Literature Survey:
The Sybil-Attack in Reputation Systems

October 12, 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, causing new buyers to have a higher likelihood to buy goods from merchants with a high rating (a metric for reputation) because a lot of other buyers left a positive feedback.

However, reputation systems are vulnerable to many types of attacks. The Sybil-attack, first described by Douceur[6], 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[1] and eclipse attacks[18]. 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 4.3)

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 for example are also vulnerable, the attacker can cripple the routing algorithm or defeat distributed storage mechanisms[11]. 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[12]. In experimental economics

First the definitions

- Truster
- Trustee
- Recommender
- Recommendation

3 The Sybil-Attack

Explain the sybil-attack

4 Defences

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

4.1 Trusted Third Party

TrustMe[17] eBay[13]

4.2 Costly Identity Creation

4.2.1 IP Address

4.2.2 Low reputation for new users

4.3 Graph Techniques

BarterCast[10] EigenTrust[7] Social network[19] SybilGuard[21] SybilLimit[20] Theory[16]

4.4 Reputation Transfer

Trust transfer[15]

4.5 Blockchain Based Techniques?

Privacy-preserving[14] Proof-of-stake[4]

4.6 Unsorted?

SybilInfer[3] Sybil-proof[2] Self-registration[5] Secure-Overlay[9] SybilProof-DHT[8]

5 Summary

References

[1] 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.

[2] 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.

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

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

[5] 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.

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

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

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

[15] 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.

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

[17] 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.

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

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

[20] 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.

[21] 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.