Improved Rank Reputation Based System for Identification of Sybil Attack

Khushboo Kadber [1], Mr. Omprakash Dewangan[2]
[1, 2] Department of Computer Science & Engineering
[1, 2] Rungta College of Engineering & Technology, Bhilai, India

Abstract- *On this paper, we cope with the peer-to-peer networks showing that the existence of Sybil attack is a critical threat. Peer-to-peer networks have many aspects which can be distinctive from conventional client server networks. The most significant factor is that each peer acts as both server and client roles in Peer-to-peer network. In other words, there is no central server that used for storing the documents and supplying download. All nodes download files directly from other peers. In Sybil attack, attacker spoofs the identities of other nodes or creates its own identification. Like this create a fake relation with other nodes. On this paper we discussed approximately the identity of Sybil attack via calculating the reputation rank of every nodes. Right here the nodes will share files and file sharing exist the free riding problem. In free riding problem the nodes will download the files from peer-to-peer networks but they are unwilling to upload the files. In this paper we are calculating the reputation rank of each node to identify the Sybil nodes.*

Keywords- Peer-to-peer networks, Sybil attack, Free riding problem, Reputation system.

I. INTRODUCTION

Peer-to-peer network have emerge as famous for certain applications and deployments for an expansion of reasons, such as fault tolerance, economics and legal issues. It has consequently emerge as reasonable for resource consuming and commonly centralized application.

A peer-to-peer network is a network that is predicated on computing energy of its clients as opposed to in the community itself. This indicates the customers (peers) will do the vital operations to maintain the network going in preference to a critical server. There are unique stages of peer-to-peer networking they are Hybrid P2P, pure P2P and mixed P2P [7].

Hybrid peer-to-peer network is a central server which keeps statistics approximately the community. The peers are accountable for storing the information. if they need to touch every other peer, they query the server for cope with.

pure peer-to-peer network is actually no imperative server or router. each peer acts as consumer and server at the identical time. this is on occasion referred to as “serverless” peer-to-peer network.

Mixed peer-to-peer network is between hybrid and pure peer-to-peer networks. An instance of this kind of network is Gnutella (Gnutella customers are free rider) [12] which has no imperative server but clusters its nodes around so called “super nodes”.

The main intention of routing protocols in peer-to-peer network is to find out the most fulfilling direction with minimal overhead, minimal bandwidth intake and minimum put off between source and vacation spot node.

Safety in peer-to-peer network is a extraordinarily hard issue. The attacks on peer-to-peer networks can be broadly labeled into categories: Active attacks and Passive attacks.

Passive attacks are those wherein the attacker gratify in hearkening or tracking of records transmission. In different words, the attacker objectives to acquire information this is in transit. The term passive shows that the attacker does now not try and carry out any changes to the statistics or the contents of an original message [13].
Active attacks are based on modification of the original message in some manner or the creation of a false message [2].

Sybil attacks is likewise known as masquerade or impersonation or spoofing attack. In this attack, a single malicious node tries to take out the identity of other nodes inside the network via marketing fake routes. It than attempts to ship packets over network with identity of other nodes making the destination trust that the packet is from authentic source. Sybil node does now not allow the packets to reach its destination, misuse the records and plenty of more damages which it reasons to a network. Sybil attack may be used as gateway to execute huge scale attacks of different sorts such as Eclipse [15].

II. LITERATURE SURVEY

Literature assessment of various papers describes the one of a kind varieties of methodology for the identification of Sybil attack. The Sybil resilient protocol approach is used by Xu Xiang in [17] for proscribing the service unit fed on by using a node. on this methodology explain that exceptional form of contribution switch: direct switch and oblique switch. In direct switch there are extraordinary types of contribution switch: contribution and transaction. In direct switch, contribution transfer takes place among adjoining nodes. without any precondition a node may also provides numerous provider units to different nodes. In oblique transfer there's only one switch mode: transaction. on this contribution switch takes location between non-adjoining nodes. The manner of transaction is achieved in steps: finding a transaction path and performing transaction. For indirect transaction Dijkstra set of rules is used. A Sybil resilient peer-to-peer protocol and dynamic reputation protocol Combining this two it enable a preferred level of record sharing whilst defeating towards Sybil attack in free riding problem. The reciprocity mechanism and PledgeRoute is also used that allows contributing peers to reap better carrier pleasant than freeloaders [16].

Meta reputation system and trust by association approach is centered with the aid of Matthew Kellett, Thomas Tran, and Ming Li [8] which results in an presenting peer with a high trust value is much more likely to get the transaction.

Guojun Wan, Felix Musaug, tune Guo [4] centered on neighbor similarity trust peer-to-peer ecommerce confirmed fastmixing assets and neighbor similarity trust which gives better defense mechanism.

Krishna P.N.Puttaswamy , HaitaoZheng, and Ben Y. Zhao [6] had been gave the steering to the approach lightweight Detection and tracking system which conclude the performance of a simple assault and corrupting the lower levels of a sufferer's routing table is sensible, but may be efficiently defended.

Yanchao Zhang, Yuguang Fang [18] have determined that novel reputation system built upon the multivariate Bayesian inference theory can be appropriate for the effectiveness and performance of the system and advanced it.

Amol Vasudeva and Manu Sood [1] have explained the lowest id clustering algorithm. A node with lowest id is taken as a clusterhead and each node is supplied with a unique identification. Boroadcast listing of its neighbor's identity together with itself id.

Nitish Balachandran and Sugata Sanyal [10], introduced the ideas of the diverse kind of technique to counter Sybil attack. They are trusted certification, resource testing, recurring costs, incentive based detection, random key predistribution[10].

Public Key records primarily based protocols for cryptographic system is likewise used to boom the security by means of allowing the nodes free in the network[3].

III. PROBLEM DEFINITION

The primary problem of peer-to-peer network is free riding problem. The peer-to-peer networks be afflicted by a excessive level of free riding wherein a few customers consume network sources without supplying any network resources. Right here within the networks nodes will take the advantages of network sources and download the documents but they may be disinclined to share the downloaded documents or stored documents to save their own assets.
The solution to the free riding problem in peer-to-peer network can be solved with the aid of the usage of the reputation mechanism. The reputation mechanism will calculate reputation rank for each node uploading and downloading the files. By way of this we measure that the uploaded and downloaded files must be nearly equal so that it is able to resolve the free riding problem.

IV. METHODOLOGY

There are distinctive sort of algorithm and protocol for the identification of Sybil attack in peer-to-peer network as defined inside the section II. Here the reputation system mechanisms is used for the detection of Sybil attack in p2p network and solve the free riding problem. In previous work the reputation system had calculated the rank of every node on the basis of incoming packets only and dijkstra algorithm is used for routing to find optimal path between the nodes.
In this paper, the reputation based system used to calculate reputation rank of each node on the basis of both incoming and outgoing packets i.e. uploading & downloading files. The uploading & downloading files are almost near to equal. If the uploading files is greater than the downloading files than there is problem of free riding. The Free riding problem can be solved by reputation based system using reputation rank of each node.

The AODV(ad hoc on demand distance vector) routing protocol is used to find the path between the peer. It

is a reactive routing algorithm, in which routing is done by the peers only on demand i.e. only when the peer needs to send a message. The sender floods its neighbors with route request packets to find route in the network. Any destination or intermediate peer in the network having path to the destination will reply back with route reply to the sender and the routing is accomplished.

Here maintaining the list out incoming & outgoing packets separately. On the basis of this the reputation rank is calculated by using following formula:

rank(node)= (∑ Outgoing packets) - (∑ incoming packets)

The list maintained is shown in the table 1. In this table the maximum reputation rank is better node and the node with least reputation rank is worst node or say Sybil node. The node with rank value zero is the honest node. As zero rank means the uploading files(outgoing packets) is almost equal to downloading files(incoming packets). Here node 12 is worst node and node 7 is honest node.

Maintaining the list of both incoming and outgoing packets would improve the method of rank reputation system wherein only incoming packets was taken.

Table 1. List of maintaining incoming & outgoing packets for calculating reputation rank.

Peers	Incoming Packets	Outgoing Packets	Rank
1	3	10	7
2	6	12	6
3	7	12	5
4	9	15	6
5	10	18	8
6	3	7	4
7	8	8	0
8	4	9	5
9	7	10	3
10	5	18	13
11	5	15	10
12	18	2	-16

The Following Fig 1. shows the flowchart of methodology for the identification of Sybil attack using reputation system.

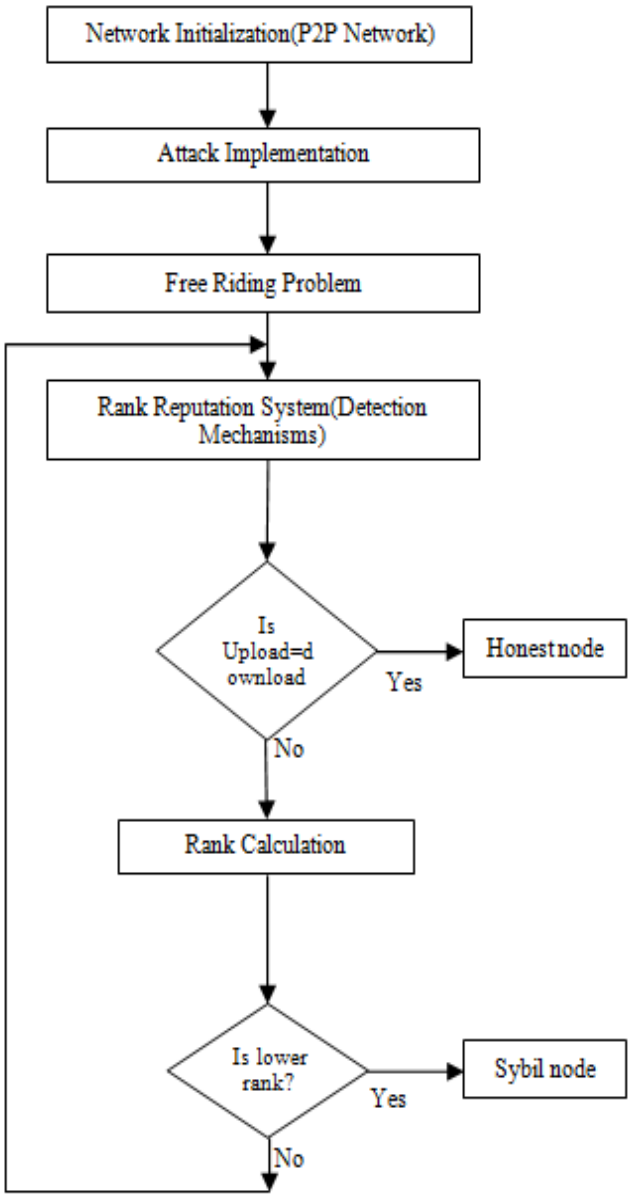

Fig 1. Flow diagram of Sybil attack detection system.

V. RESULT

The following result shows the comparison of packet delivery ratio between the Sybil node(with attack) and other node (without attack). The packet delivery ratio of Sybil node with attack is always below 10 percentage and without attack the packet delivery ratio of node is much greater than Sybil node.

Packet Delivery Ratio(PDR)=∑ number of packet receive/

∑ number of packet send

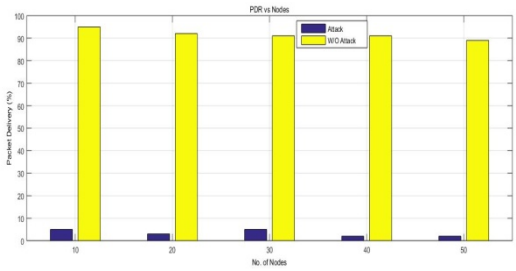

Fig 2. Packet delivery ratio of node with attack and without attack.

The time taken to detect the Sybil node is a overhead in detection. The graph plot between the nodes and time spend on detection as shown in fig 3. As the number of node increases the time to detect the node also increases. For minimum number of node it takes less time to detect the node and for maximum number of node it takes more time. So the more time spend on detection which is not useful which is taken as overhead in detection.

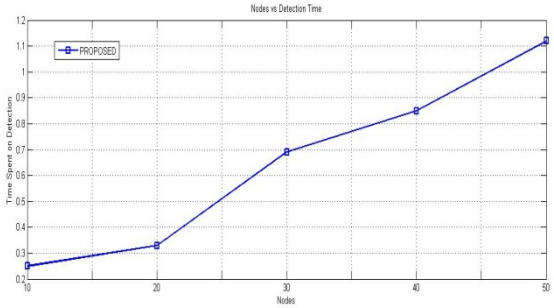

Fig 3. Time spend to detect the Sybil node(Overhead in detection).

The Fairness ratio shows that the level of packets obtained by a node is proportional to the level of packets provided by the node. A good system should have mechanism to motivate nodes to share more and reward them based on their sharing.

Fairness ratio is used in peer-to-peer network to find whether nodes are receiving a fair share of network resources. The fairness ratio is between 0 and 1, it is less than 1. So that for each source node the number of packets it receives is less than the number of packets it sends. To calculate fairness ratio, we use following formula:

Fairness ratio=Nt/Nc

where Nt is the number of packets obtained by the node and Nc is the number of packets provided by the node.

Fig 4 shows the fairness ratio with different value of nodes. This means that nodes should share to a large number of nodes with a appropriate amount of packet for each.

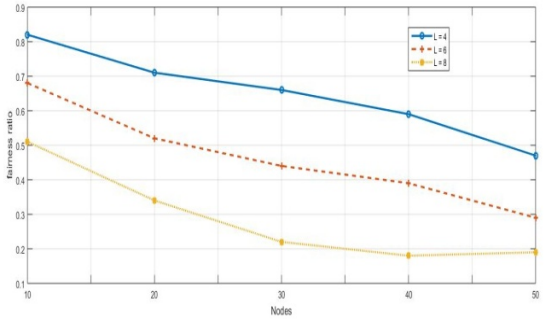

Fig 4. Fairness ratio of nodes.

VI. CONCLUSION

This paper presents reputation system mechanism, in which we find the rank for each uploaded and downloaded documents through every nodes. The rank of uploaded documents is sort of identical to the downloaded record than the network may be more efficient in terms of free riding problem. Here in this paper conclude that via using the reputation mechanism the packet delivery ratio gives better results and the time for detection is analyzed. As compare to base paper the fairness ratio is also better.

REFERENCES

[1] AmolVasudeva and Manu Sood, "Sybil Attack On Lowest ID Clustering Algorithm In The Mobile Ad Hoc Network" International Journal of Network Security & Its Applications (IJNSA),2012.

[2] Atul Kahate , book "Cryptography And Network Security".

[3] A. Aranganath and C.D.Suriyakala, "Mobile Agent Based Security In MANETS Against Sybil Attack" IEEE 2014 International conference on control, instrumentation, communication and computational technology.

[4] Guojun Wang, Felix Musau, Song Guo, Muhammad Bashir Abdullahi "Neighbor Similarity Trust Against Sybil Attack In P2P E-Commerce" IEEE Transactions On Parallel And Distributed Systems.

[5] Akash wanjari and Samidha Nagdeve "Sybil Attack Detection On Peer-to-Peer Network Based On Enhanced Sybil Resilient Protocol" 2015.

[6] Krishna P.N. Puttaswamy, HaitaoZheng, and Ben Y. Zhao, "Securing Structured Overlays Against Identity

Attacks", IEEE Transactions On Parallel And Distributed Systems2009.

[7] Lin Wang "Attacks Against Peer-to-peer Networks and Countermeasures" TKK T-110.5290 Seminar on Network Security.

[8] Matthew Kellett, Thomas Tran, and Ming Li "Trust By Association: A Meta-Reputation System For Peer-To-Peer Networks" 2011 Wiley Periodicals, Inc., Computational Intelligence, Volume 27, Number 3, 2011.

[9] M. Srikanth and K.B. Madhuri "Secure and Effective P2P Reputation System Using Trust Management And Self Certified Cryptographic Exchanges" IJCSI 2013.

[10] Nitish Balachandran, Sugata Sanyal "A Review of Techniques To Mitigate Sybil Attacks" Int. J. Advanced Networking and Applications.

[11] Sohail Abbas, Madjid Merabti, David Llewellyn-jones, and Kashif Kifayat "Lightweight Sybil Attack Detection In MANETS" IEEE system journal 2012.

[12] Ramayya Krishnan, Michael D. Smith, Zhulei Tang, Rahul Telang " The Impact Of Free-Riding On Peer-to-Peer Networks" Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[13] Adnan Nadeem, Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches For Network Layer Attacks".

[14] Prashant dewan and Parth Dasgupta, "P2P Reputation Management Using Distributed Identities and Decentralized Recommendation", IEEE Transactions on knowledge and data engineering 2010.

[15] SadekFerdous, Farida Chowdhury and Md. Moniruzzaman, "A Taxonomy of Attack Methods on Peer-to-Peer Network", Published in the Proceedings of the 1st Indian Conference on Computational Intelligence and Information Security, 2007.

[16] Raul Landa, david Griffin, richard G. Clegg, Eleni Mykoniati and Miguel Rio "A Sybil proof Indirect Reciprocity Mechanism For Peer-to-Peer network's ".

[17] Xu Xiang " Defeating against Sybil-attacks in peer-to-peer network's" 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum.

[18] Yanchao Zhang, Yuguang Fang, "A Fine Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks" IEEE Transaction On Parallel And Distributed Systems,2007.