A Survey and Analysis of Sybil Attack in Peer to Peer Network

Samidha Nagdeve
Scholar, DIMAT, Raipur
Chhattisgarh Swami Vivekanand Technical University, Bhilai, India

Aksah Wanjari
Assistant Professor, DIMAT, Raipur
Chhattisgarh Swami Vivekanand Technical University, Bhilai, India

ABSTRACT
There Peer-to-peer(P2P) networks is that they are continually subject to Sybil attacks malicious nods can compromise the network by creating and directing large numbers of fictitious identities. In this paper, Sybil attacks may underscore the successfully of such schemes as malicious peers may use fake identities to synthetically manipulate the reputation. The levels of trust of several authentic and honest peers.Inthis mostly trusted certification, Reversing testing, Random key redistribution, Location/position verification and Reputation mechanisms methodology use. We analysis of the Sybil attack with respect to the resource chuck to operate Sybilnodes and we consider the calculableeffect of Sybil nodeson the total system. Reputation systems analyze reputation keep count according to its history of logs file.

General Terms
We are using to reputation system to calculate the Sybil attack score/rank.

Keywords
P2P, Sybil attack, Sybil resilient, trusted management, Free Riding, Reputation Mechanism.

1. INTRODUCTION
P2P overlay networks are known for their many desired attributes like openness, anonymity, decentralized nature, self-organization, scalability, and fault tolerance [1]. P2P networks and further research, freeriding[2] is found to commonly exist in the real P2P systems,and then the security problems about whitewashing [2][3] and Sybil -resilient.

We can use an admission control system (ACS) for plannedP2P networks resilient to Sybil attacks. The admission control system creates and maintains a self-organized hierarchy of participating peers [4].

In a Sybil attack, an adversary creates a large number offalse/fake/Duplicate identities (Sybil identities), and sinceall Sybil identities are controlled by the adversary, It canmaliciously introduce a considerable number of falseopinions into the system, and convert it, by makingdecisions benefiting system itself. Let's consider example comes from a Facebook voting application. If an attacker maliciously creates many identities, it can easily change the overall popularity of an option by providing plenty of artificial honor, of the option throughout Sybil ids. Since the artificial opinions of the Sybils may essentially change the final decision of any distributed system.In this various type of sybil attack they are as Routing in a Distributed Peer-to-peer System, Distributed Storage Applications in Peer-to-peer Systems, Distributed Voting Applications in Peer-to-peer Systems, Vehicular Ad hoc Networks (VANETs), Data Aggregation in peer-to-peer Applications [7].

Trust management is a strategy to determine the reputationof peers by evaluating the level of trust ability. However, atrust management system may not be effective under Sybil attacks, as these attacks attempt to increase the reputation of Sybil peers and therefore, making them attractive downloadingsources for honest peers. To countermeasure that, we proposeda framework that consists of three mechanisms, a local tableto determine the collaborators of sybils and honest peers, a*k*-means mechanism to cluster peers as possible sybils orhonest peers, and a transaction verification mechanism toverify that the reported transaction actually occurred[5].

In study we can define the sybil-resilient transfer P2P protocol and a dynamic reputation protocol. Combining with two, we enable a desirable level of file-sharing while defeating against sybil attacks in free-riding problem[3].We are focus on defeating against sybil attacks infree riding problem. Our protocol can be used to protect from Sybil attacks in other issues of P2P networks. This problem solving to proposed a Sybil resilient protocol torestricting nodes to obtain the numbers of services units in a reasonable level and find the defeat against Sybil attack. We develop a dynamic reputation which show that Sybil attack are restricted to the property of Sybil- proof [17].

The remaining part of this paper is various sections. Section 2 describes about the Sybil attack in peer to peer network in this area. How attacker attacks the reputation system and score will be change. Section 3 describe the defeating to Sybil attack methodology and experimental fig. finally, conclusion are draw in Section 4.

2. SYBIL ATTACK
Peer-to-peer network numerous routing protocols and applications, file sharing is themost fundamental and important application. In file sharingapplication, files are stored in nodes, opening for sharing with other nodes, and nodes search wanted files using pre-established protocols.The application of file sharing exists the free riding problem. Free riding nodes take advantage of P2P network resources download files, but are disinclined to share downloaded files or stored files to save their own resources. Freeriding negatively affects primary property of P2P network. Solving the Sybil attack problem to using Reputation mechanisms become a promising way to overcome the free riding.For each node, reputation systems (sets of objects) calculate reputation scores according to its history logs files, by which nodes may obtaina certain amount of service such as downloading files. In Sybil attack is attack the reputation mechanism and modify the score for own profits.

The Sybil nodes may consume service of others and doesnot contribute to the network at an acceptable level. Theymay behave arbitrary and collude with each other. As previous projects, we denote to the edge between an honest node and a

sybil node as attack edge. In this condition we proposed to Sybil-resilient protocol and dynamic reputation system. Our protocol should confine the number of service units consumed by sybil nodes to a reasonable level while increasing the number of service units obtained by honest nodesin this method found the defiant against Sybil attack.

3. METHODOLOGY

3.1 Planned to Defend Sybil Attack

3.1.1 Trusted Certification

Sybil attacks can be avoided by using trusted certification.In this method central authority, they can verify thev alidity of each user, and further issues a certification for the honest node [9]. During data transmission between adjacent nodes, they can use the key for mutual authentication and validation, and can also encrypt the data[10].

3.1.2 Registration Fee

They judge that the attackerscannot easily join and affect a peer-to-peer system unless they spend a lot of money.

3.1.3 Social Network Based Techniques to Defend Sybil Attacks

In though attackers can create plenty of Sybil identities, and further establish several links among them; the total number of links between the Sybil and the honest users is limited, since the trust relationship on a social network is built based on the trust relationship among real people [11].

3.1.4 Gate Keeper

Gate keeper [15], a decentralized protocol that executes Sybil-resilient node admission control mainly based on asocial net. Gatekeeper can admit most honest nodeswhile controlling the number of Sybils acknowledged per attack edge toO (log n), where *n* is the number of attack edges [8].

3.1.5 Sybil Defender

Sybil Defender is most capable and it is scalableto large social networks. Sybil Defender can effectively identify the Sybil nodes and detect the Sybil unrestricted around a Sybil identity, even when the number of Sybilnodes presented by each attack edge is close to the critically detectable lower bound Sybil [12].

3.2 Trusted Management Scheme

Sybils attempt to increase the trust value of a single or multiple sybils to make them attractive (highly trustable) sources of files. Once a sybil is accepted for interaction withan honest peer, it may release malware and infect the honest peer [5].

3.2.1 Peer-to-Peer Network and Sybil Attack Models

In this network, a peer trusted by peer *i*is called trustee, which is the source of a file, of peer *i*, and peer *j*is called trusterof that peer. Peer *i*has a trust table, which is denoted as *T(i).* The trust value of peer*i*about peer *j*, $T_v(i, j)$, indicates the number of malware-free downloads divided by total number of downloads. Peer receiving the information use it to adjust their trust values about the reported peer(*s*). In this receiving download files score in the truster*j* identification and it is called a rating score.

3.2.2 Sybil Attack on a Trust Management Scheme

Consider a network with *n*honest peers and *s*sybil peers, each honest peer has an average number of trusters, and each sybilpeer has an average of *r*sybil identities/peer. The total number of peers in the network is

$$N = n + s + sr$$

Let $I(t)$ represent the number of infected in the networkat time slot *t*, and let $T(t)$ represent the number of honestpeers in the P2P network at time slot *t*. Therefore,

$$T(t) + I(t) = n + s + sr \quad (1)$$

Each peer performs a download at time slot *t*with probability*p*. The total number of downloads in a time slot is $(n+s+sr)p$, and the probability that a download is performed from a sybil peer at time slot *t* isγt, and

$$y(t)=\frac{I(t)}{n+s+sr} \quad (2)$$

Therefore, for $t= 0$:

$$Y(0)= \frac{I(0)}{n+s+sr} \quad (3)$$

Where$I(0) = s + sr$

Let $Y(i, t)$ denote the number of sybil peers as identified bypeer*i*at time slot *t*, and $G(i, t)$ denote the number of honestpeers as determined by peer*i*at time slot *t*, as

$$G(i,t) = n + s + sr - Y(i,t) \quad (4)$$

3.3 Sybil Resilient Protocol

Our sybil-resilient protocols is restrict the number of service units consumed by sybil nodes to a reasonable level while increasing the number of service units obtained by honest nodes. Sybil –resilient defining to three types to contribution transfers [3].

3.3.1 Direct transfer

This is two types' contribution and transaction.In this contribution transfer node *i*receive a service demand of *s* units from node *j*. The value of $R_{ij}$is stored both side. In node*i*may provideservice units to node *j*using the contribution mode and therefore Figure1.

$$R_{i,j} = s \quad (5)$$

In transaction direct transfer process the node*i* request *t*serviceunit from node j, node j repays *t*service units tonode*i* *due* to obtaining sservice units from it before, and therefore

$$R_{i,j} = s - t \quad (6)$$

3.3.2 Indirect transfer

Obtain service from non-adjacent nodes, it first runs a Dijkstra algorithm to router over thedirected graph to determinate a transfer path. The source nodes of the path is the one that issues the service demand, and the destination node *d*is the service provider. If the weight of each edge e_{ij}in the path, that is, $R_{ij}$is no less than *t*, *t*is subtracted from $R_{i.j.}$ Otherwise,

$$t = maximum\,(R_{i,j} | e_{i,j} \in P_{s-d}) \quad (7)$$

The final result is subtracting *t* from each hop in the transfer path Figure 2.

3.3.3 Rating reputation rank

If node *s*intends to obtain service from node *d*, nodes should find a shortest path to node *d* using the shortest-path algorithm Fig 3. The reputation rank value ofnode sis defined as rank

$$(P_{s-d}) = min\,(\sum \frac{1}{R_{i,j}} |e_{i,j} \in P_{s-d}) \qquad (8)$$

Where $P_{s-d}$is the path from st*od*. Since both path to node d. node d calculate reputation rank is define

$$Rank\,(P_{s-d}) < rank(P_{k-d}) \qquad (9)$$

We present a dynamic reputation protocol which holds the property of sybil-proofFig. 3(c).

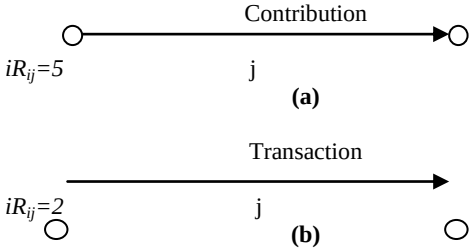

Fig.1: Direct transfer process

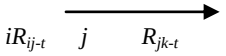

Fig.2: Indirect transfer process

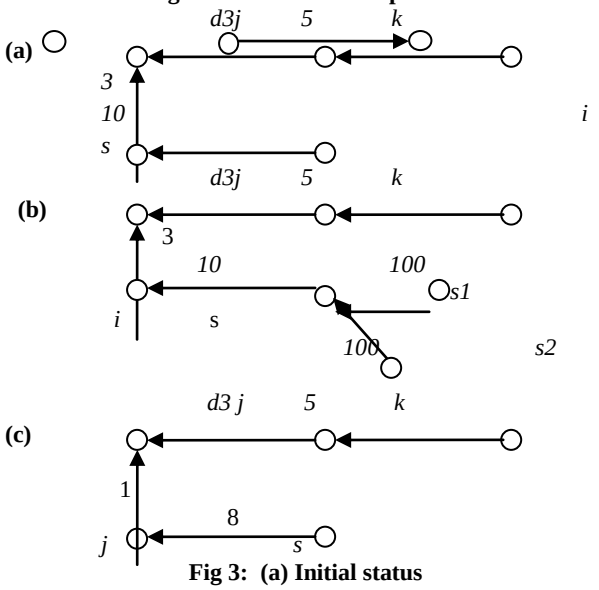

Fig 3: (a) Initial status
(b) Example of sybil attack.
(c) Status after completing an indirect transaction [4].

4. CONCLUSION

Reputation system facilitates peers to select an applicable supplier for communication however attributable to presence of malicious peers among the honest ones could create the method vulnerable. Most of the attacks are maintained decentralized P2P reputation system. The paper analyzed the varied reasonably behavior of malicious peer in P2P based requests. Malicious peers misbehave behaviors try to fake within a network either individually or collusively during a group. Our paper, proposes a reputation mechanism resolution for detection of collusions together with a penalization policy for reputation reduction of detected malicious peers. while reputation models proposes the peers from selecting malicious nodes as a service supplier, the proposed model may be a reactive approach that concentrates on detection peers that provided higher reputation to the malicious peer is more powerful in detection of collusion (if present) inside the network, whereas present mechanism are only maintained prevention of approval.

5. REFERENCES

[1] B.S. Jyothi and D. Janakiram, "SyMonA practical approach to defend large structured P2P systems against Sybil attack," Peer- to- Peer Network. Appl., vol. 4, pp. 289–308, 2011.

[2] J. Saia, A. Fiat, S. Gribble, A.R. Karlin, and S. Saroiu" Dynamicallyfault-tolerant content addressable networks" Proceedings of the 1st International Workshop on Peer-to-Peer Systems, 2002.

[3] Xu Xiang," Defeating against sybil-attacks in peer-to-peer networks", International Parallel andDistributed Processing Symposium Workshops 2012 IEEE.

[4] HosamRowaihy, William Enck, Patrick McDaniel, and Thomas La" Limiting Sybil Attacks in Structured P2P Networks",IEEE 2013

[5] Lin Cai and Roberto Rojas-Cessa," Containing Sybil Attacks on Trust Management Schemes for Peer-to-Peer Networks", IEEE ICC 2014 - Communication and Information Systems Security Symposium.

[6] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 318–328, 2006.

[7] Rakesh G.V 1, ShantaRangaswamy 2, Vinay Hegde 3, Shoba G 4, "A Survey of Techniques to Defend Against"

[8] "Sybil Attacks in Social Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014

[9] N. Tran, J. Li, L. Subramanian, and S. S.M. Chow. "Optimal Sybil resilient node admission control", In IEEE INFOCOM, 2011.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in Proc. of ACM IPSN, 2004 pp. 259–268.

[11] J. Ledlie and M. Seltzer, "Distributed, secure load balancing with skew, heterogeneity and churn," in Proc. of IEEE INFOCOM, vol.2, 2005, pp. 1419–1430.

[12] Y. Reddy, "A game theory approach to detect malicious nodes in wireless sensor networks," in Proc. of IEEE SENSORCOMM, 2009, pp. 462–468.

[13] Wei Wei∗, Fengyuan Xu∗, Chiu C. Tan†, Qun Li "Sybil Defender: Defend Against Sybil Attacks in Large Social Networks ", the College of William and Mary, †Temple University 2013.

[14] Nitin Kumar Sain, Vikas Kumar Sihag," A Reactive Approach for Detection of Collusion Attacks in P2P Trust and Reputation Systems", International Advance Computing Conference (IACC) IEEE 2014.

[15] Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky," Sybil Limit: A Near-Optimal Social Network Defense against Sybil Attacks", USENIX NSDI, 2008.

[16] James Newsome, Elaine Shi, Dawn Song, "The Sybil Attack in Sensor Networks: Analysis & Defenses", *IPSN'04,* April 26–27, 2004, Berkeley, California, USA.

[17] Chris Lesniewski-Laas," A Sybil-proof one-hop DHT", SocialNets'08, April 1, 2008, Glasgow, Scotland, UK.

[18] James Newsome**,** Elaine Shi**,** Dawn Song,"The Sybil Attack in Sensor Networks: Analysis & Defenses",IPSN'04,April 26–27, 2004, Berkeley, California,USA.