A Survey of Real Sybil Attacks (under construction)

Laurens Versluis
Delft University of Technology
Delft, The Netherlands
L.F.D.Versluis@student.tudelft.nl

ABSTRACT

1. INTRODUCTION

The sbyil attack was first described by Douceur [8]. Nowadays, it is a well-known attack on both centralized and decentralized systems and an active research area. In the sybil attack, malicious users create an unbounded number of *sybil* identities. Using these sybils, malicious users can perform several attacks. Hoffman et al. (2009) identified five classes of attacks:

1. Self-promoting: Attackers boost their own reputation or increase their gain/profit.
2. Whitewashing: Attackers avoid consequences of abusing the system and repair their own reputation to continue their attacks.
3. Slandering: Attackers manipulate the reputation of other users inside the system by e.g. false reports.
4. Orchestrated: A combination of the three attacks mentioned above.
5. Denial of Service: Attackers prevent the calculation and dissemination of reputation values.

Often these sybils are indistinguishable from real users and therefore a threat to systems relying on user input. Decentralized systems are particularly vulnerable. Without a central authority to certify users, decentralized systems are vulnerable to a variety of attacks, including the sybil attack [10]. Douceur argues that a central authority which certifies all identies may tbe the only effective solution, however even when a centralized authority is present, it still may not be feasible to certify real users and can even compromise the anonymity of peers [14, 6].

Sybil attacks occur in a variety of systems and networks such as overlay networks [20], social networks [3, 4, 15], content rating systems [12, 21] and vehicular ad hoc networks [18]. Since the problem is widespread and many solutions have been proposed, there are already surveys which compare different solutions/surveys [13, 16, 23].
The focus of this survey will not be yet another survey on the current state of the art, but will focus on real-world attacks using Sybil, eclipse and sinkholing techniques. We perceive these to be belonging to the same broad class of attacks. The goal is to provide a list of scientific articles and describe the datasets used in their evaluations. Sybils can be assigned a taxonomy as they can be compromised nodes, fake nodes [17] or whitewashed nodes, however we do not make this distinction inside datasets. The outcome of this survey will be the largest structured collection of various datasets which are collected if the data is publicly available or if the authors are willing to share their data. Additional datasets are added as well which were either created by means of manual annotation or by other parties.
The list of datasets will, for instance, cover fake profiles on social networking sites (Facebook), communication systems (Twitter), search engine link farms, auction sites, review sites, sock puppets on news sites, and various other Internet-deployed systems. A key challenge is the diversity and formatting of these datasets. The goal is to design a unifying format to enable scientists to easily use all available datasets for their latest research findings with minimal effort.

The survey will provide a structured listing with key aspects of each dataset, including, description, origin, size, creation date, and copyright license.

2. DATASETS IN SCIENTIFIC ARTICLES

We have composed a list of scientific articles on the topic of the sybil attack. We list – where applicable and available – the year, amount of nodes in the dataset, amount of sybils, whether it concerns real or synthetic data and whether the dataset is publicly available and mentioned in the paper. The results of this can be found in Table 1.

Our conclusion based upon this review is that even though most datasets use real data, often the sybils are fake or the ground-truth is missing. Some articles do not mention details of their dataset, such as amount of sybils, whether the ground-truth is known or the exact amount of nodes in their dataset. Moreover, we conclude that none of the articles mention the availability of their dataset nor actively promote it for further research.

3. DATASETS

As observed in Section 2, none of the datasets used has a ground truth. To allow further research to evaluate their work, a list of datasets is provided in Table . For each dataset, its key aspects such as size, creation date, origin To ensure minimal effort required to use the datasets, we have parsed all obtained datasets into one unifying format. This format will be explained first.

3.1 Format

The format of each dataset is as follows: *Very nice format here.*

3.2 Datasets with ground-truth

3.3 Datasets without ground-truth

4. CONCLUSION

In this paper we provided an overview of scientific articles and investigated their datasets used. From this, we conclude that even though most articles use real-world data, most papers do not or not accurately mention the details of their dataset. Moreover, we conclude that no article actively promotes/offers its dataset for further research.

We therefore gathered the datasets used in these scientific papers and added some additional datasets by means of third parties and creating new datasets ourselves using manual annotation and other means. The result is an overview of datasets which have one unifying format, are publicly available and can be used for further research.

Year	Mechanism	# Nodes	# Sybils	Real-world data	Dataset availability
2004	Overlay defense* [20]	5050	1010	No	• No link in paper • Public availability unknown • Author response pending
2005	Defending sensors* [29]	No simulation	No simulation	N/A	N/A
2006	Self-registration* [7]	±500	±20	No	• No link in paper • Public availability unknown • Author response pending
2006	SybilGuard [27]	1. 1.000.000 2. 10.000 3. 100	±100	No	• No link in paper • Public availability unknown • Author response pending
2006	Computational Puzzles [2]	No simulation	No simulation	N/A	N/A
2008	Sybillimit [26]	1. 932.512 2. 900.822 3. 106.002 4. 1.000.000	TBD	1. Yes 2. Yes 3. Yes 4. No	• No link in paper • Public availability unknown • Author response pending
2008	Cluster Analysis* [25]	1. 101 2. 94	All possible pairs: 1. 5.050 2. 4.371	Yes (Since it concerns real devices in this paper, we perceive it as real data)	• No link in paper • Public availability unknown • Author response pending
2009	SybilInfer [5]	1. 1.000 2. ±33.000	1. 100 2. ± 2.000	1. No 2. Yes	• No link in paper • Public availability unknown • Author response pending
2009	Timestamp series [18]	No simulation	No simulation	N/A	N/A
2009	SyMon [11]	50.000	2.500 to 25.000 in steps of 2.500	No	• No link in paper • Public availability unknown • Author response pending
2009	Dsybil [28]	1. 496.622 2. 2.339 3. 480.189 4. 6.040 5. 105.283	Unknown	Yes	• No link in paper • Public availability unknown • Author response pending
2009	SumUp [21]	3.002.907	No ground truth Estimation: 12% (360.349)	Yes	• No link in paper • Public availability unknown • Author response pending
2011	GateKeeper [22]	1. Varying (Synthetic) 2. 446.181 3. 539.242	1. Varying 2. 43.725 sybils admitted 3. 76.572 sybils admitted	1. No 2. Yes 3. Yes	• No link in paper • Public availability unknown • Author response pending
2011	Mitigating* [12]	> 65.000 (Sybil network attached, no information on size)	Not mentioned	Yes, real sybils unkown	• No link in paper • Public availability unknown • Author response pending

2011	Leveraging* [4]	542.133	16.264 (3%)	Yes	• No link in paper • Public availability unknown • Author response pending
2011	Incorperating trust* [15]	1. 4.158 2. 82.168 3. 11.204 4. 8.638 5. 7.066 6. 33.696 7. 75.879 8. 614.981 9. 1.000.000 10. 1.000.000 11. 1.000.000 12. 1.000.000 13. 1.134.890	Not mentioned	Yes	• No link in paper • Public availability unknown • Author response pending
2012	SybilDefender [24]	1. 3.072.441 2. 3.097.165	10.000, 5.000, 1.000 (Compromised nodes)	Yes	• No link in paper • Public availability unknown • Author response pending
2013	Sok [1]	1. 718.115 2. 26.588 3. 63.392 4. 92.117	Various	Yes	• No link in paper • Public availability unknown • Author response pending
2013	SybilShield [19]	100.000	500 (generated)	Yes, sybils are synthetic	• No link in paper • Public availability unknown • Author response pending
2014	SybilRank [3]	1. 10.000 2. 18.772 3. 9.877 4. 10.000 5. 7.115 6. 10.000 7. 10.000 8. 10.000	5.000 (connected to each dataset)	Yes, sybils are synthetic	• No link in paper • Public availability unknown • Author response pending

Table 1: Current state of the art reviewed on their datasets. (* = mechanism was not named by the author(s)).

5. REFERENCES

[1] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi. Sok: The evolution of sybil defense via social networks. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 382–396. IEEE, 2013.

[2] N. Borisov. Computational puzzles as sybil defenses. In *Peer-to-Peer Computing, 2006. P2P 2006. Sixth IEEE International Conference on*, pages 171–176. IEEE, 2006.

[3] Q. Cao. *Understanding and Defending Against Malicious Identities in Online Social Networks*. PhD thesis, Duke University, 2014.

[4] N. Chiluka, N. Andrade, J. Pouwelse, and H. Sips. Leveraging trust and distrust for sybil-tolerant voting in online social media. In *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, page 1. ACM, 2012.

[5] G. Danezis and P. Mittal. Sybilinfer: Detecting sybil nodes using social networks. In *NDSS*. San Diego, CA, 2009.

[6] P. Dewan and P. Dasgupta. Securing p2p networks using peer reputations: is there a silver bullet? In *Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE*, pages 30–36. IEEE, 2005.

[7] J. Dinger and H. Hartenstein. Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, pages 8–pp. IEEE, 2006.

[8] J. R. Douceur. The sybil attack. In *Peer-to-peer Systems*, pages 251–260. Springer, 2002.

[9] K. Hoffman, D. Zage, and C. Nita-Rotaru. A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys (CSUR)*, 42(1):1, 2009.

[10] O. Jetter, J. Dinger, and H. Hartenstein. Quantitative analysis of the sybil attack and effective sybil resistance in peer-to-peer systems. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–6. IEEE, 2010.

[11] B. Jyothi and J. Dharanipragada. Symon: Defending large structured p2p systems against sybil attack. In *Peer-to-Peer Computing, 2009. P2P'09. IEEE Ninth International Conference on*, pages 21–30. IEEE, 2009.

[12] A. M. Kakhki, A. Hannak, A. Mislove, and R. Sundaram. Mitigating sybil attacks on content rating systems. SOSP.

[13] D. Koll, J. Li, J. Stein, and X. Fu. On the state of osn-based sybil defenses. In *Networking Conference, 2014 IFIP*, pages 1–9. IEEE, 2014.

[14] N. B. Margolin, B. N. Levine, N. B. Margolin, and B. N. Levine. Quantifying and discouraging sybil attacks. *Computer Science Technical Report*, 67, 2005.

[15] A. Mohaisen, N. Hopper, and Y. Kim. Keep your friends close: Incorporating trust into social network-based sybil defenses. In *INFOCOM, 2011 Proceedings IEEE*, pages 1943–1951. IEEE, 2011.

[16] A. Mohaisen and J. Kim. The sybil attacks and defenses: a survey. *arXiv preprint arXiv:1312.6349*, 2013.

[17] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pages 259–268. ACM, 2004.

[18] S. Park, B. Aslam, D. Turgut, and C. C. Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pages 1–7. IEEE, 2009.

[19] L. Shi, S. Yu, W. Lou, and Y. T. Hou. Sybilshield: An agent-aided social network-based sybil defense among multiple communities. In *INFOCOM, 2013 Proceedings IEEE*, pages 1034–1042. IEEE, 2013.

[20] A. Singh, M. Castro, P. Druschel, and A. Rowstron. Defending against eclipse attacks on overlay networks. In *Proceedings of the 11th workshop on ACM SIGOPS European workshop*, page 21. ACM, 2004.

[21] D. N. Tran, B. Min, J. Li, and L. Subramanian. Sybil-resilient online content voting. In *NSDI*, volume 9, pages 15–28, 2009.

[22] N. Tran, J. Li, L. Subramanian, and S. S. Chow. Optimal sybil-resilient node admission control. In *INFOCOM, 2011 Proceedings IEEE*, pages 3218–3226. IEEE, 2011.

[23] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. An analysis of social network-based sybil defenses. *ACM SIGCOMM Computer Communication Review*, 41(4):363–374, 2011.

[24] W. Wei, F. Xu, C. C. Tan, and Q. Li. Sybildefender: Defend against sybil attacks in large social networks. In *INFOCOM, 2012 Proceedings IEEE*, pages 1951–1959. IEEE, 2012.

[25] J. Yang, Y. Chen, and W. Trappe. Detecting sybil attacks in wireless and sensor networks using cluster analysis. In *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*, pages 834–839. IEEE, 2008.

[26] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao. Sybillimit: A near-optimal social network defense against sybil attacks. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 3–17. IEEE, 2008.

[27] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. Sybilguard: defending against sybil attacks via social networks. *ACM SIGCOMM Computer Communication Review*, 36(4):267–278, 2006.

[28] H. Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao. Dsybil: Optimal sybil-resistance for recommendation systems. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 283–298. IEEE, 2009.

[29] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning. Defending against sybil attacks in sensor networks. In *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*, pages 185–191. IEEE, 2005.