International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Comparative Study and Evaluation of Solving Sybil Attack on Peer-To-Peer Network

Anju Shukla[1], Prachi Damodhar Shahare[2]

[1]M. Tech Scholar, Department of Computer Science Engineering (OOSD), Kalinga University Raipur, Chhattisgarh

[2]Assistant Professor, Department of Computer Science Engineering (OOSD), Kalinga University Raipur, Chhattisgarh

Abstract: ***In computer networks, computing devices allows to exchange data with one another via a data link. Peer-to-peer model (P2P architecture) is a frequently used computer networking architecture in which each workstation, or node, has the same adaptability, capabilities and responsibilities. The idea behind this attack is that a single malicious identity can present multiple identities, and thus gain control over part of the network. Various counter measures to avoid the damages through this attack are considered [3]. The algorithms has already been proposed for mitigating the impact of Sybil attack in peer to peer network, but the detection of Sybil node is only on the sender side. In this paper, the algorithm is introduced which can detect the Sybil node on peer to peer network in both sender as well as receiver side. This will help to identify the malicious node and to maintain the consistency of information on network.***

Keywords: Peer-to-Peer (P2P), Sybil Attack, security threats, various attacks

1. Introduction

Peer-to-Peer systems offer an alternative to traditional client-server systems for some application domains. Peer-to-peer (P2P) networks connect many end-hosts (also referred to as peers) in an ad-hoc manner. Peer-to-peer systems (P2P) have emerged as a significant social and technical phenomenon over the last year. Two factors have fostered the recent explosive growth of such systems: first, the low cost and high availability of large numbers of computing and storage resources, and second, increased network connectivity. Unlike traditional distributed systems, P2P networks aim to aggregate large numbers of computers that join and leave the network frequently and that might not have permanent network (IP) addresses. In pure P2P systems, individual computers communicate directly with each other and share information and resources without using dedicated servers. It differs from the traditional client-server model where a client can only send requests to a server and then wait for the server's response [10].

In computer networks, computing devices allows to exchange data with one another via a data link. Peer-to-peer model (P2P architecture) is a frequently used computer networking architecture in which each workstation, or node, has the same adaptability, capabilities and responsibilities.

There are different kinds of peers in a P2P network:

- Malicious peers is a collection of answering queries with fake identities it try to present multiple similar identities, it can modify the request coming from the honest peers.
- Compromised peers must have self healing technique; it recovers automatically from any state. Sybil attack peers create more non existing links with honest peers.
- Honest peer are trusted peers which have maintained the trusted connections between the peers.
- Sybil peer is a peer which shows a lot of changes in their identities is said to be Sybil peer.
- Legitimate Peer is a peer having fake identity, but it doesn't involve physically within a network, it has many neighbors with honest peers and legitimate peers.
- Intermediate peer is nothing but an honest peer, it receives the request coming from the peer and checks the trust value to confirm and send back acknowledgments to other peers.
- Neighbor peer is a peer which does not need any central peers to monitor other peers. It has a direct and indirect evaluation.

Peers are equally privileged, equipotent participants in the network and said to form a peer-to-peer network of nodes [6].

There are various advantages of peer to peer network over client-server network such as

- All the resources and contents are shared by all the peers, unlike server-client architecture where Server shares all the contents and resources.
- It is easy to install and so is the configuration of computers on this network.
- There is no need for full-time System Administrator. Every user is the administrator of his machine. User can control their shared resources.

There are various types of attacks in peer to peer network which are as follows:

1. Routing attack
2. Denial of Service (DoS) attack
3. Poisoning attack
4. Sybil attack
5. Eclipse attack

Routing attack: In DHT based P2P network, each node maintains a routing table and the routing table promises the look up and mapping of the keys. A malicious node which serves as an alive part of P2P network can perform some abnormal behaviors. A typical attack is that the antagonist forwards the look up request to an incorrect node.

Denial-of-service (DoS) is a common attack but difficult to be rescue both in conventional internet and peer-to-peer networks [7]. In DoS attack, antagonist utilizes reasonable service requests to exhaust the resources of a target host. Therefore, the victim host can not provide any service to other legal intended users.

Poisoning attacks can occur in the P2P networks. Antagonist use fake information, for example, fake file indexes, false routing tables, or false IP addresses, to break the integrity of P2P systems[1].

Sybil Attack: If the relation of entity to identity (i.e., one-one mapping) is destroyed by malicious peer, in other word, a malicious entity behave as a number of multiple identities[7]. The entity can handles a significant part of networks and such attack is defined as Sybil attack. This attack can occur in all the networks that require the entity and identity mapping, such as, P2P networks, ad-hoc and sensor networks.

Eclipse attack is a general attack in overlay networks. In eclipse attack, an antagonist controls a large part of the neighbors of a good node [3].

2. Routing Strategy

Routing is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. Routing is performed for many kinds of networks, including the **telephone network** (**circuit switching**), **electronic data networks** (such as the **Internet**), and **transportation networks**. It's also referred to as the process of choosing a path over which to send the packets. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. There are various types of routing strategies are considered in the computer network, the brief details are as under:

a) Fixed Routing
In fixed routing a route is selected for each source-destination pair of nodes in the network. The routes are fixed; they may only change if there is a change in the topology of the network. A central routing matrix is created based on least-cost path, which is stored at a network control center. A route is selected for each source-destination pair of nodes in the network. There is no difference between routing for datagram's and virtual circuits. In fixed routing, the flow of network is simple, but it does not provide flexibility. In terms of refinement, it supplies the nodes with an alternate next node for each destination [4].

b) Flooding
Flooding requires no network information whatsoever. Every incoming packet to a node is sent out on every outgoing line except the one it arrived on. All possible routes between source and destination are tried. A packet will always get through if a path exists. The properties of flooding are as follows:

- All possible routes btw source and destination are tried
- At least one copy of the packet to arrive at the destination will have a minimum-hop route
- All nodes connected to the source node are visited

c) Random Routing
In this routing strategy, node selects one outgoing path for retransmission of incoming packet and the selection can be random or round robin basis. Thereafter, assign a probability to each outgoing link and to select the link based on that probability. In random routing network information is not needed for further processing and route is typically of low cost or minimum hop.

d) Adaptive Routing
Dynamic routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change [11].

3. Related Work

Author (Aggarwal, 2015) discussed about the impact of Sybil attack and the counter measure to avoid the damages through this attack. Author quotes an example to familiarizes with the Sybil attack, an online voting system where one person can vote using many online identities. The specific types of Sybil attack covered by the author such as Routing, Tampering with Voting and Reputation Systems, Distributed Storage & Data Aggregation. The counter measure applied to procure from the attacks such as Trusted Certification, Resource Testing, & Identity Distribution Scheme. This types of schemes helps to counter the impact of malicious user.

Sybil attack is an attack where malicious users obtain multiple fake identities and access the system from multiple different modes. It is an attack wherein a reputation system is destroyed by falsifying identities in peer to peer networks. Communication between the users of networks only requires the users to be part of the same network. All kinds of distributed systems are capable of being wounded to Sybil attacks. The Sybil attack was described in different networks like social networks, sensor networks and peer to peer networks. In Sensor Networks, author uses several new defenses against the Sybil attack including radio resource testing, key validation for random key pre-distribution, position verification and registration. (Dr. S. Justin Samuel, 2015)

Author explains the concept of SybilGuard which helps to protect from the attacks. SybilGuard is designed such that it needs to respond only to user creation/deletion, and not to node churn (i.e., not to nodes going offline and coming online in possibly unpredictable ways). The social network definition in this paper always includes all users/nodes that have been created and not yet deleted, regardless of whether they are currently online or offline. Author uses, the model which was globally accepted Kleinberg's synthetic social network model in their evaluation of guarantee of Sybil Guard. A novel decentralized protocol for limiting the corruptive influences of sybil attacks, by bounding both the number and size of sybil groups. SybilGuard relies on

properties of the users' underlying social network, namely that (i) the honest region of the network is fast mixing, and (ii) malicious users may create many nodes but relatively few attack edges. (Gupta & Awasthi, 2011).

Authors present SybilGuard, a novel protocol for limiting the corruptive influences of Sybil attacks it is based on the "social network" among user identities. SybilGuard relies on properties of the users' underlying social network, namely that the honest region of the network is fast mixing. Malicious users may create many nodes but relatively few attack edges. Authors described a Sybil defense mechanism that leverages the network topologies to defend against Sybil attacks in social networks. Based on performing, a limited number of random walks within the social graphs are formulated. This approach focuses on restricting nodes to obtain the number of service units in a reasonable level. Here author mainly focuses on two fields Sybil-resilient protocol by which node can obtain service in reasonable level and therefore defeat against Sybil attacks. They develop a dynamic reputation system which holds the property of Sybil-proof. (Sharma & Dhawan, 2013)

Author (Nitish Balachandran, 2012) discussed about the decentralized distributed network which is particularly vulnerable to the Sybil attack. In this paper the different kinds of Sybil attacks including those occurring in peer-to-peer reputation systems, self-organizing networks and even social network systems. In addition, various methods that have been suggested over time to decrease or eliminate their risk completely are also analyzed along with their modus operandi. Author also distinguishes various kinds of Sybil attacks that can be launched on various application domains and also listed notable methods that have been proposed over time to tackle these attacks. Thereafter, elaborated on their modus operandi, advantages, and limitations.

4. Classification of Peer to Peer Network

P2P networks can be roughly classified into two types:

Pure P2P networks
In a pure P2P network, all participating peers are equal, and each peer plays both the role of client and of server. The system does not rely on a central server to help control, coordinate, or manage the exchanges among the peers. Gnutella and Free-net are examples of a pure P2P network [2].

Hybrid P2P networks
In a hybrid P2P network, a central server exists to perform certain "administrative" functions to facilitate P2P services. For example, in Napster, a server helps peers to "search for particular files and initiate a direct transfer between the clients". Only a catalogue of available files is kept on the server, while the actual files are scattered across the peers on the network. Another example is Bit-Torrent (BT), where a central server called a tracker helps coordinate communication among BT peers in order to complete a download [2].

5. Proposed Work

The known promising ways for defending against Sybil attacks can be done by verifying node resources. In this work, the packets were sending from the source location to the destination location. Number of packets carrying information routes the network. In the routing table the information regarding different parameters like number of nodes, source node , destination node, next hop, time taken to travel from one node to another are shown and the details of the routing table:

Node	Time	Source Node	Destination	Next Hop	Sequence	TOL	FLAG
16	1.004	0	0	2	4	7.004	1
15	1.018	16	16	1	4	11.01	1
15	1.108	0	0	1	4	7.001	1
15	1.017	16	19	1	4	11.01	1
15	1.017	0	0	1	4	11.01	1
0	1.035	16	15	2	4	11.03	1

In this trust based mechanism we are maintaining two list of tables which contains node, source node, time, sequence, destination, next hop, flag, time of leaving that node. In this work the frequency of packets is measured as packets send from sender node to destination node is calculated with respect to time. Similarly for the receiving side the backup is prepared for further course of action. This will help to identify the number of nodes received in another end and also help to trace the impact of Sybil node. If the number of nodes received is less than the actual then it reflects the Sybil node manipulates the data in the network and the rest of the node will suffered from the attack.

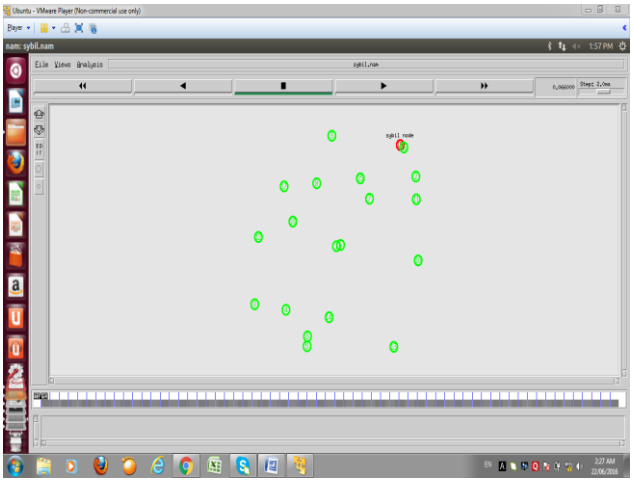


Figure 1: GUI of the simulation

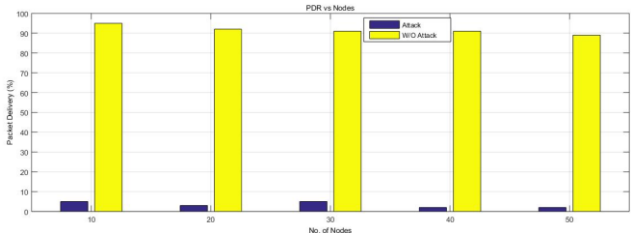
In figure 1, green nodes imply the sender side nodes and the red nodes imply the Sybil nodes. With the help of this mechanism it helps to detect the number of packets approximately received as same sends by the sender. In this simulation we are actually explaining the Sybil node 19 which receiving packets from 0 node but not sending it to the destination .which shows that Sybil attack is been detected .it is done by maintain two, list one for receiving and one for sending and on cross checking these list we can compute the trust values and from these values may further help in identifying the Sybil node.

In this paper the aim is to develop the application using trust based mechanism which can help to reduce the impact of Sybil attack in peer-to-peer network because Sybil attacks can disrupt routing protocols in ad-hoc networks, especially the multicast routing mechanism.

Packet Delivery Ratio (PDR) is used to calculate the ratio b/w the packets send from the sender and received at receiver end.

PDR=Received_Packets/generated _packets*100

It can be calculated from the packets been generated and received in the trace file.



The graph already shows the relationship b/w the Attack and non attack nodes, as the blue bar shows the data delivery by the node seems to be less than approximately 5% while the yellow bar shows representing the non attack nodes with data delivery greater than 90% which shows b/w the two bars that the sending packets in the attack nodes are very less which shows the effect of Sybil attack.

6. Conclusion & Future Work

There are a variety of attacks that hinge on the issue of identity. In this work, Sybil node detected successfully with trust based mechanism. The lost of nodes can be easily detected by maintaining two lists and the result produced after the simulation is effective as the number of nodes send by the sender side will reached to the destination. There may be many other intruder /attackers who can detect those attacks which effects the simulation of the network and many other methodologies can be combined to reduce the impact of the various attacks in future.

References

[1] Aggarwal, C. (2015). Sybil Attack in Peer-to-Peer Network. *International Journal of Engineering Research and General Science* , 1334-1337.
[2] Berlin, V. (2010). Architecture of Peer-to-Peer Systems. *Springer* .
[3] Blanc, A., Liu, Y.-K., & Vahdat, A. (2012). Designing Incentives for Peer-to-Peer Routing. *International journal of Electrical and Computer Engineering* .
[4] Cai, L., & Rojas-Cessa, R. (2014). Containing Sybil Attacks on Trust Management. *IEEE - Communication and Information Systems Security Symposium* .
[5] Dr. S. Justin Samuel, B. D. (2015). An Efficient Technique To Detect And Prevent Sybil. *IEEE* .
[6] Gupta, A., & Awasthi, L. K. (2011). PEER-TO-PEER NETWORKS AND COMPUTATION:. *International Journal Computing and Informatics,* .
[7] Li, F., Liu, B., Xiao, Z., & Fu, Y. (2014). Detecting and Defending Against Sybil Attacks in Social Networks:. *International Conference on Broadband and Wireless Computing, Communication and Applications.* Changsha, China.
[8] Nitish Balachandran, S. S. (2012). A Review of Techniques to Mitigate Sybil Attacks. *Int. J. Advanced Networking and Applications* .
[9] Sharma, & dhawan. (2013). An Enhanced and efficient mechanism to detect Sybil attack in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Engineering & Technology* .
[10] Srivastava, & Mitra. (2011). Attacks on Correlated Peer-to-Peer Networks:. *International Workshop on Security in Computers, Networking and Communications* .
[11] Suri, Germanus, & Ismail. (2015). Detecting and Mitigating P2P Eclipse Attacks. *IEEE 21st International Conference on Parallel and Distributed Systems* .
[12] Xiang, X. (2012). Defeating against sybil-attacks in peer-to-peer. *IEEE 26th International Parallel and Distributed Processing Symposium Workshops* .