Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 395 – 401

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Review on Detection and Mitigation of Sybil attack in the network

Arpita M. Bhise[a], Shailesh D. Kamble[b]

[a]*PG Student, Department of Computer Technology,Yeshwantrao Chavan College of Engineering, Nagpur 441110, India*
[b]*Assistant Professor, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur 441110, India*

Abstract

Sybil attack is an attack in which the identities of the node are subverted and the large number of pseudonymous identities is produced to gain the access of the network. In this paper, we studied the detection mechanism of Sybil attack in peer-to-peer reputation systems, self-organizing networks and even social network systems. Also, various methods to mitigate the Sybil attack are analyzed. The studied mechanisms are evaluated in terms of detection rate, false positive rate, false negative rate and non-trustworthy rate. A research component in detection and mitigation of Sybil attack is, how to improve the detection rate and to minimize the false positive and false negative rate.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Sybil attacks; reputation system; pseudonymous identities; peer-to-peer networks

1. Introduction

Many security mechanisms are developed in order to keep the network protected from various attacks. Amongst them are the identity attacks. A Sybil attack is an identity attack in which, the malicious node creates fake identities and claim to be different node. It will do so by obtaining the information of the honest node by various ways. An attacker can perform Sybil attack by communicating directly with legitimate nodes by sending the radio messages to the Sybil nodes, by fabricating the new identities or by stealing the identities of the honest peer or by participating inthe network in large amount and by allowing only some to launch an attack[21].The common targets for Sybil attack are the reputation system, along with the real world systems such as social networking sites and wireless sensor networks[2,3,4,5,6,12,14,15,19,20].

* Arpita M. Bhise. Tel.:+91-9665670064.
*E-mail address:*arpita.bhise08@gmail.com.

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.080

A Sybil attack is becoming severe problem in many areas for example in voting system, many fake IP are created to cast a vote and also be used to link the results of searches to the terms searched for political advantages. In the ad-hoc networks like MANET, because of lack of centralized authority, the Sybil nodes can mislead the honest nodes resulting into hijacking the nodes[31]. Security provided to the networks also face some security challenges because, wireless networks are susceptible to the passive and active attacksAlso in social networking sites, the acceptance of the fake identity accounts are made in large ratio[13].

Many solutions are developed for the detection of Sybil attack in various networks. Some of them results well in particular network such as Sybil Guard, Sybil Limit for social networking sites[13,14], while watchdog and path rater in ad-hoc networks also RSSI based and channel based detection in Wireless sensor networks[21,23]. Likewise, the defence mechanisms are also developed in order to overcome the Sybil attack it includes trusted certification[1], Votetrust[6], Sybil Defender[4], Sybil Limit[14]. These schemes works in centralized or distributed manner in order to defend the Sybil attack. Advantages of these schemes are that they are very effective and they all are modified to improve the performance of algorithm. But the disadvantages are either they are costlier or they are based on the models which themselves are vulnerable to the attacks. The performance evaluation parameters used in this paper to analyse the mechanisms are : detection rate, non-trustworthy rate, false positive rate and false negative rate. Detection rate is the proportion of detected Sybil nodes to the total Sybil nodes. Non-trustworthy rate is the ratio of the number of honest peers which are falsely marked as Sybil peers to the number of total honest peers. False positive rate is the rate of detecting the honest nodes as Sybil nodes.

The survey of the existing schemes of detection and defence of Sybil attack are summarized. We then review the application domains vulnerable to the Sybil attacks. The rest of the paper is organized as follows: In section 2 the literature survey of the detection and defence strategies of Sybil attack is done section 3 surveys general approaches for countermeasures against Sybil attack. Section 4 explains the security challenges of Sybil attack in the network. And finally we make some discussion and future scope in section 5.

2. Literature Survey

In this section, we surveyed various effective detection and defence mechanisms on types of networks. Wei Wei et al.[4] proposed the approach called Sybil defender for social networks. This approach is based on performing a limited number of random walks within the social graphs. Conducting the experiment on real world topologies, researchers claimed that this strategy is the most efficient and effective in order to identify the Sybil nodes and Sybil communities around the Sybil node. Also this strategy is useful in limiting the attacking edges in online social networks by relationship rating. Wang et al.[2] developed the mechanism to address Sybil attack, in p2p e-commerce applications. By exploiting the neighbour similarity trust relationship, duplicated Sybil attack peers can be identified in P2P E-Commerce. The security and performance analysis shows that this approach can minimize the attack. Sybil Belief is a mechanism developed by Neil et al.[5] proposed the mechanism, based on the semi supervised learning approach to detect the Sybil attack in the network. It takes nodes of social network and small set of Sybils as an input and propagates the label information from known Sybil node to the remaining nodes. With low false positive rate and low false negative rate, it is accurate in identifying the Sybil nodes.

Liang Xiao et al.[10] proposed a mechanism of detecting the Sybil clients in the wireless sensor networks. This method is implemented by using the concept of channel based mechanism. The Sybil detector performance is verified via both a propagation modelling software and field measurements using a vector network analyser, for typical indoor environments. By proving the low false alarm rate and miss rate researchers estimated number of channel estimates, number of total clients, number of Sybil clients, and number of access points**.** Ying ying Chen et al.[11] proposed the mechanism to detect and localize the positions of the Sybil attack in the wireless sensor networks. The proposed approach contains the RSSI based detector and by integrating attack detector into a real time indoor localization system, the position of the attack is localized efficiently. With high detection rate and low false positive rate, the attack detector utilizing spatial correlation of RSS and attack localizer can detect and locate the Sybil attack accurately. A novel Sybil attack detection mechanism was proposed by Shan Chang et al.[12] for urban vehicular network. The mechanism Footprint was proposed by the researchers using trajectories of vehicles by preserving

their location privacy. By using the temporal limitation on the linkability of two authorized messages, thevehicle can generate the location hidden trajectories for location-privacy-preserved identification by collecting authorized messages. This strategy can detect Sybil community very efficiently in urban vehicular network.

Yu et al.[13,14] proposed the mechanisms to defend against the Sybil attack in p2p social networks. By assuming that the social networks are fast mixing, Sybil Guard can allow large Sybil nodes to be accepted. Sybil Limit is an approach which uses the same approach as that of Sybil Guard but the Sybil attack acceptance is minimized to 200 times that of Sybil Guard. Sybil Limit accepts only Sybil per attack edges. Sybil Limit uses balance condition to deal with escaping tails of the verifier hence is an effective mechanism for defence against the Sybil attack. P.Vinoth Kumar et al.[16] proposed mechanisms which aims to provide safety and traffic management in VANET. In this proposed approach, Batch authentication and key agreement method is used to authenticate multiple request sent from different vehicles. The priority is provided to the request messages by using priority Batch Verification algorithm. This system prevents Sybil attack by restricting timestamps by RSU and can effectively defend against the Sybil attack in VANETs.

Light weight identity certificate method was used by Zhang et al.[32] to defeat against Sybil attack in the sensor networks. The proposed approach uses one way key chains and Merkel hash trees. This proposed method also provides means for authentication of all data messages. The Sybil attack is defended with very lower computational requirements and providing better security measures against the Sybil attack in wireless sensor network. Fong[34], formalized Denning's principle of privilege attenuation as a run time property and proved that it is necessary and sufficient condition for preventing the Sybil attack. The static policy analysis is also devised to show that Facebook-style social network is principle of privilege attenuation. Ling Xu[40], proposed Sybil resisting network clustering to resist Sybil attack by preventing honest nodes to participate into communication. This mechanism tries to detect attack edges by clustering Sybil nodes and honest nodes. . Xiangtao Liu et al.[41] measures Sybil attack in kademlia based networks. OSN based Sybil defences has been proposed by David Koll et al.[44]. They measured the performance of OSN based mechanism in classical as well as modern scenario. The study points out the efficient structure of modern scenario.

3. General approaches for countermeasures against Sybil attack

Since the first countermeasure developed against Sybil attack, many researchers tried to build the new solutions each time stating that it overcomes the previous disadvantages. Various schemes has been developed by the researchers for counter measuring the Sybil attack. The review of these schemes are as given below:

3.1 Trusted Certification

Trusted certification is the first solution developed against the Sybil attack. Douceur[1]proposed that the trusted certification is the only potential approach to defend against the Sybil attack. In this approach, the centralized Authority CA is used to validate the entities. Each entity is uniquely identified by its unique digital signature assigned to them by the certifying authority. Authentication is usually provided by asymmetric key cryptography. But this approach has larger overheads when applied to the large scale system also it is not cost efficient.

3.2 RSSI based scheme

Demirbas et al.[23] proposed the lightweight received signal strength based scheme for Sybil attack problem. This is the robust and accurate scheme to detect the Sybil attack. This scheme is based on the received signal strength of messages. The cooperation of communication message and additional node makes this scheme successful but unreliable. In this strategy, detector node is used to receive RSSI value and its identity from each node. This scheme generates false positive alarm making it unreliable.

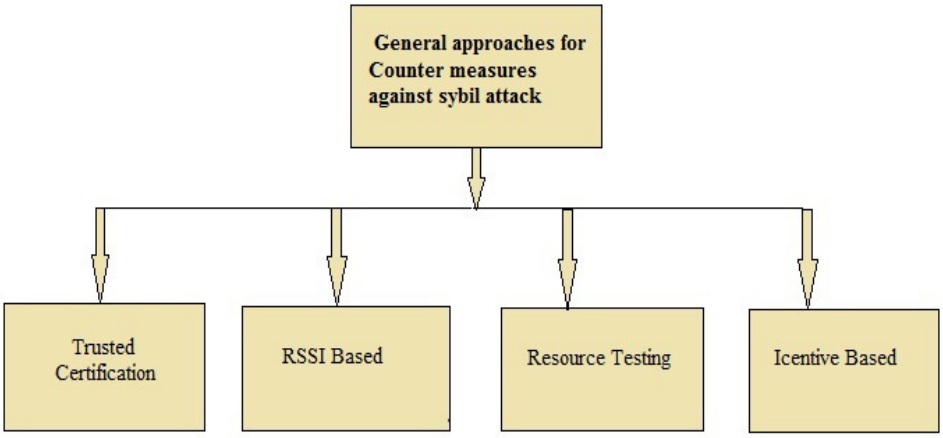

Fig.1. General approaches for counter measures against Sybil attack

3.3 Resource testing

The aim of resource testing is to determine if the number of identities possess fewer resources than would be expected if they were independent. Newsome[21] proposed the resource testing as another scheme for countermeasure against Sybil attack. In this strategy, a verifier calculates the resources i.e. energy, storage, capacity of the identities. If the node with the larger resources than a starved node is found, it is considered as an attacker node. The verifier messages may flood the network which makes this scheme unsuccessful. Hence to overcome this Newsome proposed another "radio resource testing" scheme, where the each node has one radio which can transmit and receive radio only at one channel.

3.4 Incentive based scheme

Incentive based scheme is proposed by Margolin et al.[36] based on reward scheme where economic incentives are used and with the wide range of application area. This protocol offers a reward to the adversaries if the identities which are controlled by it are revealed. The target peer name is stated by an identity when payment in exchange is received by it.

Table 1. General approaches with their application domain, advantages and disadvantages

	Trusted Certification	Resource Testing	RSSI Based	Incentive Based
Methodology	Based on centralised Certification authority	Calculation of resources	Based on radio signal strength	Based on rewards
Advantages	Efficient in large network	No bandwidth overhead	Robust, less false positive rate	No clock synchronization needed
Disadvantages	Not much cost efficient	Cannot provide complete defence	Reliability is lesser	May encourage attackers economically
Application Domain	General	General	Wireless sensor network	Ad hoc network

4. Security challenges in the network

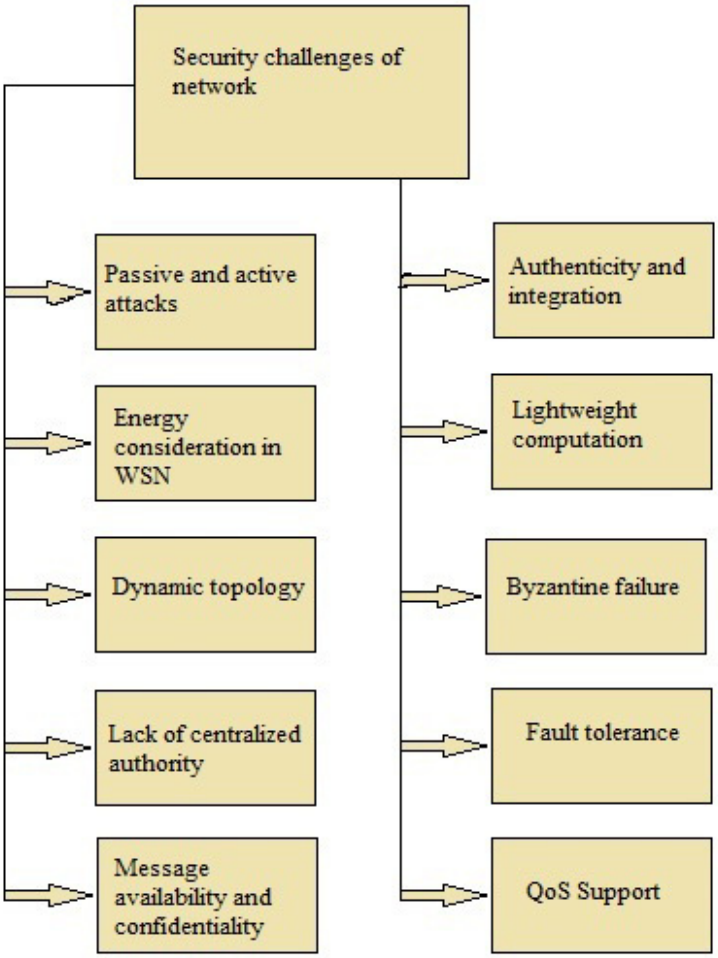

Fig.2. Security challenges of Network

Security has become primary concern of the researchers now-a-days. Many security mechanisms are based on some specific assumptions which are vulnerable to severe attacks. While building the security mechanism, all security challenges of network should be taken into consideration. This section refers to the security challenges in the network. These are as follows:

- Passive and active attacks: most wireless networks are vulnerable to the passive and active attacks. In which, the identities of the nodes are stolen hence the detection of honest peers become challenging task.
- Energy consideration in WSN: Energy consideration in wireless sensor networks plays very vital role as sensor nodes have limited energy in which the task is to be completed.
- Dynamic topology: Dynamic topology of the network is also the security challenge of network for detecting the attack nodes.
- Lack of centralized authority: Centralized authority is absent in some networks this will lead to disturb the mechanism of detecting the Sybil attack.

- Message availability and confidentiality: All messages should be available but at the same time, the confidentiality of the messages should also be maintained. Loss of confidentiality may lead the network prone to the attack.
- Authenticity and integration: The messages should be provided integrity in the sense that it should not be altered by an attacker.
- Lightweight computation: The computations build should be lightweight in order to make the mechanism cost effective and time efficient.
- Byzantine failure : In wireless sensor network, some node taking participation in routing may be disrupted by an attacker this may cause unrecoverable failure to the network
- Fault tolerance: Sometimes fault tolerance is very less in network e.g. in wireless network. Hence the defense mechanism has to be strong in order to face the faults in the network.

5. Discussion

The security of networks plays very vital role in transaction and communication. To keep these networks attack free we have to develop the mechanisms to identify and defeat against those attacks. In order to tackle with the Sybil attack in various network we surveyed various effective detection and mitigation mechanisms for Sybil attack in the network. This paper also includes the general approaches used to tackle the Sybil attack. The detection rate, false positive rate, false negative rate and non-trustworthy rate are the parameters used to evaluate the performance of the existing mechanisms.

The future scope involves the development of cost effective and efficient detection and mitigation mechanism in the network with the specific focus on improving the detection rate. At the same time the focus of the future scope will be on minimizing the false positive rate and false negative rate.

References

1. J. R. Douceur, The Sybil attack .*In Proceedings for the First International Workshop on Peer-to-Peer Systems* (IPTPS'02), vol. 2429.Cambridge, MA, USA: Springer; 2002. p. 251-260.

2. Guojun Wang, Felix Musau, Song Guo, and Muhammad BashiAbdullahi.Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce. *IEEE Transactions on Parallel and Distributed Systems*, March 2015. Vol. 26.p.824-833.

3. Lin Cai and Roberto Rojas-Cessa. Containing Sybil Attacks on Trust Management Schemes for Peer-to-Peer Networks. *IEEE ICC - Communication and Information Systems Security Symposium.* 2014. p. 841-846.

4. Wei Wei, FengyuanXu, Chiu C. Tan, Member, IEEE, and Qun Li, Senior Member, IEEE. SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks. *IEEE Transaction On Parallel And Distributed Systems*, Dec. 2013. Vol. 24, p. 2492-2502.

5. Neil Zhenqiang Gong, Mario Frank, and Prateek Mittal.SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection. *IEEE Transaction on Information Forensic And Security* June 2014. Vol. 9. p. 976-987.

6. Zhi Yang, JilongXue, Xiaoyong Yang, Xiao Wang, and Yafei Dai.VoteTrust: Leveraging Friend Invitation Graph to Defend against Social Network Sybils.*IEEE Transactions on Dependable and Secure Computing,* 2015.p. 1-14.

7. Pengfei Liu, Xiaohan Wang, XiangqianChe, Zhaoqun Chen and YuantaoGu. DefenseAgainst Sybil Attacks in Directed Social Networks. *19th International Conference on Digital Signal Processing* Aug. 2014. p. 239-243.

8. Chayan Banerjee, ShubhraSaxena.Sybil Node Detection in Peer-to-Peer Networks using Indirect Validation. *Annual IEEE India Conference (INDICON)* 2014

9. Xu Xiang. A Sybil-resilient Contribution Transaction Protocol. *7th International Conference on Computational Intelligence and Security* 2011. p. 690-693.

10. Liang Xiao,Larry J. Greenstein, Narayan B. Mandayam, Wade Trappe. Channel-Based Detection of Sybil Attacks in Wireless Networks.*IEEE Transaction on Information Forensics And Security* Sep. 2009. Vol. 4. p. 492-503.

11. Yingying Chen, Jie Yang, Wade Trappe, Richard P. Martin. Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks,*IEEE Transaction On Vehicular Technology*June 2010. Vol. 59. P. 2418-2434.

12. Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, Xuemin (Sherman) Shen. Footprint: Detecting Sybil Attacks in Urban Vehicular Networks.*IEEE Transaction On Parallel And Distributed Systems*June 2012. Vol. 23. P. 1103-1114

13. Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham D. Flaxman, SybilGuard: Defending Against Sybil Attacks via Social Networks, *IEEE/ACM Transaction On Networking*June 2008. Vol. 16.p.576-589.

14. Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, Feng Xiao. SybilLimit: A Near-Optimal Social Network DefenseAgainst Sybil Attack.*IEEE/ACM Transaction On Networking* June 2010. Vol. 18. p. 885-898.
15. Jyothi B S, DharanipragadaJanakiram.SyMon: Defending Large Structured P2P Systems Against Sybil Attack. *IEEE P2P'09* September 2009. p. 21-30.
16. P.Vinothkumar,M. Maheshwari.Prevention Of Sybil Attack And Priority Batch Verification In VANETs. *ICICES* 2014.
17. Xiaohui Liang, Xiaodong Lin, Xuemin (Sherman) Shen. Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks. *IEEE Transaction On Parallel And Distributed Systems*February 2014. Vol. 25.p. 310-320.
18. N. Tran, J. Li, L. Subramanian, S. S.M. Chow. Optimal Sybilresilient node admission control .*IEEE INFOCOM*2011.
19. Manjunatha T., Sushma M., Shivakumar K. Security Concepts and Sybil Attack Detection in Wireless Sensor Networks.*IJETTCS*March – April 2013. Vol. 2.
20. SomnathSinha, Aditi Paul, Sarit Pal. The Sybil Attack In Mobile Adhoc Network: Analysis And Detection
21. James Newsome, Elaine Shi, Dawn Song, Adrian Perrig. The Sybil Attack in Sensor Networks: Analysis &Defenses.
22. G. Theodorakopoulos, J. S. Baras. Trust Models and Trust Evaluation Metrics for Ad hoc Networks. *IEEE Journal on Selected Areas in Communications*2006.vol. 24. p. 318–328.
23. M. Demirbas, Y. Song. An RSSI-based scheme for Sybil attack detection in wireless sensor networks.*Proceedings of Internationalon a Symposium World of Wireless, Mobile and Multimedia Networks(WoWMoM'06)*2006.p. 564–570.
24. G. Danezis, P. Mittal. Sybilinfer: Detecting Sybil nodes using social networks. *NDSS* 2009.
25. A. Cheng, E. Friedman. Sybilproof reputation mechanisms. *Proceedings of IEEE ISCC* 2008. p. 246-253.
26. T. Nguyen, L. Jinyang, S. Lakshminarayanan, S. M. Chow. Optimal Sybil-resilient peer admission control.*Proceeding of the 30th IEEE International Conference onComputer Communications (INFOCOM)* 2011. p. 3218–3226.
27. Lorenzo Alvisi, Allen Clement, Alessandro Epasto. SoK: The Evolution of Sybil Defense via Social Networks.*IEEE Symposium on Security and Privacy* 2013. p. 382-396.
28. Shahrzad Golestani Najafabadi, Hamid Reza Naji, Ali Mahani. Sybil Attack Detection: Improving Security of WSNs for Smart Power Grid Application.*Conference on Smart Electric Grids Technology (SEGT2012)* December 2012. p. 273-278.
29. Ruixia Liu, Yinglong Wang. A New Sybil Attack Detection for Wireless Body Sensor Network, *Tenth International Conference on Computational Intelligence and Security* 2014. p. 367-370.
30. Murat Demirbas, Youngwhan Song. An RSSI-based Scheme for Sybil Attack Detectionin Wireless Sensor Networks.*International Symposium on a World of Wireless, Mobile and Multimedia Networks*2006.
31. V. Palanisamy,P. Anndaurai. Curbing and Curing Sybil attack in Ad hoc Network. *ICAC* 2009. p. 1-5.
32. Qinghua Zhang, Pan Wang, Douglas S. Reeves, Peng Ning.Defending against Sybil Attacks in Sensor Networks. *Proceedings of25th IEEE International Conference on Distributed Computing Systems Workshops*2005.
33. Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel. Exploring the design space ofsocial network-based Sybil defences.Fourth International Conference on Communication Systems and Networks (COMSNETS) 2012.
34.Philip W. L. Fong. Preventing Sybil Attacks by Privilege Attenuation :A Design Principle for Social Network Systems.*IEEE Symposium on Security and Privacy* 2011. p. 263-278.
35. Krishna P.N. Puttaswamy, Haitao Zheng, Ben Y. Zhao. Securing Structured Overlaysagainst Identity Attack, *IEEE Transactions On Parallel And Distributed Systems*October 2009. Vol. 20. p. 1487-1498.
36.A.Margolin, N. Boris, L.B.Neil. Informant: Detecting Sybils using incentives. *Proceedings of Financial Cryptography (FC*) 2007.Springer.p. 192-207,
37. Zhong Su, Chuang lini. Security mechanisms analysis of wireless sensor networks specific routing attacks. *First International Symposium on Pervasive Computing and Applications* 2006.
38. Haifeng Yu, Chenwei Shi, Michael Kaminsky.DSybil: Optimal sybil-Resistance for Recommendation Systems.*Proceedings of IEEE Symposium on Security and Privacy (S&P'09)* May 2009. p. 283–298.
39. Daniele Quercia, Stephen Hailes. Sybil Attacks Against Mobile Users:Friends and Foes to the Rescue.*IEEE INFOCOM* 2010.
40. Ling Xu, SatayapiwatChainan, Hiroyuki Takizawa. Resisting Sybil Attack By Social Network and Network Clustering. *10th Annual International Symposium on Applications and the Internet*2010.
41.Xiangtao Liu. Measuring Sybil attacks in Kademlia-based networks.*AICCSA* 2011.
42.YongHao, Jin Tang, Yu Cheng. Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs.*IEEE Communications Society subject matter experts for publication (Globecom)* 2011.
43. Xun Li, Guangjie Han. Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks.*International Symposium on a World of Wireless, Mobile and Multimedia Networks2009.*
44. David Koll, Jun Li, Joshua Stein.On the State of OSN-based Sybil Defenses.*IFIP*2014.
45. Bayrem TRIKI.An RFID based System for the detection of Sybil attack in Military Wireless Sensor network. *World Congress on Computer Applications and Information Systems (WCCAIS)* 2014 .
46. Borisov.Computational Puzzles as Sybil Defense.*Proceedings of Sixth IEEE International Conference onPeer-to-Peer Computing* October 2006. p. 171-176.
47. B. Chen, K. Jamieson, H. Balakrishnan, R.Morris.Span: An energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *J ACM Wireless Networking* September 2002.Vol. 8. p. 481–494.
48. C. Piro, C. Shields, B.N. Levine. Detecting the Sybil Attack in Mobile Ad Hoc Networks.*Proceedings of Securecomm and Workshop* Aug. 2006. p. 1-11.
49. A. Cheng , E. Friedman. Sybilproof reputation mechanisms.*Proceedings of ACM SIGCOMM Workshop on Economics of peer-to-peer systems (P2PEcon'05)* Aug. 2005.p. 128–132.
50. J. A. Goguen, J. Meseguer. Security policies and security models.*Proceedings of IEEE Symposium on Security and Privacy (S&P'82)*1982.p. 11–20.