IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 8, Issue 6 (Jan. - Feb. 2013), PP 79-82
www.iosrjournals.org

Defending Sybil attack using Associate Membership method in Distributed P2P Network

Dr. Md. Nasim Akhtar, Rowsan Jahan Bhuiyan
Associate Professor, Dept. Of Computer Science and Engineering, Dhaka University of Engineering and Technology, (DUET) Gazipur-1700, Bangladesh.
M.Sc in Engineering Programme, Dept. Of Computer Science and Engineering, Dhaka University of Engineering and Technology (DUET), Gazipur-1700, Bangladesh.

Abstract: *The Peer-to-peer networks popularity is increasing day by day for its resource allocation system like file sharing, Skype etc .The system is extremely fast because of its fully decentralized nature. Although this is efficient system but this system's security is vulnerable and can be attacked anytime by attackers. This paper describes P2P's most challenging threat Sybil attack. Generally Sybil attack is defined as an attack by a malicious user who creates multiple identities and act as separate and real nodes. These fake nodes are called Sybil nodes. After creating these fake IDs, malicious user can control the network by controlling the nodes which contains resources. They can also change the resources and can attack node's routing table, they can damage node's communication on the network. This paper describes possible solutions against this attack by using existing SyMon protocol with our proposed "Associate membership" method .By implementing the proposed model performance will increase to defense against Sybil attack.*

Keywords: *Associate membership, P2P, Security, Sybil attack, SyMon.*

I. Introduction:

Peer-to-Peer overlay network has been developed for very fast resource sharing over internet and have rapidly been spreading since its establishment. Nevertheless, together with its fast development, many security issues have also been emerged. Byzantine failures, resources edit, damages nodes communication link, generates spam messages etc. can be done by malicious user who takes control of several nodes by creating multiple identities. This is identified as Sybil attack [1]. We have proposed Sybil defense scheme theoretically and showed that our presented model is so secured that it is very hard for a challenger to join in network because transaction monitor system SyMon[2] is used together with our proposed method. Our proposed solution's feasibility can also be achieved by integrating it with other existing Sybil defense protocol.

II. Related Work:

There are many existing protocols which utilize network coordinates [3] system for defending Sybil attack e.g. Konjevod and Bazzi [4]. Network coordinates system is also used for sensor networks [5] for defense Sybil attack. But the system can only bind the number of Sybil groups. Danezis et al [6] proposed an idea for making DHT lookups against sybil attack. The idea is to control the bootstrap tree of the DHT, where two nodes can share an edge if one node introduces the other into the DHT. The sybil nodes can only join at a small number of nodes to the rest of the tree. Recently, to detect sybil and to fight against of probable attack, solutions have been introduced based on social network study. Sybil Guard [7] and Sybil Limit[8] are example of this kind of solutions. Another related work which is very helpful to fight against Sybil attack is discussed below.

2.1 SyMon Discovery Protocol:

A new solution to defense Sybil attack 'SyMon' was proposed by Jyothi B.S and Dharanipragada Janakira where every node is joined together with another node as verifier, these verifier is called SyMon.The Monitor nodes selected randomly that's why it is rare for both verifier nodes to be Sybil. SyMon monitors the transacting two nodes closely so that an honest node cannot be cheated by a malicious user. From the protocol, it can be assumed that an honest guess peer always choose a honest node as its verifier but a Sybil suspect node select verifier from many of its own created Sybil node, this is the best selection system of SyMon.

General idea of SyMon selection: Following Fig 1and 2 [2] demonstrate SyMon selection procedure.

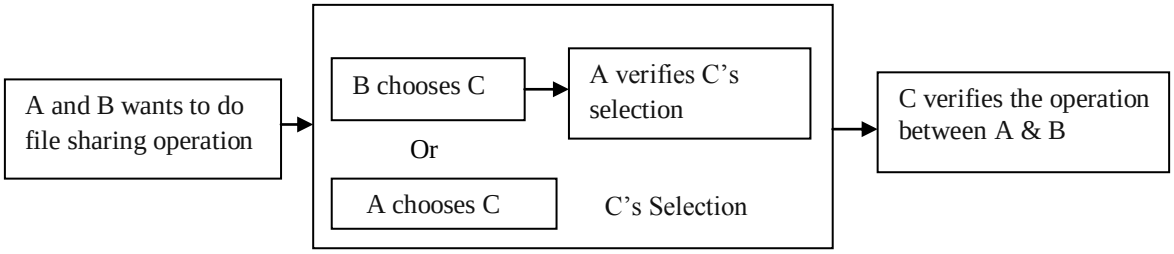


Figure: 1. Model A

The above Figure point to selection procedure of verifier. If A and B two nodes want to do a file sharing operation in this case either node B will chose C as verifier and that case node A will check C's selection procedure. Or node A will chose C as verifier. After that, C will verify file operation between A and B. Finally a node D will verify the selection of C. This is rare case two of the verifier will malicious or Sybil node.

III. Our Proposed Model:

In this section, we will introduce a method based on associate membership concept similar to real world. SyMon protocol [2] is used to cooperate in this model. When a trusted node receives join request in the network from an unknown peer (may be honest or Sybil), the unknown node need to go though several steps to become a trusted member for sharing the resources of network.

Initially, when an unknown node ask to join in P2P network by sending join request to another existing trusted node (see in figure- 1), the trusted node will check its own Sybil & Non-Sybil table. Each trusted node must maintain these tables which contains previous tested result of a particular node. Records in these tables are updated time to time after verifying each incoming node's request.

Node ID	Sybil
192.168.121.251	Yes
192.168.121.121	Not verified
202.4.73.34	Yes

Sybil Table

Node ID	Non-Sybil
203.84.209.75	Yes
219.94.9.94	Not verified
103.9.112.17	Yes

Non-Sybil Table

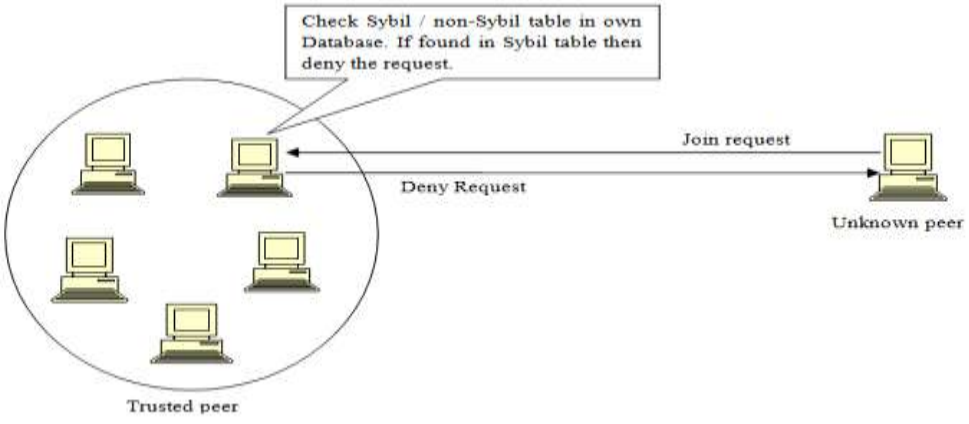


Figure. 3. Join request from an unknown peer and judgment technique.

If the unknown node ID has already been stored in Sybil table in Database (previously tested), the 'join request' will immediately be denied. Hence testing process will be terminated for this node and stored-record in Sybil table will remain same. In case, the node is not found in any table of own database then the unknown node will be allowed as "associate member". Acknowledgement will send to it (see Fig-2). Thus it will also allow transacting less important resource for a certain time (e.g. 50 transactions). In this phase, the operations and activities of "associate member" will be monitored by "SyMon protocol" [2]. SyMon closely watch all transactions between transacting nodes and discovers Sybil or malicious nodes.

When SyMon protocol discovers that the 'associate member' node is really a Sybil node and performing malicious operations (e.g. resources editing, breaking nodes' communication and so on),then " associate membership" will be cancelled and the node ID will be put in Sybil table at database.

By exploiting the property of "SyMon" protocol, when the associate member node's activities are discovered as 'non-malicious', then it will be replaced trusted node's non-Sybil table. In this stage, it will also verify some of trusted node's Sybil &Non-Sybil table to whom the associate member already sent join request. If there are 80% of nodes who get join request from that particular associate node and have stored it in their own non-Sybil table after verifying, then make it trusted node and generate messages to other request received trusted nodes to consider it as newly trusted node. Otherwise they will keep it in non-sybil table. Moreover the process will end for this particular node. It will not be able to test again by this trusted node.

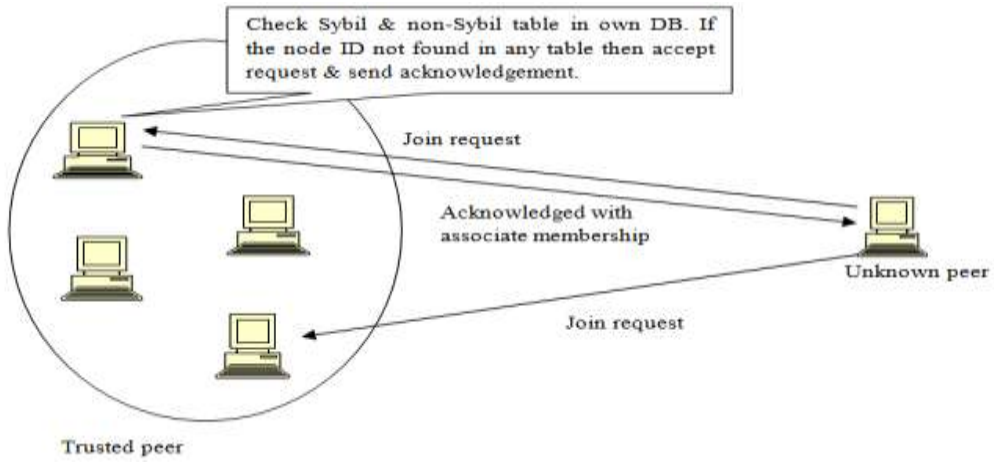


Figure:4 Acknowlegment of join request to an unknown peer if the peer ID is not in the DB.

Whenever it still likes to be a trusted member and wish to contribute in resource sharing activities, it must be accepted by 80% of request obtained trusted node. Suppose the associate node sent join request to fifteen (15) nodes, then 80% of 15 is 12. So, while twelve (12) trusted nodes declare it as non-Sybil, only then the unknown associate node will be permanent trusted node.

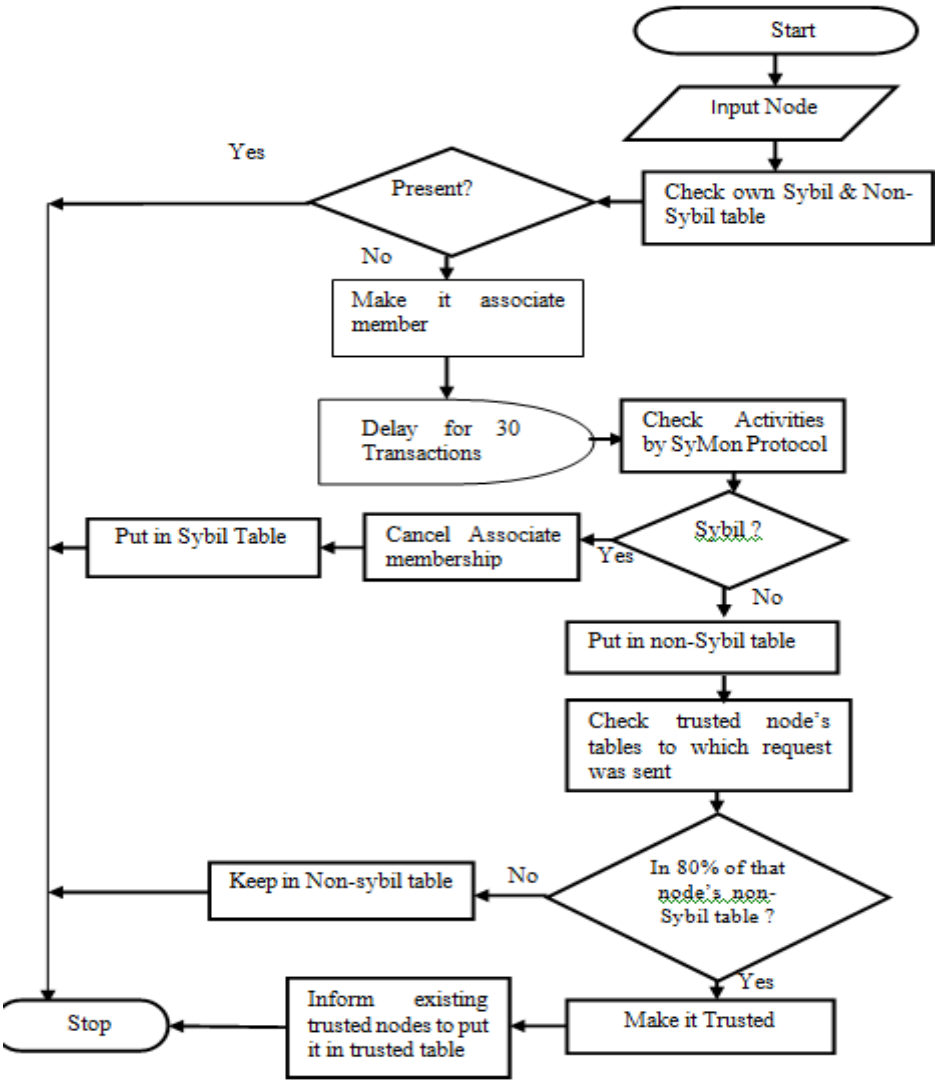
Performance Measurement:-

Time Period	Suspect /unknown Node	Sent Request to	Request Received by	Get Associate membership of	Entitled to be kept in Non-sybil table of	Required points to be included in non-sybil table (80% of node who accepted request)	Points earned	Result
1	a	b, c, d, e,	b , c ,d, e	b, c, d, e	d, c	3.2 (80% of 4 nodes)	2	Not trusted but keep in non-sybil table
2	f	b, c, d, e, g	b, c, d, e, g	b, c, d, e, g	b, c, e, g	4 (80% of 5 nodes)	4	Make Trusted
3	a	b, c, d, e, f	b, c, d, e, f	b, c, d, e, f	d, c, f	4 (80% of 5 nodes)	3	Not trusted

Table- Performance Measurement of protection.

For example, from the above table at time period-1 an unknown node 'a' sent request to nodes b, c, d, e and they all accepted the request and get associate membership from them. After verification with SyMon protocol node d and c keep the unknown node in its Non-Sybil table. But from our proposed model node 'a' should be keep by 80% of requested accepted nodes to be trusted. It is seen from the above table that node 'a' is accepted by 4 nodes but store as non-sybil only by 2 nodes d and c. So node 'a' is kept in Non-Sybil table but not considered as trusted member. So the security has increased than previously mentioned method.

FLOWCHART OF PROPOSED MODEL:



IV. Conclusion And Future Work: -

Malicious attackers are challenging distributed resource sharing system. By using a dependable and standard system, threat can be minimized. This paper, we have presented a description of Sybil attack and possible solution for prevention such attack by using existing model SyMon discovery protocol and our proposed model together with. We have proposed a solution that allows every honest node to defend against Sybil attack. The model can be used in combine with other existing Sybil defense protocol. However, there is still some work to do, for illustration in the proposal as future work, we intend to implement this concept in the view of some real-world applications and reveal its effectiveness.

References

Journal Papers:

[1] J. Douceur. The Sybil attack. *In IPTPS, 2002.*
[2] Jyothi B.S and Dharanipragada Janakira, SyMon: An approach to defense Sybil Attack in structured P2P network.
[3] T. S. E. Ng and H. Zhang. Predict the network distance of internet with coordinates-base method. *IEEE, 2002.*
[4] R. Bazzi and G. Konjevod. The establish of different id in overlay networks. *ACM PODC, 2005.*
[5] J. Newsome, E. Shi, D. Song, and A. Perrig. Sybil attack in sensor networks Analysis and defenses. *ACM/IEEE IPSN, 2004.*
[6] G. Danezis, C. Lesniewski-Laas, M. F. Kaashoek, and R. Anderson. Sybil-resist DHT routing. *The European Symposium Research, 2005.*
[7] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. Defense against Sybil attacks by using Sybil Guard based on social networks. *Technical Report IRP-TR-06-01, Intel Research Pittsburgh, June 2006.*
[8] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao. Nearly optimal solution using Sybil limit based on social network. *Technical Report TRA2/08, SNU, School of Computing, Mar. 2008.*
[9] W. J. Bolosky, J. R. Douceur, D. Ely, and M. Theimer. Feasibilities of server less distributed system on an existing set of desktop PC. *In ACM SIGMETRICS, 2000.*
[10] A. Cheng and E. Friedman. Sybil proof reputation system. *In ACMSIGCOMM seminar on Economics of P2P Networks, 2005.*