Abstract—This chapter provides detailed of attacks on Peer-to-Peer network with their suitable defensive technique or algorithm. We try to reduce the effect of Sybil attack from p2p network. In peer-to-peer (p2p) network is a way of structuring distributed applications such that the individual nodes have symmetric roles. Peer-to-peer network having no any hierarchy that means all peers are equal and no administrator responsible for the network. There are a several kinds of attacks in peer-to-peer network. Like, DOS Attack, DDOS attack, Rational attack, Sybil attack and Eclipse attack. In Sybil attack, Attacker create Fake Identities on p2p network either to gain better reputation or increase download capabilities or take entire control over network. A faulty node may present multiple identities to a peer-to-peer network and then after becoming part of the p2p network and act maliciously. By using Reputation ranking algorithm after efficient changing we can check the reputation rank of all the peers connected to that network. After checking the reputation rank we decide which nodes are real and which nodes are fake. That means aim of reducing Sybil attack is done from the following proposed flow and algorithm.

Index Terms—Sybil Attack, Self-certification Algorithm, Peer-to-Peer Network, Reputation Management.

I. INTRODUCTION

To reducing the effect of Sybil Attack in Peer-to Peer network, we can do reputation management on peers and after applying simulations on the simulator to reducing the effect of Sybil attack.

Peer-to-Peer network is a way of structuring the distributed applications such that individual node have symmetric roles. Peer-to-Peer network is also called a workgroup. Peer-to-peer network is different from client-server architecture because in peer-to-peer network, one specific peer acts as either client or server. Peer-to-Peer using a decentralized model in which each machine, referred to as a peer, functions as a client with his personal coat of server functionality. A couple plays the role of a client and a server simultaneously. Customers (pairs) will the necessary operations to keep it going rather than a central server network.

In Sybil attack, attacker creates fake identity on to the network to take the control over part of the network and after that control over a whole network. The idea behind Sybil attack is that a single malicious identity can present multiple identities, and thus gain control over part of the network. Sybil attack can be seen in social network, structured p2p network and distributed p2p network. Effect in distributed p2p network of Sybil attack is more harmful than other network. This problem of Sybil attack is reducing by giving reputation ranking to all the peers in distributed peer-to-peer network.
II. ATTACKS ON PEER-TO-PEER NETWORK

There are different types of attacks on peer-to-peer network.

A. Denial of Service (DOS) Attack

DoS attack is an attack on a computer or a network, trying to make a computer resource available to its users. In P2P networks, the most common form of DoS attack is an attempt to flood the network with dummy packets, thus preventing network traffic reasonable. The second method is to drown the victim demanding node to node becomes too busy to respond to other questions computation. Defense: Pricing technique is used for defending against this attack in peer to peer network. Where the host will submit the puzzles to the all its clients. When attacker want to attack on any victim then he has to solve a puzzle first, that’s why difficult for attacker to attack on p2p network.

B. Distributed Denial of Service (DDOS) Attack

DDOS attack is the modified attack technique that uses DOS attack. The figure of the main attacker who controls the different partitions. The sub attackers are often personal computers with broadband connections that are committed with the Virus or Trojan. That means attackers sub attacks on the network and control the entire network for the main attacker.

C. Man-in-the-Middle Attack

Man-in-the-middle attack is an indirect interference, and the attacker inserts your computer undetected between two nodes. In the figure, Alice and Bob are regular users. Showing the attacker in the middle can intercept the data, modify data and send data without being detected by Alice and Bob.

Defense: Authentication technique is used for solving this type of attack on p2p network. In this defense technique the information is encrypted by the user before transmitted to another user. After transmitting this information second user want to decrypt that information. Without knowing how to decrypt the message, second user can’t get that message therefore attacker unable to intercept the message.

D. Pollution Attack

The network attacker is to replace a file on the network for any malicious file, and this file unusable polluted than customers. The attacker makes the target content unusable changing the content of it in content independently, and then makes this content available for sharing contaminated. In order to attract people to download the contaminated content, harmful content must disguise as the target content, such as having the same format and similar size. It is also necessary to maintain broadband connections.

Defense: To ensure our system this attack; if the user learns the downloaded files are harmful, then the user should be to remove that file from the P2P system.

E. Rational Attack

For our selfish behavior at the expense of the system it can be termed as rational Attack. In the figure above, if the node A wants to transmit the content. To reduce the bandwidth load on node A, only a small number of node B and node F connected directly to A. The contents were then propagates from node B and node F to additional services such as the node pairs C, D and E. because of the behavior auto-interested in most P2P systems, a self-interested node may realize that you can
save expensive bandwidth rise if not choose to share. In this case, enough nodes B and F become self-interest, so the system cannot guarantee a reasonable charge and discharge.

G. Eclipse Attack
In a fit of Eclipse, an attacker control over much of the good neighboring nodes. In this scenario, the collection of harmful nodes works together to fool a good node writing their addresses in the list of neighbors of a good node. Using Eclipse attack, an attacker can control on an important part of a network, even across the network. Thus, nodes cannot forward correctly and then the whole network can be managed message. Sybil attack can be simplified as a specific attack Eclipse, if the attacker generates lots of identifications to act as a good neighbor node.

F. Sybil Attack
Attacker create fake identities on peer to peer network for gaining better reputation or increasing download speed and taking the entire control over the network. The idea behind Sybil attack is that a single malicious identity may have multiple identities, and thus gain control of part of the network.

From the above figure of Sybil Attack, when a normal node makes redundant backup, select a group of entities as the node A, B, C and D have different identifiers. But in fact, the B, C and D node does not really exist, because the malicious nodes are created by the attacker, so the backup may not finish. A faulty node (Malicious Node) or an adversary may present multiple fake identities to a p2p network in order to appear and function as multiple distinct nodes. After becoming part of the peer-to-peer network, the adversary may act maliciously. By masquerading and presenting multiple identities, the adversary can control over the whole network.

Defense: Self-Certification Algorithm and Reputation Ranking Algorithms is used for defending against Sybil Attack.
A new node hashes the IP address and port for the calculation of its identifier, and then recording its identifier in the already registered nodes, which are the whole process of registration of the new node. Then, later, the new node requests to join the P2P network. Other registered nodes have the ability and the responsibility to identify if the new node is real or not. If the new node is real, then it will be accepted by the P2P network.

**Registration Nodes:** Registration procedure in the nodes, the nodes is verified that are not fake nodes.

**New nodes:** In this procedure, a node checks your ID and record ID are mapping one by one.

**V. LITERATURE REVIEW**

1. **A Survey of Peer-to-Peer attacks & Counter Attacks**

In this survey paper, Author has given explanation about all the attacks and defense on peer-to-peer network.

2. **The Sybil Attacks and Defense**

In this article we take a close look at the Sybil attack and advances in the defense against it, with special emphasis on recent work. We identified three large veins in the research literature that describes ways to defend against the attack: the use of trusted certificate, using the means test, and the use of social networks. Our study and analysis of the various schemes of the three veins in the literature show several deficiencies, which are several interesting directions and research questions worthy of investigation.

3. **Defending against Sybil Attack in P2P Network**

In this paper, we present a novel system to defend against Sybil attacks. Our direct and indirect transaction protocols limit the number of service units that a node can obtain. Furthermore, we design a dynamic reputation ranking algorithm for the indirect transaction protocol. Combining these two, a node with a high priority has more probability of obtaining service.

4. **Parental Control Algorithm for Sybil Detection in Peer-to-Peer Network**

Distributed social peer to peer network are most vulnerable to Sybil attack. It forms a small network within the P2P network and can give unwanted results to other nodes in network, thereby decreasing the interest of non-malicious nodes in the P2P network. We are proposing a Parental Control algorithm which is based on reputation scheme. It uses the false message concept for identifying and verifying the Sybil nodes in to the peer-to-per network.
VI. PROPOSED WORK

In my Proposed Work, I have used two algorithms for detecting Sybil Attack in Peer-to-Peer Network. First is Self-Certification and second is Reputation Ranking Algorithm.

**Stepwise Proposed Work**

1. First we give the certificate from third-party authority to the peers who want to participate in P2P network.
2. Requester (Peer) sends or broadcast the request in P2P network.
3. All Providers have those service or files reply to the requester.
4. Then Requester calculates the reputation rank of all providers who has responded to the request.
5. Requester accepts the service from maximum reputation rank service provider.
6. If Service completed successfully then increase the reputation rank of the provider & goto step 8; else decrease reputation rank of the provider.
7. If Reputation rank<=0 then delete that node & goto step 2; else repeat the procedure from Step 2.
8. End.

**Comparison of the results for existing and proposed scheme**

![Communication Cost (Payload Length)](attachment://chart.png)

VII. CONCLUSION & FUTURE WORK

The goal of Reputation Management of Peers is to reducing the fake node in peer-to-peer network and makes the network more secure. First we gave certification authority to the peers and after that requester broadcast request for files, after that providers those have that requested files reply to that requester. After that requester calculates the reputation rank of those providers. Then requester took files from highest reputation rank provider. This is the main aim of Reputation Ranking in peer-to-peer network.

As per the research, future work extends that we can calculates Reputation rank of the providers only that’s why in future, If calculations of the reputation rank of both requester and provider then we can make it more efficient.

ACKNOWLEDGMENT

I would like to give thanks to Prof. Chaita Jani (Asst. Prof, Computer Department, KITRC, Kalol) and also Rahul Vaghela (ME Completed from L.D. College Engineering-2013). Without support of them this work cannot be completed. Their Motivational Supports and valuable guidance always encouraged me time to time.

REFERENCES


