I. J. Computer Network and Information Security, 2016, 9, 56-63
Published Online September 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.09.08

Detection and Mitigation of Sybil Attack in Peer-to-peer Network

Arpita M. Bhise
PG Scholar, Yeshawantrao Chavan College of Engineering/Department of Computer Science and Engineering, Nagpur, 441110, India
E-mail: arpita.bhise08@gmail.com

Shailesh D. Kamble
Associate Professor, Yeshawantrao Chavan College of Engineering/Department of Computer Science and Engineering, Nagpur, 441110, India
E-mail: shailesh_2kin@rediffmail.com

Abstract—Peer-to-peer networks are widely used today. Due to this wide use, they are the target of many attackers. The most mentionable of them is the Sybil attack. This is an attack in which it creates many fake identities. In this paper, the detection scheme and efficient mitigation mechanism to counteract Sybil attack in the peer-to-peer network is proposed. The proposed Sybil detection scheme is used to detect Sybil attack. The detection of Sybil attack is depending upon the behavior of the packets. The identity and the location of the packet are checked. If the location and identity of the packet are changed than that of the mentioned, the packet is detected as a Sybil attack. Sybil mitigation scheme is the combination of cost incurred method and certified authentication method. The Sybil packet will be removed by closing read/write operations. The proposed scheme is evaluated on the basis of detection rate and false positive rate. The experimental results show that Sybil attack is accurately detected by the proposed system in terms of low false positive rate and high detection rate. Moreover, the proposed system works efficiently in terms of Sybil detection rate and false positive rate.

Index Terms—Peer-to-peer networks, Sybil attack, Sybil detection scheme, Sybil mitigation scheme, Sybil detection rate, false positive rate.

I. Introduction

The communication has to take place through the network between the peer-to-peer systems. P2P systems are the distributed systems, the communication between them happens through internet. The communication between P2P systems may include sharing of confidential data. Confidentiality of data should be maintained in such systems. The data privacy and confidentiality in the network is maintained by maintaining the network security. Security of networks plays vital role in transactions and communications. Many researchers have developed mechanisms for detection and defence of all possible attacks and threats. The mechanisms proposed sometimes fail to address the problem of security and sometimes may prove as an effective one. So, the aim of this chapter is also to propose the effective and efficient mechanism in detecting and mitigating the Sybil attack.

Amongst many harmful attacks, is the Sybil attack in which, the fake identities are created by the malicious node and the created fake identity claims to be a different node. Sybil attack has become the genuine problem in many different networks like Wireless Sensor Network (WSN), Ad-hoc networks like VANETs and MANETs, Social networking sites, e-commerce applications [1][2][3][4][5][11][13][14][19][31]. The effects of Sybil attack in such networks are also different. Some examples of such systems can be quoted as: in voting system, for the political advantages, many fake IP are created to cast votes and also to alter the result of the searches of the related terms. In ad-hoc networks like MANETs, the lack of centralised authority leads to Sybil node misleading the honest nodes resulting hijacking the honest nodes [26]. Also in wireless sensor networks, the energy and power consumption are used on account of making attack successful [19] [20]. In social networking sites, the rate of fake identities accounts acceptance is increased [12].

Many peer-to-peer systems are vulnerable to Sybil attack in which an adversary creates many bogus identities called Sybil identities and try to gain the control of the network by polluting the network with the fake identities [30]. In peer-to-peer networks, the identities are used as an abstraction to hide the correspondence of the identities. By default, each identity corresponds to the distinct entity whereas after Sybil attack, many identities correspond as a single local entity. After becoming part of the peer-to-peer network, fake identities may then overhears the communication or act maliciously. By masquerading and presenting multiple fake identities, it becomes easier for an adversary to control the network substantially. Sybil attack is divided into taxonomies depending upon their behaviour [19][31]. Sybil node may directly communicate with the honest node or may steal the identity of the other nodes or may create some identities to work in the network.

We propose the mechanism to handle the Sybil attack

in the peer-to-peer network. The proposed approach contains the combination of the mechanism for detecting and mitigating the Sybil attack. The detection mechanism works by observing the behaviour of the malicious file. The Sybil mitigation mechanism is combination of the two approaches that is cost incurred and certified authentication. This will be further elaborated in the coming section. Rest of the paper is organised as: section II contains related work about the topic discussed. Security issues and problem definition will be discussed in section III. The proposed work will be explained in section IV. The results and discussion part will be included in section V. Section VI contains the conclusion and future scope.

II. Related Work

Sybil attack has affected to the number of networks showing different effects. Many defense systems were proposed for various networks. The defense systems previously proposed for different networks with the issues are discussed in this section.

A. Social Network

There are many defense systems developed for social networks. Sybil Defender [3] is a defense mechanism which is depending upon the random walks within the social network. Wei Wei et al. proposed this mechanism for the large social networks using real network data as a database. They claimed that this mechanism can correctly identify Sybils within the network. It is observed that the detection rate is slower as random walks were used. Neil Zhenqiang Gong et al.[4] proposed a scheme based on semi supervised learning framework. This scheme is able to accurately detect the Sybil nodes with low false positive rate. This scheme is also called as a ranking mechanism. Yu et al. [12] uses the fast mixing property of the social networks. The trustworthy social networks were used to detect the Sybil node within the network. In this proposed approach, each node creates its routing table for the incoming as well as outgoing edges. After that, it starts the random walk considering the adjacent node in the routing table and publicly registers the random walk starter and witnesses node if it becomes suspect. The verifier detects whether the suspect is Sybil or not. This approach gives 99.8% result in verifying the suspect as Sybil attack. Pengfei Liu et al. [6] proposed a scheme using an algorithm based on set of iterative optimization. This proposed scheme was evaluated based on the real world social topology. This algorithm is effective in directed social network for detection of the region of sybils.

B. Wireless Sensor Networks

Wireless sensor networks have many challenges, in spite of all challenges; the researchers were able to defend Sybil attack in such networks. Liang Xiao et al.[9] developed a mechanism to counteract against Sybil attack in WSN. A concept of enhanced physical layer authentication scheme was used. The performance is examined on the basis of many parameters as bandwidth, signal power, number of channel estimates, number of Sybil clients and number of access points. It can be executed in most of the existing WSN and with very low overheads. This scheme works better when the terminals are inside buildings or in crowded urban areas. Spatial correlation of Received Signal Strength was used by Yingying Chen et al. [10] to construct the attack detection model. This was performed on the real network setup that is, IEEE 802.11 and IEEE 802.15.4. This model was able to detect the Sybil attack with high detection rate and low false-positive rate. Concept of light weight identity certificate method was used by Qinghua Zhang et al. [27] to defend aginst Sybil attack in WSN. This method provides a means for authentication of all data messages. Overhead computations were shown to be acceptable in sensor networks.

C. Ad-hoc Networks

P. Vinoth Kumar [15] used Batch authenticated and key agreement scheme to authenticate multiple requests sent from number of vehicles. Batch verification algorithm was used to classify the requests obtained from various vehicles to provide immediate response to the emergency vehicles. The data of ad-hoc vehicular network was used to evaluate this proposed scheme. By restricting the timestamps provided by road side units Sybil attack can be prevented in early stages itself. Shan Chang et al. [11] used the trajectories of vehicles while preserving their location privacy concept to defend Sybil attack in vehicular ad-hoc network. The performance of the scheme was used on false positive and false negative error. Footprint can largely restrict Sybil attack and can enormously reduce the impact of Sybil attack. The concept of packet delivery ratio was used to identify the Sybil attack by V. Palansamy et al. [26]. Simulated graphs were used to analyze the performance of the proposed model. Sybil attack can be efficiently and effectively detected in online auction group.

D. Peer-to-peer Networks

Wang et al.[1] used neighbor similarity trust to detect Sybil attack in e-commerce site, in which, the duplicate attack peers are detected as a neighbors. Non-trustworthy rate and detection rate are the parameters used to evaluate the proposed mechanism. Sybil attack can be effectively minimized using this proposed approach and is much effective in e-commerce applications. Chayan Banerjee [7] used a new type of indirect validation in which the two stage validation is useful in checking the suspected node is a Sybil node or not. It is less in storage and computing complexity. This is an effective mechanism in defending Sybil attack in peer-to-peer network. Symons were chosen dynamically also were entrusted with moderating the transactions, this concept was used by Jyothi B S et al. [14]. The probability of considering the sybils and detecting them was higher in this proposed approach.

III. Security Issues in P2P Network and Problem Definition

Securing data in peer-to-peer network is a challenging task, due to their open nature. As, in p2p,the peers cannot be necessarily trusted to have a safe data sharing, it is important to build a trusted and secured data sharing application for p2p network. The environment in which peers function is open, which welcomes any peer to join the network. These peers cannot be trusted and hence these peers are more vulnerable to the attacks such as, Sybil attack. Today's p2p network does not totally fulfill the requirements of the security of the network like availability and file authentication. As, it may be difficult to prevent Sybil attack in p2p network, it is important to develop techniques that are able to: 1) Detect attack, 2) Mitigate attack and also 3) manage to communicate with the other peers.

A. Availability

There are different resources availability requirements that are important to the p2p systems. Each node in p2p system should be able to communicate with the other nodes in a system to offer resources. In Sybil attack, an intruder may gain access of resources even if not granted, by creating the fake identities.

B. File Authentication

It is the second security requirement for p2p systems. An authentication should be sent by the sending peer and should be exactly received by the other peer in order to provide the authentication of file sharing. A masquerade may use the suspected physical device to send the authentication message to the peer which it may have considered it is coming from the authenticated peer.

Hence looking at the above security issues of p2p system, it is necessary to build a mechanism to counteract Sybil attack by considering these issues. The built mechanism should also be efficient enough to handle the Sybil attack.

IV. Proposed Work

This section explains the proposed approach for the detection and mitigation of Sybil attack. We propose a Sybil Detection Scheme for detecting the Sybil attack in the network and Sybil Mitigation Scheme for removing

A. Sybil Detection Scheme

Sybil detection scheme is proposed for detection of Sybil attack in the network. The main objective of this scheme is to detect the Sybil attack in the network to make it easy to defend network from such harmful attacks. The proposed approach for detection of Sybil attack is based on the behavior of packet when entered into the network. The Sybil packet shows the behavior as it creates fake identities targeting the system and takes the control of the network to steal information in the network. The proposed detection mechanism is also based on this behavior.

The proposed approach works on the behavior of received packet. The incoming packet in the network carries their identity and location where it is to be placed. ID and location are the two distinguishing parameters for normal packets from Sybil attack packets. As the ID and location of the packet after entering in the network is same as that of the received packet, then it is detected as the normal packet. But if the incoming packet makes its copies that is creates the fake identities at different location that that of mentioned, then it is detected as a Sybil attack packet. This will be continued throughout the stream of packets and for each packet, the packets showing the behavior as Sybil, will be counted and give the count of the detected Sybil packets. Fig. 1 shows the flow of Sybil detection scheme.

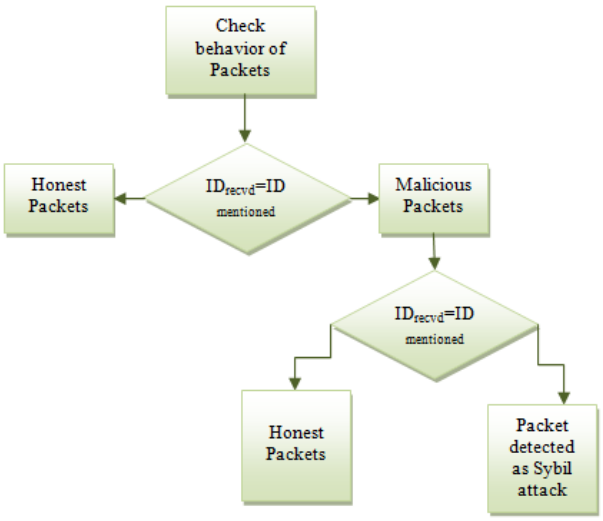

Fig.1. Flow of Sybil Detection Scheme

Step: Before detection is to be done, the server client connectivity is must to establish the communication between these two systems

1) While client communicates with the server_Receive packets from client by the server.
2) Check the behaviour of the received packet based on the condition:

If
$ID_{recvd}=ID_{mentioned\ in\ packet}$
Detect the packet as the normal packet.
Else
If
$ID_{rcvd} \neq ID_{mentioned\ in\ packet}$
Detected packet is the malicious packet.
End If
End Else
End If

3) Check the location of the received packet based on the conditions:

If $Loc_{rcvd}=Loc_{mentioned}$

Detect the packet as the normal packet
Else
If Loc $_{rcvd}$≠Loc $_{mentioned}$
Detect the packet as the malicious packet
Find the location of the multiplied packets
Detect the packet as the Sybil packet
End If
End If

B. *Sybil Mitigation Scheme*

The next step after detection of Sybil attack is to mitigate in the network to stop it causing unnecessary damage to the network. This scheme is designed by keeping in mind, the drawbacks of the earlier proposed mechanisms of defending network from Sybil attack. The earlier proposed approaches for defending network from Sybil attack are either much costlier of they are based on the models which themselves are vulnerable to the attacks. We propose a cost efficient and effective Sybil mitigation scheme to make network free of this harmful attack.

Proposed Sybil Mitigation Scheme is the combination of the two schemes that is, cost incurred and certified authentication. The incoming file in the network will be accompanied by the location and the authorization key. This authorization key is generated using MD5 algorithm. The key is signed and this is kept as a unique key for each file. If the key verification with the original key fails, and if it is making the multiple copies of itself at the various locations, the path is traced for the multiple copies formed to get the details as where the copies of the file are formed. If the file without permission is trying to make copies of itself at different locations other than the specified one, that file is not allowed to make copies of it by withdrawing the read/write actions. The multiple copies will not be formed by this way and even if formed will not be able to modify the contents of the file or to write the malicious code which can be harmful for the information in the network. In this approach the cost and time is minimized as, the file is denied with the read/write permission before behaving maliciously and it is stopped from making harm to the network.

Steps:

1) If $Loc_{rcvd} \neq Loc_{mentioned}$
The file is the Sybil file

2) Find the location of the multiplied files
3) Close the read/write operations of the file

End If
For each location of incoming file
Do

Apply MD5 to generate the authorization key.
Apply Signature to make it unique

If $Key_{verified} \neq Key_{generated}$
Trace the path of the multiplied files by detecting the location
4) Close the read/write operations of the file

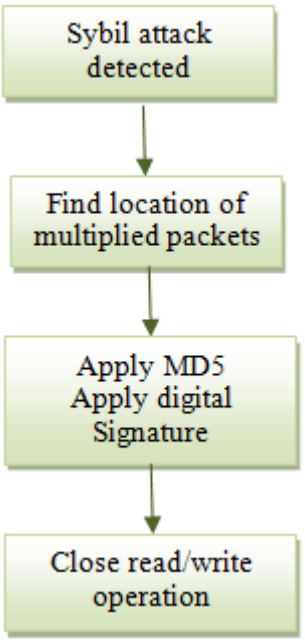

Fig.2. Diagram Showing Flow of Sybil Mitigation Scheme

V. Results and Discussion

A. *Experimental results*

The first step before proceeding is to make the server client environment. The server client environment is created by letting the server communicated with the client. The client and server will recognize themselves and the communication will take place as the gateway is established. Fig. 3 shows the status of server before starting the communication. The server status is shown as "Stopped" as the server is yet to start.

Before starting the server, the file receiving path is to be selected to keep the file received by a server. The status will be changed as: Server Status: running and waiting to receive file. The key receiver window will be opened after starting the server. Fig. 4 shows the server status and the file receiving path. Also, fig. 5 shows the key receiver window.

At the client side, the window to select the file to send to the server will be opened. From this window, we can select the file to be sent. The IP address is also shown on the window. The IP to connect to the server is to be inserted to make the communication secured and authenticated. The file to be uploaded can also be encrypted to provide the verification of the client. Fig. 6 shows the client side window where the file name is the name of the selected file that is, Sybil file and the text of the file is also shown in the text box on left. After uploading a file, the file will be in authentication process as to provide the established communication authentication. The status of the client will be

disconnected as a file is in authentication process. Only after the process has been completed, the client will be connected to the server. After the authentication is over, the key window will be opened.

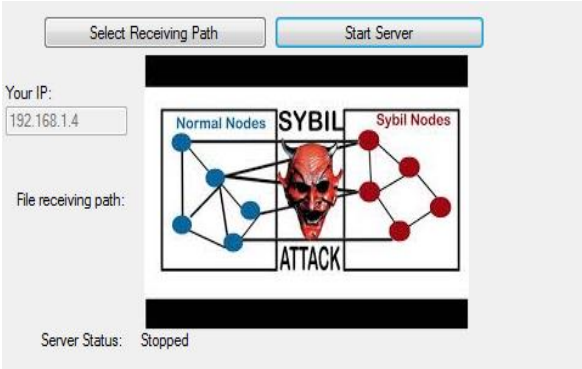

Fig.3. Status of the Server before Starting Communication

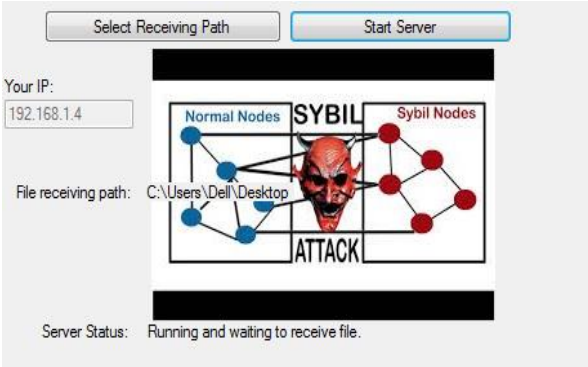

Fig.4. Server Status and File Receiving Path

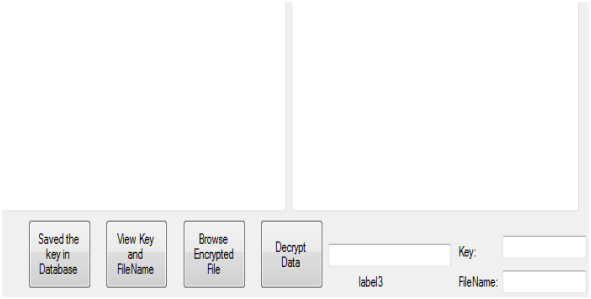

Fig.5. Key Receiver

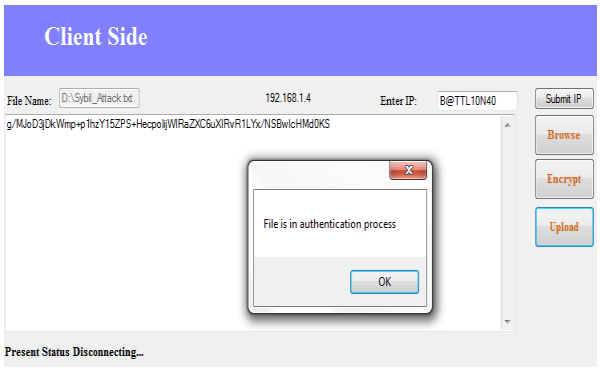

Fig.6. File Uploading At Client Side

At the key window, the username and password of the user will be displayed and this information along with the key computed will be transferred to the server to provide the verification at the server side, the key will be verified and the location of the file will also be verified. If the location and the key remain same, the file is not a Sybil file. But if the file is found to be multiplied at the various locations copying the key of the honest file, the file will be detected as a Sybil file. Fig. 7 shows the key window for verification of the user.

At the server side, the information of the user sent will be displayed and stores at the background. After receiving a file, if the file is observed to be multiplied at the various locations, it is detected as a Sybil attack file. Fig. 8 shows the detection of Sybil attack file.

Fig.7. Key Window at Client Side

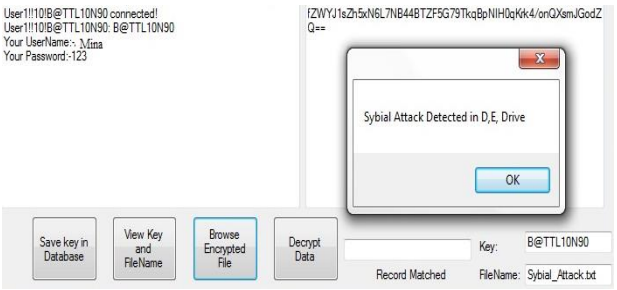

Fig.8. Detection of Sybil Attack File

After detection of Sybil attack, Sybil mitigation scheme will be applied. This scheme targets the Sybil attack packets. The behavior shown by the packet confirms it as a Sybil attack. The keys are made unique for each file. If the key is not matched the file is detected as the malicious file. The address where the file is copied with fake key is identified. The file in not allowed to make any operations by closing read/write access of the file and the file is further not allowed for any of the operations. Fig. 9 shows the window after mitigation scheme is being applied. In this approach the cost and time is minimized as, the file is denied with the read/write permission before behaving maliciously and it is stopped from making harm to the network.

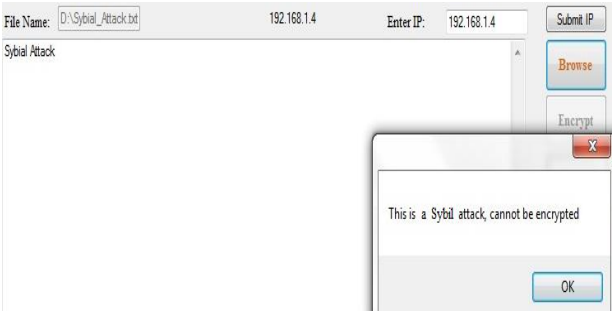

Fig.9. Mitigation of Sybil Attack

B. Evaluation results

The impact of Sybil attack in the network is studied using the attack detection rate. An attack detection rate is the rate of detecting the attack packets among the total number of packets received. Each packet is verified for checking its behavior. As a server receives first packet of the flow, the behavior of the packet is checked. The packet showing some malicious activity is traced and depending upon the observation of the behavior of the packet, it is detected as the Sybil packet. Proposed scheme can efficiently detect the Sybil attack packets among the total number of packets sent. This procedure is followed for all the packets in the stream of packets. Fig. 10 shows the result of the detection of packets as Sybil attack packets amongst the total number of attack packets. The result of the test shows that Sybil packets are detected efficiently in each test.

The false positive rate is the rate of falsely detecting honest packets as Sybil packets. Sometimes, honest packets show the behavior as if it is malicious one. The system may detect such packets as malicious packets. The aim is to decrease false positive rate so that the honest packets should not frequently be detected as Sybil attack packets. Fig. 11 shows the graph of the false positive rate with respect to the detection rate. The false positive rate is minimized for increase in detection rate. The table of false positive rate is shown in Table 1.

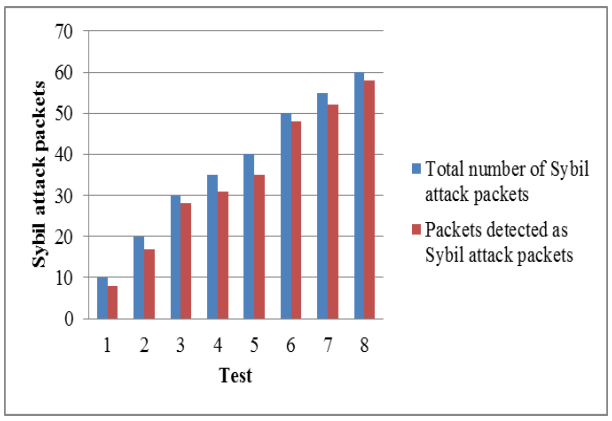

Fig.10. Graph Showing Detection Rate of Sybil Attack

Table 1. Values of False Positive Rate Along With Detection Rate

Detection rate	False positive rate
0.9	0.04
0.91	0.038
0.92	0.031
0.93	0.03
0.94	0.028
0.95	0.025
0.96	0.02
0.97	0.018
0.98	0.015

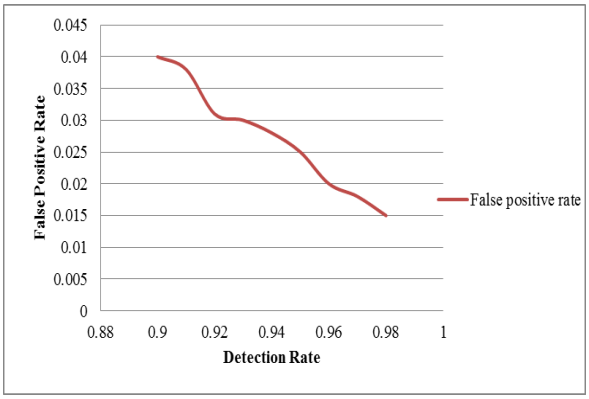

Fig.11. Graph Showing False Positive Rate

Table 2. Values of False Negative Rate Along With Detection Rate

Detection rate	False negative rate
0.9	0.02
0.91	0.018
0.92	0.012
0.93	0.01
0.94	0.009
0.95	0.007
0.96	0.004
0.97	0.004
0.98	0.004

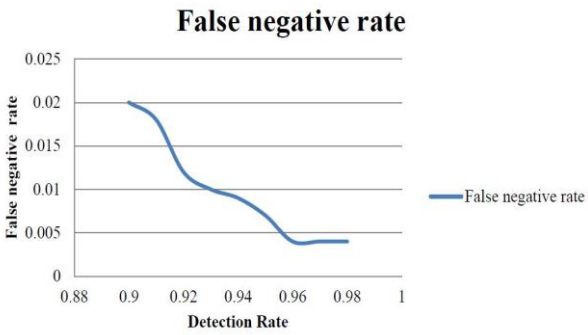

Fig.12. Graph Showing False Positive Rate

False negative rate is the third evaluation parameter. The false negative rate is the rate of detecting Sybil attack packet as an honest packet falsely. The system may sometimes detect Sybil packet as an honest packet. This abnormality may be due to some malicious activities happening in the network or the behavior of the Sybil packet to show as an honest packet. The table showing the values of false negative rate against the detection rate is shown in Table 2. Fig. 12 shows the graph plotted for false negative rate against detection rate. It can be clearly observed from the graph that the false negative rate is decreasing as increase in the detection rate. The false negative rate should be minimized to achieve the better efficiency in detection of Sybil attack in the network. The false negative rate has been minimized for the proposed approach.

VI. Conclusion and Future Scope

In this paper, the mechanism is proposed both to detect and mitigate Sybil attack in the peer-to-peer network. Sybil detection scheme is able to detect Sybil attack packets observing the behavior of the packets. Mitigation scheme is the combination of two methods cost incurred method and certified authentication method. In this scheme, the Sybil packets are mitigated from the network with a very efficient way.

The evaluation of the proposed system is done on the basis of the evaluation parameters, shows that the proposed scheme is able to identify Sybil attack in the network very efficiently. Also the mitigation scheme works effectively. The experimental results show that the proposed scheme works better in terms of good detection rate, low false positive rate and low false negative rate.

The future scope of this work may include making scheme more cost efficient and easy to implement in any type of network. The main focus will be on detection rate and false positive rate.

References

[1] G. Wang, F. Musau, S. Guo and M. B. Abdullahi,“Neighbor Similarity Trust against Sybil Attack in P2P E- Commerce”, IEEE Transaction on Parallel & Distributed Systems, vol. 26, no. 3, pp. 824-833, Mar 2015.

[2] Lin Cai and Roberto Rojas-Cessa, “Containing Sybil Attacks on Trust Management Schemes for Peer-to-Peer Networks”, International Conference on Communication (ICC), 2014, pp. 841-846. IEEE.

[3] W. Wei, F. Xu, C. C. Tan and Q. Li, "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2492-2502, Dec 2013.

[4] N. Z. Gong, M. Frank and P. Mittal, "SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection," IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 976-987, Jun 2014.

[5] J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen and Y. Dai, "VoteTrust: Leveraging friend invitation graph to defend against social network Sybils," INFOCOM, 2013 Proceedings IEEE, Turin, 2013, pp. 2400-2408.

[6] P. Liu, X. Wang, X. Che, Z. Chen and Y. Gu, "Defense against sybil attacks in directed social networks," International Conference on Digital Signal Processing (DSP), 2014, pp. 239-243.

[7] C. Banerjee and S. Saxena, "Sybil node detection in peer-to-peer networks using indirect validation," India Conference (INDICON), 2014, pp. 1-7 .IEEE.

[8] X. Xiang, "A Sybil-resilient Contribution Transaction Protocol," International Conference on Computational Intelligence and Security (CIS), 2011, pp. 690-692.

[9] L. Xiao, L. J. Greenstein, N. B. Mandayam and W. Trappe, "Channel-Based Detection of Sybil Attacks in Wireless Networks," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 492-503, Sept 2009.

[10] Y. Chen, J. Yang, W. Trappe and R. P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2418-2434, Jun 2010.

[11] S. Chang, Y. Qi, H. Zhu, J. Zhao and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103-1114, Jun 2012.

[12] H. Yu, M. Kaminsky, P. B. Gibbons and A. D. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," IEEE/ACM Transactions on Networking, vol. 16, no. 3, pp. 576-589, Jun 2008.

[13] H. Yu, P. B. Gibbons, M. Kaminsky and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks", IEEE/ACM Transactions on Networking, vol. 18, no. 3, pp. 885-898, Jun 2010.

[14] B. S. Jyothi and J. Dharanipragada, "SyMon: Defending large structured P2P systems against Sybil attack," International Conference on Peer-to-Peer Computing, P2P 2009.pp. 21-30. IEEE.

[15] P. V. Kumar and M. Maheshwari, "Prevention of Sybil attack and priority batch verification in VANETs," International Conference on Information Communication and Embedded Systems (ICICES), 2014, pp. 1-5.

[16] X. Liang, X. Lin and X. S. Shen, "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 310-320, Feb 2014.

[17] N. Tran, J. Li, L. Subramanian and S. S. M. Chow, "Optimal Sybil-resilient node admission control," Proc. in INFOCOM, 2011, pp. 3218-3226. IEEE.

[18] S. Sinha, A. Paul and S. Pal, "The sybil attack in Mobile Adhoc Network: Analysis and detection," International Conference on Computational Intelligence and Information Technology, (CIIT) 2013, pp. 458-466.

[19] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," Information Processing in Sensor Networks, IPSN 2004, pp. 259-268.

[20] M. Demirbas and Youngwhan Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," International conference on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2006, pp. 564 -570.

[21] G. Danezis and P. Mittal, “Sybilinfer: Detecting Sybil nodes using social networks,” NDSS, 2009.

[22] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, “Optimal Sybil-resilient peer admission control,” International Conference Computer Communication, 2011, pp. 3218–3226, IEEE.

[23] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi and A. Panconesi, "SoK: The Evolution of Sybil Defense via Social Networks," International Symposium on Security and Privacy (SP), 2013 pp. 382-396. IEEE.
[24] S. Golestani Najafabadi, H. R. Naji and A. Mahani, "Sybil attack Detection: Improving security of WSNs for smart power grid application," Smart Grid Conference (SGC), 2013, pp.273-278.
[25] R. Liu and Y. Wang, "A New Sybil Attack Detection for Wireless Body Sensor Network," International Conference on Computational Intelligence and Security (CIS), 2014, pp.367-370.
[26] V. Palanisamy, P. Annadurai and S. Vijilakshmi, "Curbing and curing sybil attack in ad hoc network," International Conference on Advanced Computing (ICAC), 2009, pp. 1-5.
[27] Q. Zhang, P. Wang, D. S. Reeves and P. Ning, "Defending against Sybil attacks in sensor networks," International Conference on Distributed Computing Systems Workshops, 2005, pp. 185-191.IEEE.
[28] B. Viswanath "Exploring the design space of social network-based Sybil defenses," International Conference on Communication Systems and Networks (COMSNETS), 2012, pp. 1-8.
[29] K. P. N. Puttaswamy, H. Zheng and B. Y. Zhao, "Securing Structured Overlays against Identity Attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 10, pp. 1487-1498,2009.
[30] J. R. Douceur. "The Sybil attack." IPTPS, Mar 2002.
[31] A. Bhise and S. D. Kamble, "Review on detection and mitigation of Sybil attack in the network", International conference on Information Security and Privacy (ICISP), Dec. 2015.
[32] Mandeep Kaur, Manish Mahajan,"Movement Abnormality Evaluation Model in the Partially Centralized VANETs for Prevention Against Sybil Attack", IJMECS, vol.7, no.11, pp.20-27.
[33] Bibhu, V., Roshan, K., Singh, K. B., & Singh, D. K. Performance Analysis of black hole attack in VANET. International Journal of Computer Network and Information Security (IJCNIS), vol.4, no.11, pp.47-54, 2012.
[34] Joe, M. M., Shaji, R. S., & Kumar, K. A. Establishing Inter Vehicle Wireless Communication in Vanet and Preventing It from Hackers. International Journal of Computer Network and Information Security (IJCNIS), vol. 5, no. 8, 55, 2012.

Author's Profiles

Arpita M. Bhise is a PG Scholar at Yeshwantarao Chavan College of Engineering, Nagpur (An Autonomous Institution Affiliated to Rashtrasant Tukdoji Maharaj Nagpur University). She received Bachelor's degree (B.E.) in Information Technology, from St. Vincent Pallotti College of Engineering, Nagpur. She also has received Master's degree (Master of Business Administration) in Human Resources subject from Pune University. Her main research area includes network security, communication security and information security.

Shailesh D. Kamble received Master of Engineering degree from Prof Ram Meghe Institute of Technology and Research, formerly known as College of Engineering, Badnera under Sant Gadge Baba Amravati University, Amravati, India. Presently, he is Ph.D. candidate in department of Computer Science and Engineering from G.H. Raisoni College of Engineering (An Autonomous Institution Affiliated to Rashtrasant Tukdoji Maharaj Nagpur University), Nagpur, India. He is currently working as an associate professor at Yeshwantarao Chavan College of Engineering, Nagpur. His current research interests include image processing, network security, video processing and language processing. He is the author or co-author of more than 40 scientific publications in International Journal, International Conferences, and National Conference.

How to cite this paper: Arpita M. Bhise, Shailesh D. Kamble,"Detection and Mitigation of Sybil Attack in Peer-to-peer Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.9, pp.56-63 2016.DOI: 10.5815/ijcnis.2016.09.08

