Rewarded tasks for reducing ad fraud

Tuna Toksoz

John Dukellis

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
Toksoz, Tuna and Dukellis, John, "Rewarded tasks for reducing ad fraud", Technical Disclosure Commons, (December 03, 2018) https://www.tdcommons.org/dpubs_series/1744

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
Rewarded tasks for reducing ad fraud

ABSTRACT

Ad fraud occurs when unscrupulous web or app publishers generate clicks, ad-impressions, or other events using bots that emulate human visitors to the web-page, app, or ads within. Ad fraud improperly diverts significant amounts of revenue to such publishers. Ad networks have long grappled with controlling or eliminating ad fraud.

This disclosure uses rewarded ads to issue challenges to willing users so as to discriminate between bots and humans. Users that are determined to be bots are tracked, ads appearing on associated web-pages or apps discarded, and such publishers noted for further action. The techniques enable detection of fraud using an API-approach, e.g., inside the ad, such that the use of a software development kit (SDK) for collecting ad-spam signals is lessened.

KEYWORDS

Ad fraud, rewarded ads, captcha-ads, fraud detection, click fraud

BACKGROUND

Ad fraud occurs when unscrupulous web or app publishers generate clicks, conversions, ad-impressions, traffic, or other data events using bots that mimic human visitors to the web-page, app, or ads within. Ad fraud improperly diverts significant amounts of revenue to such publishers. Ad networks have long grappled with controlling or eliminating ad fraud.

DESCRIPTION

This disclosure uses rewarded ads to issue challenges to willing users so as to discriminate between bots and humans. Rewarded ads are an ad format that gives users the option to watch an ad in exchange for a reward, e.g., in-game or in-app points. Because the choice of watching the ad rests with the users, they don’t have to watch ads they’re not interested
in, and the ads they do see, e.g. video ads, are presented in full. Rewarded ads enable publishers to build ad monetization into the mechanics of their apps or games, and improve user engagement with both app and in-app ads.

![Diagram showing the process of rewarded ads to detect ad fraud]

**Fig. 1: Rewarded ads to detect ad fraud**

Fig. 1 illustrates the use of rewarded ads to detect ad fraud, per techniques of this disclosure. A rewarded ad is displayed to the user (102), and if the user accepts the ad, the user is presented with a bot-vs-human test. Such a test can be a task that would be difficult or impossible for a bot or emulator to do, e.g., rotate the mobile device; sum up two numbers; check a box that says “I’m not a robot”; choose from a list of images one that is described in text or audio; etc. The bot-vs-human test may be thought of as being similar to a captcha within an ad.

If the test passes (106), e.g., the user is confirmed as being human, the reward is granted, and the ad continues to be displayed (108). The process repeats.
If the test fails (106), then such non-complying users are marked as potential bots, and their apps or publishers / developers marked as potential bot-clients. The ad is discarded, and the reward associated with the ad is not granted. Such users and publishers, suspected to be bots or bot-clients, are tracked across apps to see if they are not able to comply in other apps. Action may be taken against such apps or web-pages and their publishers or developers if evidence mounts of their continued bot usage to commit fraud.

Different mechanisms are employed across different apps to assure that the requested task is appropriate for particular legitimate users to perform. The techniques of this disclosure apply to interstitial ads, native ads, banner ads, instream ads, etc. The techniques also allow background ads to be identified as such, since no action is performed on the ad because a user is generally unable perform the requested task on them.

Although rewarded ads are typically implemented using a software development kit (SDK) to collect ad-spam signals, the techniques of this disclosure enable fraud detection using an API-approach, e.g., inside the ad, which is an apposite approach for many markets.

**CONCLUSION**

This disclosure uses rewarded ads to issue challenges to willing users so as to discriminate between bots and humans. Users that are determined to be bots are tracked, ads appearing on associated web-pages or apps discarded, and such publishers noted for further action. The techniques enable detection of fraud using an API-approach, e.g., inside the ad, such that the use of a software development kit (SDK) for collecting ad-spam signals is lessened.