MEASURING AND FINGERPRINTING CLICK-SPAM IN AD NETWORKS

Vacha Dave *, Saikat Guha★ and Yin Zhang *
* The University of Texas at Austin
★ Microsoft Research India
Online advertising is a 31 billion dollar industry *

Publishers can monetize traffic
- Blogs, News sites, Syndicated search engines
- Revenue for content development

Pay-per-click advertising
- Advertisers pay per-click to ad networks
- Publishers make a 70% cut on each click on their site

*Based on Interactive Advertising Bureau Report, a consortium of Online Ad Networks
Click-spam in Ad Networks

- Click-spam
  - Microsoft, which offers pay-per-click ads through its adCenter service, says click laundering -- an offshoot of click fraud, which has plagued the industry for years -- is growing in scale and sophistication. "This is the newest form of criminal activity on the Internet," says Brad Smith, Microsoft's general counsel.

- Possible Motives
  - Malicious advertisers (or other parties)
    - Deplete competitor's ad budgets
    - Isolated cases
  - Publishers/Syndicated search engines
    - Make money on every click that happens on their site

- Fraudulent or invalid clicks
  - Users delivered to the advertiser site are uninterested
  - Advertisers lose money

- Having control of the landing page
  - Provide a better user experience
  - Increase ad engagement

- Fraudulent impressions
  - Advertisements that are not displayed
  - Decrease ad visibility

- Click laundering
  - Manipulating click data to inflate ad performance
  - Misleading advertisers about ad effectiveness

- Click stealing
  - Clicks that are recorded without the user's intent
  - Misappropriating ad revenue

- Click-stacking
  - Artificially increasing the number of clicks on an ad
  - Manipulating ad performance metrics

- Click-fraud
  - Exploiting vulnerabilities in the ad system
  - Financial loss for advertisers

- Non-fraudulent click manipulation
  - Malicious site optimization
  - Exploiting ad system features

- Ad networks:
  - Microsoft adCenter
  - Google AdWords

- Volume of clicks
  - Advertiser campaigns
  - User engagement

- Importance of accurate tracking
  - Ensuring ad performance is measured correctly
  - Preventing fraud and misappropriation of ad revenue
Mobile Devices and Ads

- Mobile game
- Squish the ant to win the game
- Ads placed close to where user is expected to click
Click-spam Detection

- No ground truth
  - Almost impossible to know if particular click is genuine
  - Need to guess the intent of user

- Different levels of click-spam in different segments
  - Aggregate numbers are meaningless

- Ad networks aren’t transparent
  - Security by obscurity

- Real problem – lot of work needed
  - Researchers lack real attack data
Contributions

- **First method to independently estimate click-spam**
  - As an advertiser
  - For specific keywords

- **Test across ten ad networks**
  - Search, contextual, social and mobile ad networks
  - Show that click-spam is a problem
    - For Mobile and Social ad networks

- **Discover five classes of sophisticated attacks**
  - Why simple heuristics don’t work

- **Release data for researchers**
Estimating click-spam – Approach

- Hard to classify any single click
  - Estimate fraction of click-spam

- Designed Bayesian estimation framework
  - Uses only advertiser-measurable quantities

- Cancel out unmeasurable quantities
  - By relating different mixes of good and bad traffic
Estimating Click-spam – Main Idea

Both non-spammers and spammers click ads

A fraction of non-spammers buy

Equate ratios of buyers to non-spammers

How many?

Both non-spammers and spammers click ads

Lose spammers and some non-spammers

Some non-spammers buy
Dissecting Black box – Hurdles

Spammers and non-spammers click on an ad

- Different hurdles have different hardness
  - 5 sec wait, Click to continue

- Send only a fraction of traffic through hurdles
  - To minimize impact on user experience

- Perfect hurdle would block all spam
  - In reality, some spammers get through (False Negatives)
Dissecting Black box - Bluff Ads[1]

- Bluff Ads
  - Junk ad text with normal keywords, same targeting
  - Normal users unlikely to click

[1] Fighting online click fraud using bluff ads [CCR 2010]
Dissecting Black box - Bluff Ads[1]

- **Bluff Ads**
  - Junk ad text with normal keywords, same targeting
  - Normal users unlikely to click

[1] Fighting online click fraud using bluff ads [CCR 2010]
Dissecting Black box - Bluff Ads[1]

- Maximum False Negative rate known for each hurdle
- Can be subtracted out

[1] Fighting online click fraud using bluff ads [CCR 2010]
Testing Ad Networks

- Sign up as *advertisers for ten ad networks*
  - Search, Contextual, Mobile and Social
  - Google, Bing, AdMob, InMobi, Facebook and others

- 240 Ads
  - Keywords: Celebrity, Yoga, Lawnmower
  - Hurdles: Click to continue, 5 sec wait

- 50,000 Clicks
  - 30,000 bluff ad clicks

- Cost: $1500
Uh-oh. How do we validate?

No ground truth!

Compare against search ads on Google and Bing
Results – Validation using search ads

Clicks charged are close to the estimated valid clicks
Results – Estimating Mobile Spam

Most mobile ad networks fail to fight click-spam

Ad Network’s Estimate

Our Estimate
All networks seem to be underestimating the amount of spam
Where is click-spam coming from?

- Analyze bluff ad clicks
  - Publishers: Strong motive
    - Instead of clicks/users
  - Manual Investigation

- Challenge: Scale
  - 3000+ publishers, 30,000 Clicks

- Identical sites!

- Cluster on cosine similarity
  - Feature vector
    - WHOIS, IP Address/Subnet, HTTP parameters
Publishers creating sybil nodes to beat ad network thresholds
Case Study 1 - Malware driven click fraud

- Jane searches for books
- Botmaster generates list of publishers
- Publisher List
- Publisher URL
- www.moo.com
- Auto-Redirect (Fraud)
- AD URL

Malware infected PC

Jane clicks on a search result

All background traffic – Jane sees nothing

(BOTID=50018&SEARCH-ENGINE-NAME&q=books) Base64
Case Study 1 - Malware driven Click fraud

- Responsible Malware: TDL4
  - Validation: Run malware in VM
- Can intercept and redirect all browser requests
  - Browser specific filtering doesn’t work
- Only 1 click per IP address per day
  - Threshold based filtering doesn’t work
- Mimics real user behavior
  - Timing analysis doesn’t work
ClickSpam and Arbitrage

- Polished forum sites
- Bluff ad clicks on ad network X
- No malware reports
- Not popular
  - Where do they get traffic?
- No ads on the site !!
Click-spam and Arbitrage

- Advertiser on network Y
  - Creates 4500+ ads
- Publisher on network X
- Page now has only ads
  - No questions or answers
- Confusing users into clicks
Click-spam and Arbitrage

- Tricking real users into clicking
- Bot detection techniques don’t apply

Site pays $ to Y

Site earns $$$$ from X
Case Study 3 - Click Fraud using Parked Domains

Jane mistypes `icicbank.com` in her browser and presses enter.

- Parked Domain
- Auto-Redirect
- Pull ads for “icicbank” from a Syndicated Search Engine
- Auto-Redirect (Fraud)
- AD URL

Jane ends up on `icicbank.com`
`icicbank.com` pays for a click.
Case Study 3 - Click Fraud using Parked Domains

- 41 of 400 parked domains hosted on a single IP
  - Misspellings of common websites:
    - icicbank.com, nsdi.com 😊
  - Auto-redirect depends on Jane’s geo-location
  - IP hosts 500,000 such domains

- User mistypes a URL
  - Advertiser must pay!

- User behavior indistinguishable from normal traffic
  - Naively using conversions don’t work
Case Study 4 – Mobile click-spam

- Indian Mobile ad network
  - Supplies WAP Ads to a group of WAP porn sites
  - Ad links indistinguishable from porn video links

- Gaming apps
  - Place ads close to where users are expected to click
  - Ant-Smasher, Milk-the-Cow, and 50 others
Only 26% percent of traffic investigated

Malware
Arbitrage
Parked
WAP
Sybil Nodes
Summary

- Click-spam remains a problem
- First way of estimating click-spam Independently
  - As an advertiser, for a set of keywords
  - Extensive validation
- Sophisticated click-spam attacks today
  - Sybil sites
  - Malware mimics user behavior
  - Social engineering attacks and others
- Dataset is available for download
  - All clicks (minimally sanitized)
Thanks!

Data at:

http://www.cs.utexas.edu/~vacha/sigcomm12-clickspam.tar.gz
Dwell Time for Mobile Ad Networks

The graph shows the cumulative distribution function (CDF) for dwell times across mobile ad networks labeled A, B, C, and D. The CDF is plotted against dwell time in seconds (0s, 2s, 4s, 6s, 8s, 10s), with the CDF values ranging from 0 to 1. The networks exhibit different dwell time distributions, with network A showing the highest CDF values across all dwell times compared to networks B, C, and D.
Dwell Time for Reputable Search Networks
Conversion Definitions

- Original
- Control
- Fraction gold-standard
- 5s dwell, 1 mouse ev
- 15s dwell, 5 mouse ev
- 30s dwell, 15 mouse ev
Advertiser’s Webserver Logs

Network layer attributes
IP: 208.94.146.81
IP Subnet: 208.94.146.0/24
Domain Owner: Domains By Proxy, LLC
Domain Registrar: GODADDY.COM, LLC
Registration Date: 07-sep-1999
Hosting provider: NTT America, Inc

Application layer attributes
URI: results.php
URL parameters: “uvx=“
Style sheet
Font

HTTP Referer Header identifies the publisher or syndicator: dotellall.com
Mechanics of a click:

Jane Searches For Books

Ad Impression

Jane Sees the Ad and Clicks it

Redirects Jane to Advertiser Site

Ad Click

[Truncated] Cookie: _FS=NU=1; _SS=SID=5007D45C58CB43A587D4709E89A283DE&C=20.0&CW=1230&CH=604&bIm=541869;
It’s acceptable to omit “www” in a website name.

Incredibly hard to detect spam traffic, because of similar domain names.
Estimating ClickSpam — Main Idea

Both Jon-does and spammers click Ads

Spammers and some Jon-does are turned away by hurdles

A fraction of Jon-does become gold standard

P(GS) = 🙈 / 😨

= 0.5

0.5 = 😨 / 🔟

X = 😨

P(V) = 😨

Both Jon-does and spammers click Ads

A fraction of Jon-does become gold standard