Literature Survey:
The Sybil-Attack in Reputation Systems

October 12, 2016

Abstract

1 Introduction

Reputation systems (described in section 2) allow entites, 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 Aamazon or eBay often use a reputation system, causing new buyers to have a higher likelihood to buy goods from merchents 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[2], 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 merchent 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[5]. Thus, preventing the sybil-attack is likely to significantly increase the credibility of reputaiton 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 4.3), 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.

In this work, 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 system. 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[3]. However, wireless sensor networks do not usually involve reputation systems, thus it is not covered.

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[4]. 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

4.2 Reputation Transfer

4.3 Costly Identity Creation

4.3.1 IP Address

4.3.2 Low reputation for new users

4.4 Graph Techniques

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

[3] 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.

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

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