A Survey of Real Sybil Attacks

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

ABSTRACT

1. INTRODUCTION

This survey 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 which are based on a publicly available real-world datasets. The outcome of this survey will be the largest structured collection of various datasets and the actual datasets themselves in the form of supplementary material.

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, such as, description, origin, size, creation date, and copyright license.

2. DATASETS

In this section, the current state of the art on Sybil attacks and their datasets is reviewed. We list well-known papers on the sybil attack and list several aspects including the year, size, amount of sybils, real or artificial data and availability of the dataset.

[1]

3. 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] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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*

[1] * = The proposed mechanism has not be named by the authors.

Year	Mechanism	# nodes	# sybils	Real-world data	Dataset availability
2004	Overlay defense* [12]	5050	1010	No	• No link in paper • Public availability unknown • Author response pending
2005	Defending sensors* [20]	No simulation	No simulation	N/A	N/A
2006	Self-registration* [6]	±500	±20	No	• No link in paper • Public availability unknown • Author response pending
2006	SybilGuard [18]	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 [17]	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* [16]	1. 101 2. 94	All possible pairs: 1. 5.050 2. 4.371	Yes	• No link in paper • Public availability unknown • Author response pending
2009	SybilInfer [5]	33.000	• 2000 • No ground-truth	Yes	• No link in paper • Public availability unknown • Author response pending
2009	Timestamp series [10]	No simulation	No simulation	N/A	N/A
2009	SyMon [7]	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 [19]	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 [13]	3.002.907	No ground truth Estimation: 12% (360.349)	Yes	• No link in paper • Public availability unknown • Author response pending
2011	GateKeeper [14]	33.000	• 2000 • No ground-truth	Yes	• No link in paper • Public availability unknown • Author response pending
2011	Mitigating* [8]	• 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]				
2011	Incorperating trust* [9]				
2012	SybilDefender [15]				
2013	Sok [1]				
2013	SybilShield [11]				
2011	GateKeeper [14]				
2014	SybilRank [3]				

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

European workshop, page 21. ACM, 2004.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.