Click Fraud Detection In Mobile Ads Served In Programmatic Exchanges

Anup Badhe

Abstract: Programmatic inventory auction or Real Time Bidding is the latest buzz in the mobile advertisement industry. This concept refers to a real time auction held for mobile advertisement spots and bidders bidding for that spot to show their advertisement. For a programmatic exchange that conducts these auctions detecting advertisements that auto click becomes very important since click fraud can quickly degrade the quality of supply for the exchange. Click fraud robs advertisers of their connection to unique users / potential customers they might acquire. Click fraud nowadays is achieved with scripts to make it more legitimate and convincing.

Index Terms: Auto clicking ads, RTB, Programmatic auctions, Programmatic exchange, mobile click fraud, headless browser

1 Introduction

Click fraud or auto clicking ads is a bane to the advertising industry, which annually results in a loss of $11 billion to marketers and advertisers. Initially click fraud was driven manually with human intervention but with the advances in technology nowadays this is achieved using bot code that automatically simulates clicks thereby giving false conversions to advertisers. Estimates vary but today close to 40% publisher traffic is bot activity. Between three and 31 percent of programmatically bought ad impressions were found to be from bots. Even "premium" programmatic campaigns on private advertising exchanges aren't safe, with around 10 percent of ad impressions coming from bots. These staggering rates cause serious damage to publishers and advertisers alike. For advertisers who work tirelessly to increase their exposure and attract new users, it's money down the drain. Mobile ads were previously excluded from this due to limited support for scripts on mobile phones, but with the release of smartphones and support for enhanced scripts this problem has also crossed over in the mobile domain. The solutions that exist today rely mostly on post click data that includes demographics and previously recorded activity to analyze user patterns or similarities to then draw conclusions on fraudulent activity. These solutions also make the assumption that the demographic data for a user does not change. In the mobile world demographic data is constantly changing due to changing networks and Wi-Fi hotspots.

2 Proposed system for click fraud detection

The proposed system consists of a server side solution that scans the ads before passing them over to the end mobile device. The RTB protocol enforces a strict exchange mechanism between exchanges and bidders in form of structured XML. The exchange anyways parses this XML to extract the ad payload to massage it before sending it to the requesting device. In this system an extra layer is added on the backend to pass the ad payload through a headless browser and check for auto redirection via JavaScript or HTML headers. The headless browser is based on the industry standard web-kit engine so that it renders the ad payload the same way a mobile device would.

- *Anup Badhe is currently the Director of Engineering at OperaMediaworks Inc, USA, PH-510-331-3710.*
- *E-mail: anupbadhe@gmail.com*

The fraud detection logic then checks to see that after the payload is loaded, there is no auto redirection to another domain that is different from the initial domain from where all the ad assets were requested. This approach will eliminate 90% of click frauds since fraudsters might employ more advanced methods than simple redirection via JavaScript or headers. The solution would also cache domains from where click fraud was detected in a blacklist that can be used for potential blocking of such ads.

3 Problems with the solution

Scalability of the solution is the main problem since any exchange handles billions of ads everyday. The other problem that might be encountered is support for MRAID. Many rich media ads request the support for an MRAID layer to perform complex transitions / animations. Since MRAID is purely for in-app containers, a standard web-kit based headless browser does not have the support for it. Taking a random sampling of ads that are passed to the scanner system might solve the scalability issue. Also the random sampling would also help in reducing the number of trackers fired when the ad payload is rendered to make sure that the exchange does not get branded for impression fraud. The MRAID problem requires implementation of the MRAID specification using the browser available functions to support MRAID functionality.

4 Conclusion

This solution incentivizes an exchange to crack down on fraudulent traffic and clean up it's inventory in turn driving the enhancing the brand of the exchange for "quality of traffic". Also advertisers will be able to getter higher ROI for every dollar they spend on the exchange without them having to run to other exchanges in search of clean traffic.

Acknowledgment

The author wishes to thank Prajakta Badhe for her continuous encouragement and support.

References

[1] http://techbeacon.com/how-avoid-click-fraud-todays-mobile-ad-economy.

[2] http://adexchanger.com/mobile/mobile-fraud-its-time-to-start-paying-attention/

[3] https://en.wikipedia.org/wiki/Click_fraud