MEASURING AND FINGERPRINTING CLICK-SPAM IN AD NETWORKS

Vacha Dave *, Saikat Guha★ and Yin Zhang *
* The University of Texas at Austin
★ Microsoft Research India
Internet Advertising Today

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

- **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
Click-spam in Ad Networks

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.

How Click Laundering Works

In the Red Orbit case, Microsoft says it discovered the alleged scheme after detecting a growing number of suspicious clicks from Red Orbit's site over a two-week period starting in January 2009. The site had previously averaged 75 clicks a day, but the number spiked above 10,000 clicks per day, according to the complaint.

According to Microsoft, Red Orbit was able to manufacture large numbers of bogus clicks on shady sites known as parked domains—Web sites that are legal but exist only to display ads. In this case, many of the ads were invisible to the naked eye. Then, using a technical slight of hand, it submitted the clicks to Microsoft in a way that made them appear to have occurred on Red Orbit's own site, a requirement for getting paid.
Mobile Devices and Ads

Ant Smasher

- 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

Black box

How many 🙁 ?

Equate ratios of buyers to non-spammers

Celebrity Cruise
Be Recognized, Celebrated, And Indulged Aboard Celebrity Cruises

Celebrity Cruise
Be Recognized, Celebrated, And Indulged Aboard Celebrity Cruises

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

Spammers and curious users click on an ad

Some spammers and users may see the content

---

[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

Some spammers and curious users click on an ad

[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

Ad Network’s Estimate

- Our Estimate

Valid Traffic Fraction (Normalized)

<table>
<thead>
<tr>
<th>Ad Networks</th>
<th>celebrity</th>
<th>yoga</th>
<th>lawnmower</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Clicks charged are close to the estimated valid clicks
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

Valid Traffic Fraction (Normalized)

Ad Network’s Estimate

Our Estimate

A
B
C
D

Most mobile ad networks fail to fight click-spam
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

Publisher Website: Cosine Similarity:
Case Study 1 - Malware driven click fraud

Malware infected PC

Jane searches for books

Malware infected PC

Botmaster generates list of publishers

Publisher List

Publisher URL

Auto-Redirect (Fraud)

www.moo.com

AD URL

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

Site pays $ to Y

Site earns $$$$ from X
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.

icicbank.com

Parked Domain

Auto-Redirect

Pull ads for “icicbank” from a Syndicated Search Engine

Auto-Redirect (Fraud)

AD URL

Jane ends up on icicibank.com

icicibank.com pays for a click
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
Malware

Sybil Nodes
Arbitrage
Parked
Malware
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)
Data at:

http://www.cs.utexas.edu/~vacha/sigcomm12-clickspam.tar.gz