

Chapter 3.11

Detecting Shill Bidding in Online English Auctions

Jarrold Trevathan

James Cook University, Australia

Wayne Read

James Cook University, Australia

ABSTRACT

Shill bidding is where spurious bids are introduced into an auction to drive up the final price for the seller, thereby defrauding legitimate bidders. While shilling is recognized as a problem, presently there is little or no established means of defense against shills. This chapter presents an algorithm to detect the presence of shill bidding in online auctions. It observes bidding patterns over a series of auctions, providing each bidder a score indicating the likelihood of his/her potential involvement in shill behavior. The algorithm has been tested on data obtained from a series of realistic simulated auctions, and commercial online auctions. The algorithm is able to prune the search space required to detect which bidders are likely to be shills. This has significant practical and legal implications for commercial online auctions where shilling is considered a major threat. This chapter presents a framework for a feasible solution, which acts as a detection mechanism and a deterrent.

INTRODUCTION

Shill bidding is the act of introducing fake bids into an auction on behalf of the seller to artificially inflate the price of an item. The seller either can: 1) register as a bidder under a false identity, or 2) be in collusion with one or more of the bidders.

Bidders who engage in shilling are referred to as *shills*. To win the item on auction a legitimate bidder must outbid a shill's price. If one of the shills accidentally wins, then the item is re-sold in a subsequent auction. Shill bidding is a problem as it forces legitimate bidders to bid against false bids hence paying significantly more for the item.

The most common type of auction is the English auction. In an English auction a seller offers an

DOI: 10.4018/978-1-61350-323-2.ch3.11

item for sale and many bidders attempt to outbid each other to obtain the item. The winner is the bidder with the highest bid after a given time-out period. English auctions are particularly susceptible to shill bidding practices.

The advent of online auctions such as eBay and ubid, have made shill bidding much more exploitable. This is because it is relatively simple for a seller to register under many aliases and operate in rings with impunity. Furthermore, as bidders are not physically present it becomes much easier for a shill to anonymously influence the bidding process. This chapter examines shill behavior in the online setting and presents an algorithm to detect the presence of shill bidders in English auctions. The algorithm examines bidding information across several auctions and produces a score indicating the likelihood that a bidder is engaging in shill behavior.

The algorithm is applied to real auction data where shills are present. We believe this is the first formal (documented) attempt to detect shills using a conformatory analysis of bidding behavior.

This chapter shows that the algorithm can effectively reduce the search space required to detect shills. This enables the implementation of exploratory analysis using data mining techniques.

RELATED WORK

This section explores some related work that has been conducted into shilling. At present there is limited coverage on how to detect shill bidding.

eBay has been involved in many legal disputes where bidders/sellers have been accused of shilling (see Schwartz and Dobrzynski (2002)). eBay has clear rules regarding shill bidding behavior in their auctions. Their policy clearly outlines undesirable bidder behavior and the penalties for shill bidding. The regular process for a bidder who suspects that they have been shilled is to contact eBay, who then investigates the incident. eBay does not state exactly what factors they use to

determine whether shilling has occurred, nor how to detect which bidders are shills.

Shah et al (2003) use data mining techniques to produce evidence of shilling. Their work used data from approximately 12,000 commercial auctions looking for associations between bidders and sellers. Bidders (or groups of bidders) that participated frequently in auctions held by particular sellers were deemed suspect. However, the authors' state that their analysis is very limited in that it only looks for simple associations. They suggest that a much more thorough analysis must be performed using complex associations which consider a wider range of shill behavior.

There are also companies who offer data mining techniques to detect fraud in online auctions. However, like eBay, these companies have not made their techniques public.

Wang et al (2002) discuss an approach that attempts to deter shilling in the first place. The Auctioneer is allowed to use fees to make shilling unprofitable for the seller. In auctions using a reserve price, a seller is charged an increasing fee based on how far the winning price is from the reserve price.

Aspects regarding the economic theory of shilling have been examined by Kauffman and Wood (2003), and Barbaro and Bracht (2005).

ONLINE ENGLISH AUCTIONS

This section describes the operation of online English auctions, which is the auction model used in this paper. Formally an English auction can be defined as an ascending-price, open-bid auction. Each bid submitted must be higher than the current highest bid. The minimal amount required to outbid others is usually a percentage of the current highest bid. The value of the current highest bid is available to all parties, along with the auction timing. The winner is the bidder with the highest bid when the auction terminates.

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/detecting-shill-bidding-online-english/60972

Related Content

Daubechies Wavelets Based Robust Audio Fingerprinting for Content-Based Audio Retrieval

Wei Sun, Zhe-Ming Lu, Fa-Xin Yu and Rong-Jun Shen (2012). *International Journal of Digital Crime and Forensics* (pp. 49-69).

www.irma-international.org/article/daubechies-wavelets-based-robust-audio/68409

Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases

Young B. Choi (2021). *International Journal of Cyber Research and Education* (pp. 58-64).

www.irma-international.org/article/organizational-cyber-data-breach-analysis-of-facebook-equifax-and-uber-cases/269728

A Socio-Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness

Nikolaos Serketzis, Vasilios Katos, Christos Ilioudis, Dimitrios Baltatzis and George J. Pangalos (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice* (pp. 173-184).

www.irma-international.org/chapter/a-socio-technical-perspective-on-threat-intelligence-informed-digital-forensic-readiness/252688

Analysis of a Training Package for Law Enforcement to Conduct Open Source Research

Joseph Williams and Georgina Humphries (2019). *International Journal of Cyber Research and Education* (pp. 13-26).

www.irma-international.org/article/analysis-of-a-training-package-for-law-enforcement-to-conduct-open-source-research/218894

iPhone Forensics: Recovering Investigative Evidence using Chip-off Method

Nilay R. Mistry, Binoj Koshy, Mohindersinh Dahiya, Chirag Chaudhary, Harshal Patel, Dhaval Parekh, Jaidip Kotak, Komal Nayani and Priyanka Badva (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice* (pp. 308-324).

www.irma-international.org/chapter/iphone-forensics/252695