the required data is common, it is easy to search for it but it becomes complex to find a data which is rarely available among the peers.

P2P can be categorized into two types: Structured and Unstructured P2P networks.

- *Unstructured P2P Networks*

In this type of networks, the peers search for the required data within their own network as they are not informed about the exact location of the data. They communicate with each other by flooding the requests which in turn increases the traffic and thus result in wastage of bandwidth. The drawback with this type of network is that, the peers do not know if they will be able to access the respective data or not[6].

- *Structured P2P Networks*

In this type of networks, globally consistent protocols are used for an effective search. A hash table, named Distributed Hash function Table (DHT) is used which provides the ownership to a particular file on the basis some key elements[6].

3. Security Threats In Peer to Peer Networks

These are some of the serious security issues which leads to decrease in the popularity of peer to peer system:

3.1. Eavesdropping

In P2P Network, any unauthorized node can connect to the network and thus eavesdrop the communication

happening between the peers. This hampers the integrity feature of security.

3.2. Communication Jamming

In this attack, the attacker can even jam the network and disturb the network by repeatedly sending false data, joining and leaving the network as well as by routing resulting in denial of service.

3.3. Injection and Modification

Here, the attacker can also flood files containing malicious code like virus, worms, bots and try to infect the nodes in the network. It can also float false files to create congestion in network and try to waste the bandwidth.

3.4. Sybil Attack

Sybil Attack can also be vulnerability as the attacker generates number of pseudo nodes and these nodes break the link between the actual peers and file exchange is not accomplished.

3.5. DDoS Attack

Here, the attacker can exhaust all the resources of the victim so that the victim is neither able to use or provide any services. These can be of two types –

- *TCP DDoS Attack*

All the resources of the victim are malfunctioned by the attacker in this case. By this, the victim will be left with no resources to establish a connection. This can be done by Index Poisoning Attack in which the attacker inserts fake records using the victim's ID or any other identifier. So, whenever another peer would request for the respective file, he would be directed towards the victim's system resulting in the establishment of the fully open TCP connection. In this attack, it is not mandatory for victim to be a part of the P2P network[6].

- *Bandwidth Attack*

The attacker may occupy the whole bandwidth of the victim so the victim is now not able to share anything. In such attacks the attacker acts as the neighbour of many in the routing table. And whenever a peer would want to share something, then he may choose the attacker as its nearest neighbour instead of choosing the appropriate peer. Considering there are millions of users, it may lead to overloading of the bandwidth, resulting in Bandwidth DDoS attack[6].

4. Structure For Secure Communication

Following are the key measures which should be considered for a safe and secure communication in peer to peer network[6 8],

4.1. User authentication

Before joining the network, every peer must prove its identity, which can be done using mechanisms like, username and password or any other unique identifier.

4.2. Privacy protection

Anonymity is one the key feature in security in which the real identity of the user is not revealed.

4.3. Data integrity

This feature deals with the genuineness of the data. The data must be protected from any unauthorized access as the attacker can add malicious code that can modify the data or can even change the data completely.

4.4. Access control

This feature of security makes the system secure by allowing access to only those users who have certain set of rights which makes them eligible to access that data.

4.5. Usability

The interface should be user friendly so that the user can easily understand and change the settings according to his preferences. More complex the interface more will be the chances that the user might choose such a setting that might be a threat to the network.

4.6. Availability

The data should be available to the authorized user whenever he requests for it.

5. Measures For Secure System

These are some of the measures which can be taken into consideration to fulfil the requirements of security.

5.1. Encipherment

The data being exchanged between the peers should be in the encrypted form. This can be done using classical cryptosystem.

5.2. Key exchange

The keys used for encryption of data must be safely exchanged between the peers.

5.3. Access control list

This list is object oriented, that is, the subject's access is presented with respect to the object.By subject we mean the user who wants to access and by object we mean the data he wants to access. This helps to prevent the unauthorized access.

5.4. Notarization

In this, time stamp and the origin can help to manage the integrity of the file.

6. Major Problems And Their Proposed Solutions

6.1. Incentives

Majority of the users of the peer to peer network are not cooperating and not contributing to the network. They download data from other peers, but do not share data themselves, and this is what we call as free riding. Free riding is a serious threat to a peer to peer network which hampers availability of data. Due to such threats, only some of the

users are sharing and further they are also losing interest in the system as there are very less files, and further this may restrict the system from being operational.

Consider a system having N peers and only N_s peers share data and on an average, if there happens to be R requests per unit time then, R/N_s requests have to be managed by peers per unit time. Less the value of N_s, more the load on peers, which may lead to CPU overload of the peers. To prevent such problems incentives mechanisms are used, one of them is Barter Mechanism[5 6].

- *Barter Mechanism*

It is trade based incentive system where the consumer remunerates the provider by providing a service in return, and this service can be executed during or immediately after the provider provides the service, or the service can be delayed with a promise that it will be executed in future. This scheme is quite popular in Bit Torrent file sharing client. Barter Trade system provides control over Free-Riding, but problem here is finding peers who are exchanging same files, this becomes a big issue as the system has less number of clients, but within a large group this can be done easily. Another big advantage of barter trade system is anonymity as the services are exchanged immediately.

6.2. Reputation and Trust

Data sharing system is the most popular peer to peer network. In such systems users can search for files and download them, so it consist of 2 phases - content search phase and content download phase.

In the search phase, a node generates a query and sends it to all other peers whom he is directly connected to, in turn these peers forward it to their neighbouring peers. If some node has the requested content then it may reply to the node who sent the query, and now the user can download the file. This is the content download phase.

Now comes the threats involved in the search phase, malicious nodes can restrict forwarding queries to other nodes or they can change the query itself or then can reply that they have the content even if they don't have and send malicious programs during the content download phase, here comes in the concept of reputation. Peers are assigned reputations based on the content they provide and their behaviour, a peer with less reputation will not be selected for download phase.

These reputations scores are assigned by Reputation Computation Agent (RCA), so peer to peer network cannot be called as fully decentralized system. Each peer generates a public, private key pair and shares it with the central RCA. RCA also has its own public and private key pair and it shares its public key with every peer registered in the network.

For every contribution each peer keeps it *proof of processing* (PP) and further contacts RCA to get credits and RCA computes reputation of each peer on the basis of these PP.
Disadvantage with this approach is that if a new peer enters the network then his reputation will be less comparative to others and users won't download data he is sharing so he would never be able to increase its reputation in such a case.

One solution to this problem is that the RCA can assign a specific reputation score to a new peer that connects into the network and if the performance of the peer is not upto the mark then the score will be decreased and if the service provided is not posing any problem to other peers then the score will be increased and a new peer can gain reputation[5].

- *Problem in Reputation Mechanism*

Within an Intranet multiple peers are connected to each other and they may exchange data with each other. Suppose there exists a peer that has currently gained a high reputation by contributing effectively to the peer to peer network. It may happen that this peer, having high reputation, can try to harm the network using malicious programs and take

advantage of its high reputation, because other peers will trust it based on the reputation score and download files from the peer without any hesitation. This can harm a numbers of peers in the network.

- Now the peer who has been attacked might not be able to provide an accurateinfo to the authorityas its system might be damaged by the attack.

- Similarly the user may sometimes not be able to inform the authority about the attack and the reputation of the provider peer may not be hampered and it may continue to harm other peers also.

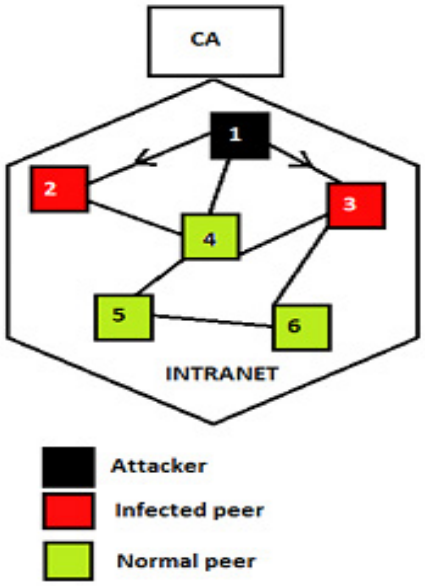

Fig 2:- Reputation Mechanism Problem Resolver Framework

Solution proposed to this problem is:

We introduce a Central Authority (CA) so that the network is not fully decentralized. For each Intranet there exists a CA which monitors and checks the network and identifies any malicious activity.

What CA does is that it will randomly scan the whole Intranet for malicious data transmission and trace the peer who is sending the data and it will directly affect the reputation of the peer, so that the other peers don't download the data after an attack has been done by the provider. In this way the misuse of the reputation can be stopped.

Another measure that can be applied is that a network can have a particular pattern so the CA can look for any unusual behaviour. If it finds something wrong in the network, in can immediately stop transmission of data so the uninfected peers could be saved. For example, in normal conditions two or three peers leave the network but in a state where an attacker is passing malicious data to peers, large number of peers will start getting damaged and disconnected from the network. Here the CA can recognize the unusual behaviour and can stop the attacker from any further damage.

7. Applications

- The most popular application of peer-to-peer network is Bit Torrent. For this, the Reputation mechanism problem resolving framework solution can be used much effectively.

- Just like Bit Torrent, another P2P program is Pando, which is more geared towards simplicity and security. So proposed Framework can be applied upon this program.

- Skype is also decentralized. It does not involve a complex infrastructure. It is a type of Real time communication.

8. Future Scope

- Using the central authority in any peer-to-peer network will help to prevent the peers from getting infected by any malicious code or data.

- The main advantage of the proposed framework solution is that it checks the data before it is sent. This advantage of proposed solution is effective in terms of both, network as well as the peer because it prevents the infected data from entering the network which in turn, prevents the data from reaching the peer, protecting the peer from any damage.

- Using the proposed framework solution, Data will be more secure which in turn will increase peer's trust and can be used for multiple programs.

9. Conclusion

In this research paper, we have tried to answer certain questions on security in peer to peer network. We have proposed certain solutions for some attacks that take place in peer to peer networks. We started our research by trying to find out the answers for what, when and how for the attacks. After overcoming the drawbacks of the solutions already proposed and the one after our research, lead us to the solution as mentioned above.

According to the solution as mentioned in the last section, a central authority will be responsible for the security of all the peers in an Intranet network. All the data before being sent (Even if the data is being sent to another network) will be checked by the central authority. This check, by the central authority, will be mainly based on the genuineness of the data irrespective of the reputation of the sender in the network. Reputation of the sender was mainly taken into consideration as it may happen that the sender may increase its reputation by first sending genuine data but can later try to take advantage of its reputation for sending malicious data. If this data is accepted by any peer in the network, then it may infect him to the extent that the peer may not be able to give the score for this data, making it difficult for other peers to know that this data is infected. This is where the need of central authority came into action.

There are still many questions in this area, on which we want to devote our work in the future.

10. Acknowledgement

The authors would like to thank the anonymous reviewers for the many helpful comments and suggestions.

11. References

1. Yasutomi, M.Mashimo, Y and Shigeno, H. GRAT.Group Reputation Aggregation Trust for Unstructured Peer-to-Peer Networks.IEEE 30th *International Conference on Distributed Computing Systems Workshops (ICDCSW)*; 2010. p. 126 – 133.
2. Johnson, M.E, McGuire D. and Willey, N.D. The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users. *Hawaii International Conference on System Sciences*, Proceedings of the 41st Annual; 2010. p. 383.
3. Chopra, D., Schulzrinne, Henning Marocco E. and Ivov, E. Peer-to-peer overlays for real-time communication: security issues and solutions. Communications Surveys & Tutorials, IEEE; 2009. p. 4-12.
4. Huang Kun, Wang Lu. Research of Trust Model Based on Peer-to-Peer Network Security. International Conference on Information Technology and Applications (ITA); 2013. p. 126-129.
5. Jochem van Vroonhoven. Peer to Peer Security.*4th Twente Student Conference on IT*, Enschede; 2006.
6. Tatsuaki Hamai, Masahiro Fujii, Yu Watanabe. *ITU-T* Recommendations on Peer-to-Peer (P2P) Network Security", Autonomous Decentralized Systems, ISADS International Symposium; 2009. p. 1-6.
7. Jung-Tae Kim, Hae-Kyeong Park, Eui-Hyun Paik. Security issues in peer-to-peer systems. *Advanced Communication Technology, ICACT. The 7th International Conference*; 2005. p. 1059-1063.
8. Schafer J, Malinka K., Hanacek P. Peer-to-Peer Networks Security.*Internet Monitoring and Protection, ICIMP. The Third International Conference;* 2008. p. 74-79.