Sybil Attacks and Their Defenses in Reputation Systems

October 19, 2016

Abstract

1 Introduction

Reputation systems (described in section 2) allow entities, usually humans, to trust each other in the cyberspace based on their prior interactions (logical) or knowledge from other entities. For instance, online marketplaces such as Amazon or eBay often use a reputation system, and new buyers are more likely to buy goods from merchants with a high rating (a metric for reputation).

However, reputation systems are vulnerable to many types of attacks. The Sybil-attack, first described by Douceur[15], is an attack where an entity can assume multiple identities or Sybils, and then attack either another entity or undermine the whole reputation system (we discuss it in more details in section 3). In the marketplace example, the merchant could create multiple fake accounts and submitting a lot of positive feedback to the real account to boost the rating. It is one of the most important attacks because it leads to a large number of consequences including but not limited to spreading false information, ballot stuffing[6] and eclipse attacks[55]. Thus, preventing the Sybil-attack is likely to significantly increase the credibility of reputation systems.

Sybil-defence mechanisms come in various shapes and sizes. Some rely on a trusted third party (subsection 4.1), some introduce a cost in identity creation (subsection 4.2), some exploit the graph characteristics (subsection 4.4)

and so on. To the best our knowledge, there does not exist a recent and comprehensive survey that focuses on the Sybil-attack in reputation systems.

To this end, we survey the defence mechanisms proposed by various reputation systems to eliminate or minimise Sybil-attacks as well as general approaches that do not depend on any specific reputation systems. Note that Sybil-attacks do not only exist in reputation systems. Wireless sensor networks and more generally MANETs (mobile ad hoc networks) for example are also vulnerable, the attacker can cripple the routing algorithm or defeat distributed storage mechanisms[42]. Thus defence mechanisms that do not apply to reputation systems are outside the scope of this work and are not covered. On the other hand, since reputation systems are often also peer-to-peer systems, we do cover the more general defence mechanisms.

Our main contributions are the following.

1. TODO
2. TODO

2 Reputation Systems

Reputation systems are of interest in many scientific domains. In evolutionary biology, scientists study indirect reciprocity[43]. In experimental economics

First the definitions

- Truster
- Trustee
- Recommender
- Recommendation

One of the first systems - Beth 94[5] PGP (Zimmermann) 95[76] Use of direct and also indirect trust

3 The Sybil-Attack

Explain the sybil-attack

Important theoretical results: Sybil-proof[8] - symmetric reputation functions cannot provide Sybil-proofness, must use asymmetric reputation functions.

a test bed for sybil attacks[24]

Quantifying Sybil attack[36]

4 Defences

In this section we categorise various defence techniques against the sybil-attack in reputation systems.

4.1 Trusted Third Party

One of the earliest and best known reputation system is eBay[46]. The buyers and sellers rely on a trusted third party, in this case eBay, to gather and distribute feedbacks after every transaction. Even when there are no incentives to provide feedback, Resnick and Zeckhauser observed that feedback was provided more than half of the time[46], making eBay one of the most well-known online marketplaces.

In general, trusted third parties manage the issurance and verification of identities. Thus they can apply a fee on the peer for creating a new identity[45] or rate-limit the creation of new identities[15], making sybil-attacks more difficult. Furthermore, trusted third parties often have the ability to manipulate the identities. For example they could punish the attackers by disabling all of their identity when caught, making the sybil-attack much riskier especially when identities are costly.

Trusted third party is likely the most widely used technique in practice. Marketplaces such as Amazon or eBay, online forums such as Stackoverflow or Reddit, all use a form of trusted third party.

Unfortunately, a trusted third party is often a single point of failure. Moreover, being a centralised system, it is difficult to scale up to suit increasing user demands. In the remainder of this section, we focus on distributed techniques for preventing the sybil-attack.

Credence 06[65] - uses central authority to sign key

4.2 Costly Identity Creation

4.2.1 IP Address

4.2.2 Low reputation for new users

Feldman 04[16] - adaptive stranger, low score on entry

4.3 Indirect Information

EigenTrust[28] - doesn't prevent sybils, suggests to add cost in ID creation R2Trust[60] - credibility, tackles colluders, time decay factor

4.4 Graph Techniques

Theory[52] Gal-Oz et al. [17] communities are collection of knots, sybils can form a knot? Regret[47, 48] - information from multiple dimensions Guha 04[18] - no mention of sybil attacks or attacks in general

4.4.1 Flow Based

BarterCast[39] SybilRes[12]

4.4.2 Topology

SybilGuard[72] SybilLimit[71] SybilInfer[11] SybilShield[53] - assuming sybils have bad connectedness SumUp[61] GateKeeper[62] - based on SumUp Social-network[63] - community detection

Distributed Sparse Cut Monitoring[31]

Other systems are built on top: ReDS[2] suggests to use sybilimit or sybilinfer SybilProof-DHT[33]

4.5 Reputation Transfer

Trust-transfer[50]

4.6 Self Registration

P-GRID 01[1] Self-registration[14] - distributed registration based on IP address

4.7 Cryptography Based Techniques?

Secure-Overlay[35] - ID crypto and SSS Privacy-preserving[49] - blockchain? Proof-of-stake[13] SybilConf[58]

4.8 Content Driven

[7]

4.9 Other

Parental control[59] - uses parents to "observe" find suspects, only for detection, requires a sybil-proof reputation scheme DSybil[70] - recommendation system, need historical data Symon[27] - pair peers together, likelihood for both to be sybils is low, the pair monitor each other to prevent attacks XRep 02[10] IP check, and checks digest, uses existing P2P systems like Gnutella

4.10 Unsorted?

Beth and PGP limits Sybil attack to some extent by using social graphs Beth 94[5] PGP (Zimmermann) 95[76]

Yu 00[69] Lee 03[32] - uses flooding, might not be scalable, only talks about DoS Marti 04[38] ARA 05[21] - no mention of sybil, prevents freeriding, prevents short-term abuse because reputation increases gradually FuzzyTrust Song 05[56] - uses fuzzy logic P2PRep/Fuzzy 06[4] - also fuzzy, does not prevent generation of false rumors Xiong 05[67] - no mention of sybil, but tries to mitigate false information PowerTrust 06[75] - uses "power nodes" (from power-law), no mention of sybil, some defence against colluders

Histos and Sopras[73], doesn't really have structure? Beta[25] Gupta et al.[20]

PeerTrust[66] - DHT, used P-GRID source code, has credibility rating

PerContRep[68]

4.11 Does not handle Sybil-attack?

TrustMe[54] is a reputation that focuses on anonymity, no mention of sybil attack

H-Trust[74] does not mention sybil

Coner et al.[9] assumes clients cannot perform sybil attack

TrustGuard 05[57] - assumes it is built on secure overlay networks (sybil-proof networks)

Scrivener 05[41] - assumes ID cannot be created and discarded

5 Related Work

Reputation Surveys: [37] [26] ? [23] [30] [51] ? [22]

Sybil Surveys: [34] [40] [44] [19] [29] Sok[3] but also some contribution

Other: [64]

6 Summary

References

[1] Karl Aberer. "P-Grid: A self-organizing access structure for P2P information systems". In: *International Conference on Cooperative Information Systems*. Springer. 2001, pp. 179–194.

[2] Ruj Akavipat et al. "ReDS: A framework for reputation-enhanced DHTs". In: *IEEE Transactions on Parallel and Distributed Systems* 25.2 (2014), pp. 321–331.

[3] Lorenzo Alvisi et al. "Sok: The evolution of sybil defense via social networks". In: *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE. 2013, pp. 382–396.

[4] Roberto Aringhieri et al. "Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems". In: *Journal of the American Society for Information Science and Technology* 57.4 (2006), pp. 528–537.

[5] Thomas Beth, Malte Borcherding, and Birgit Klein. "Valuation of trust in open networks". In: *European Symposium on Research in Computer Security*. Springer. 1994, pp. 1–18.

[6] Rajat Bhattacharjee and Ashish Goel. "Avoiding ballot stuffing in ebay-like reputation systems". In: *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*. ACM. 2005, pp. 133–137.

[7] Krishnendu Chatterjee, Luca de Alfaro, and Ian Pye. "Robust content-driven reputation". In: *Proceedings of the 1st ACM workshop on Workshop on AISec*. ACM. 2008, pp. 33–42.

[8] Alice Cheng and Eric Friedman. "Sybilproof reputation mechanisms". In: *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*. ACM. 2005, pp. 128–132.

[9] William Conner et al. "A trust management framework for service-oriented environments". In: *Proceedings of the 18th international conference on World wide web*. ACM. 2009, pp. 891–900.

[10] Ernesto Damiani et al. "A reputation-based approach for choosing reliable resources in peer-to-peer networks". In: *Proceedings of the 9th ACM conference on Computer and communications security*. ACM. 2002, pp. 207–216.

[11] George Danezis and Prateek Mittal. "SybilInfer: Detecting Sybil Nodes using Social Networks." In: *NDSS*. San Diego, CA. 2009.

[12] Rahim Delaviz et al. "SybilRes: A sybil-resilient flow-based decentralized reputation mechanism". In: *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*. IEEE. 2012, pp. 203–213.

[13] Richard Dennis and Gareth Owenson. "Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain". In: (2016).

[14] Jochen Dinger and Hannes Hartenstein. "Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration". In: *First International Conference on Availability, Reliability and Security (ARES'06)*. IEEE. 2006, 8–pp.

[15] John R Douceur. "The sybil attack". In: *International Workshop on Peer-to-Peer Systems*. Springer. 2002, pp. 251–260.

[16] Michal Feldman et al. "Robust incentive techniques for peer-to-peer networks". In: *Proceedings of the 5th ACM conference on Electronic commerce*. ACM. 2004, pp. 102–111.

[17] Nurit Gal-Oz, Ehud Gudes, and Danny Hendler. "A robust and knot-aware trust-based reputation model". In: *IFIP International Conference on Trust Management*. Springer. 2008, pp. 167–182.

[18] Ramanthan Guha et al. "Propagation of trust and distrust". In: *Proceedings of the 13th international conference on World Wide Web*. ACM. 2004, pp. 403–412.

[19] Rupesh Gunturu. "Survey of Sybil attacks in social networks". In: *arXiv preprint arXiv:1504.05522* (2015).

[20] Minaxi Gupta, Paul Judge, and Mostafa Ammar. "A reputation system for peer-to-peer networks". In: *Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video*. ACM. 2003, pp. 144–152.

[21] MyungJoo Ham and Gul Agha. "ARA: A robust audit to prevent free-riding in P2P networks". In: *Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05)*. IEEE. 2005, pp. 125–132.

[22] Ferry Hendrikx, Kris Bubendorfer, and Ryan Chard. "Reputation systems: A survey and taxonomy". In: *Journal of Parallel and Distributed Computing* 75 (2015), pp. 184–197.

[23] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. "A survey of attack and defense techniques for reputation systems". In: *ACM Computing Surveys (CSUR)* 42.1 (2009), p. 1.

[24] Athirai Aravazhi Irissappane, Siwei Jiang, and Jie Zhang. "Towards a comprehensive testbed to evaluate the robustness of reputation systems against unfair rating attack." In: *UMAP Workshops*. Vol. 12. 2012.

[25] Audun Jøsang and Roslan Ismail. "The beta reputation system". In: *Proceedings of the 15th bled electronic commerce conference*. Vol. 5. 2002, pp. 2502–2511.

[26] Audun Jøsang, Roslan Ismail, and Colin Boyd. "A survey of trust and reputation systems for online service provision". In: *Decision support systems* 43.2 (2007), pp. 618–644.

[27] BS Jyothi and Janakiram Dharanipragada. "Symon: Defending large structured p2p systems against sybil attack". In: *2009 IEEE Ninth International Conference on Peer-to-Peer Computing*. IEEE. 2009, pp. 21–30.

[28] Sepandar D Kamvar, Mario T Schlosser, and Hector Garcia-Molina. "The eigentrust algorithm for reputation management in p2p networks". In: *Proceedings of the 12th international conference on World Wide Web*. ACM. 2003, pp. 640–651.

[29] David Koll et al. “On the state of OSN-based Sybil defenses”. In: *Networking Conference, 2014 IFIP*. IEEE. 2014, pp. 1–9.

[30] Eleni Koutrouli and Aphrodite Tsalgatidou. “Taxonomy of attacks and defense mechanisms in P2P reputation systems-Lessons for reputation system designers”. In: *Computer Science Review* 6.2 (2012), pp. 47–70.

[31] Aditya Kurve and George Kesidis. “Sybil detection via distributed sparse cut monitoring”. In: *2011 IEEE International Conference on Communications (ICC)*. IEEE. 2011, pp. 1–6.

[32] Seungjoon Lee, Rob Sherwood, and Bobby Bhattacharjee. “Cooperative peer groups in NICE”. In: *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. Vol. 2. IEEE. 2003, pp. 1272–1282.

[33] Chris Lesniewski-Lass and M Frans Kaashoek. “Whanau: A sybil-proof distributed hash table”. In: NSDI. 2010.

[34] Brian Neil Levine, Clay Shields, and N Boris Margolin. “A survey of solutions to the sybil attack”. In: *University of Massachusetts Amherst, Amherst, MA* 7 (2006).

[35] Eng Keong Lua. “Securing peer-to-peer overlay networks from sybil attack”. In: *Communications and Information Technologies, 2007. ISCIT’07. International Symposium on*. IEEE. 2007, pp. 1213–1218.

[36] N Boris Margolin and Brian Neil Levine. “Quantifying resistance to the sybil attack”. In: *International Conference on Financial Cryptography and Data Security*. Springer. 2008, pp. 1–15.

[37] Sergio Marti and Hector Garcia-Molina. “Taxonomy of trust: Categorizing P2P reputation systems”. In: *Computer Networks* 50.4 (2006), pp. 472–484.

[38] Sergio Marti and Hector Garcia-Molina. “Limited reputation sharing in P2P systems”. In: *Proceedings of the 5th ACM conference on Electronic commerce*. ACM. 2004, pp. 91–101.

[39] Michel Meulpolder et al. “Bartercast: A practical approach to prevent lazy freeriding in p2p networks”. In: *Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on*. IEEE. 2009, pp. 1–8.

[40] Aziz Mohaisen and Joongheon Kim. "The Sybil attacks and defenses: a survey". In: *arXiv preprint arXiv:1312.6349* (2013).

[41] Animesh Nandi et al. "Scrivener: Providing incentives in cooperative content distribution systems". In: *Proceedings of the ACM/IFIP/USENIX 2005 International Conference on Middleware*. Springer-Verlag New York, Inc. 2005, pp. 270–291.

[42] James Newsome et al. "The sybil attack in sensor networks: analysis & defenses". In: *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM. 2004, pp. 259–268.

[43] Martin A Nowak and Karl Sigmund. "Evolution of indirect reciprocity". In: *Nature* 437.7063 (2005), pp. 1291–1298.

[44] GV Rakesh et al. "A Survey of techniques to defend against Sybil attacks in Social Networks". In: *International Journal of Advanced Research in Computer and Communication Engineering* 3.5 (2014).

[45] Paul Resnick et al. "The social cost of cheap pseudonyms". In: *Journal of Economics & Management Strategy* 10.2 (2001), pp. 173–199.

[46] Paul Resnick and Richard Zeckhauser. "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system". In: *The Economics of the Internet and E-commerce* 11.2 (2002), pp. 23–25.

[47] Jordi Sabater and Carles Sierra. "REGRET: reputation in gregarious societies". In: *Proceedings of the fifth international conference on Autonomous agents*. ACM. 2001, pp. 194–195.

[48] Jordi Sabater and Carles Sierra. "Social regret, a reputation model based on social relations". In: *ACM SIGecom Exchanges* 3.1 (2002), pp. 44–56.

[49] Alexander Schaub et al. "A trustless privacy-preserving reputation system". In: *IFIP International Information Security and Privacy Conference*. Springer. 2016, pp. 398–411.

[50] Jean-Marc Seigneur, Alan Gray, and Christian Damsgaard Jensen. "Trust transfer: Encouraging self-recommendations without sybil attack". In: *International Conference on Trust Management*. Springer. 2005, pp. 321–337.

[51] Chithra Selvaraj and Sheila Anand. "A survey on security issues of reputation management systems for peer-to-peer networks". In: *Computer Science Review* 6.4 (2012), pp. 145–160.

[52] Sven Seuken and David C Parkes. "On the Sybil-proofness of accounting mechanisms". In: (2011).

[53] Lu Shi et al. "Sybilshield: An agent-aided social network-based sybil defense among multiple communities". In: *INFOCOM, 2013 Proceedings IEEE*. IEEE. 2013, pp. 1034–1042.

[54] Aameek Singh and Ling Liu. "TrustMe: anonymous management of trust relationships in decentralized P2P systems". In: *Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on*. IEEE. 2003, pp. 142–149.

[55] Atul Singh et al. "Eclipse attacks on overlay networks: Threats and defenses". In: *In IEEE INFOCOM*. Citeseer. 2006.

[56] Shanshan Song et al. "Trusted P2P transactions with fuzzy reputation aggregation". In: *IEEE Internet computing* 9.6 (2005), pp. 24–34.

[57] Mudhakar Srivatsa, Li Xiong, and Ling Liu. "TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks". In: *Proceedings of the 14th international conference on World Wide Web*. ACM. 2005, pp. 422–431.

[58] Florian Tegeler and Xiaoming Fu. "SybilConf: computational puzzles for confining sybil attacks". In: *INFOCOM IEEE Conference on Computer Communications Workshops, 2010*. IEEE. 2010, pp. 1–2.

[59] Ankush Tehale et al. "Parental Control algorithm for Sybil detection in distributed P2P networks". In: *International Journal of Scientific and Research Publications* 2.5 (2012).

[60] Chunqi Tian and Baijian Yang. "H^2 Trust, a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks". In: *Future Generation Computer Systems* 27.8 (2011), pp. 1135–1141.

[61] Dinh Nguyen Tran et al. "Sybil-Resilient Online Content Voting." In: *NSDI*. Vol. 9. 1. 2009, pp. 15–28.

[62] Nguyen Tran et al. "Optimal sybil-resilient node admission control". In: *INFOCOM, 2011 Proceedings IEEE*. IEEE. 2011, pp. 3218–3226.

[63] Bimal Viswanath et al. “An analysis of social network-based sybil defenses”. In: *ACM SIGCOMM Computer Communication Review* 40.4 (2010), pp. 363–374.

[64] Dan S Wallach. “A survey of peer-to-peer security issues”. In: *Software Security-Theories and Systems*. Springer, 2003, pp. 42–57.

[65] Kevin Walsh and Emin Gün Sirer. “Experience with an object reputation system for peer-to-peer filesharing”. In: *USENIX NSDI*. Vol. 6. 2006.

[66] Li Xiong and Ling Liu. “Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities”. In: *IEEE transactions on Knowledge and Data Engineering* 16.7 (2004), pp. 843–857.

[67] Li Xiong, Ling Liu, and Mustaque Ahamad. “Countering feedback sparsity and manipulation in reputation systems”. In: *Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007. International Conference on*. IEEE. 2007, pp. 203–212.

[68] Zheng Yan, Yu Chen, and Yue Shen. “PerContRep: a practical reputation system for pervasive content services”. In: *The Journal of Supercomputing* 70.3 (2014), pp. 1051–1074.

[69] Bin Yu and Munindar P Singh. “A social mechanism of reputation management in electronic communities”. In: *International Workshop on Cooperative Information Agents*. Springer. 2000, pp. 154–165.

[70] Haifeng Yu et al. “Dsybil: Optimal sybil-resistance for recommendation systems”. In: *2009 30th IEEE Symposium on Security and Privacy*. IEEE. 2009, pp. 283–298.

[71] Haifeng Yu et al. “Sybillimit: A near-optimal social network defense against sybil attacks”. In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE. 2008, pp. 3–17.

[72] Haifeng Yu et al. “Sybilguard: defending against sybil attacks via social networks”. In: *ACM SIGCOMM Computer Communication Review*. Vol. 36. 4. ACM. 2006, pp. 267–278.

[73] Giorgos Zacharia, Alexandros Moukas, and Pattie Maes. “Collaborative reputation mechanisms for electronic marketplaces”. In: *Decision Support Systems* 29.4 (2000), pp. 371–388.

[74] Huanyu Zhao and Xiaolin Li. "H-trust: A group trust management system for peer-to-peer desktop grid". In: *Journal of Computer Science and Technology* 24.5 (2009), pp. 833–843.

[75] Runfang Zhou and Kai Hwang. "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing". In: *IEEE Transactions on parallel and distributed systems* 18.4 (2007), pp. 460–473.

[76] Philip R Zimmermann. *The official PGP user's guide*. MIT press, 1995.