

MobiAd: Private and Scalable Mobile Advertising

Hamed Haddadi
Royal Veterinary College
University of London, UK

Pan Hui
Deutsche Telekom Labs
Berlin, Germany

Ian Brown
Oxford Internet Institute
University of Oxford, UK

ABSTRACT

We introduce MobiAd; a scalable, location-aware, personalised and private advertising system for mobile platforms. Advertising is the driving force behind many websites and service providers on the Internet. With the ever-increasing number of smart phones, there is a fertile market for personalised and localised advertising. The key benefit of using mobile phones is to take advantage of the vast amount of information on the phones and the locations of interest to the user in order to provide personalised ads. Preservation of user privacy is however essential for successful deployment of such a system. MobiAd would perform a range of data mining tasks in order to maintain an interest profile on the user's phone, and use the infrastructure network to download and display relevant ads and reports the clicks via a Delay Tolerant Networking (DTN) protocol. In this paper we provide an overview into existing advertising systems and privacy concerns on mobile phones, in addition to the scalable local ad download and privacy-aware DTN-based click report dissemination methods that we propose for MobiAd.

Categories and Subject Descriptors

J.4 [Computer Applications]: Social and Behavioral Sciences

General Terms

Human Factors, Design

Keywords

Advertising, Mobile Devices, DTN

1. INTRODUCTION

Advertising is the largest revenue source of many Internet giants. Targeted and personalised ads, provided by ad brokers such as Google and Microsoft, are displayed on designated ad slots on websites that in return receive payment

from the ad network. Google's advertising revenue in 2008 was over \$20 billion and this number is expected to increase [2].

The mobile phone advertising market is becoming increasingly significant. There are currently over 3 billion mobile phone subscribers in the world and surveys from Gartner and Telsyte group suggest that nearly a third of these are using smart phones, with the smart phone market increasing at a rate of nearly 50% last year. With modern smart phones having 3G and wireless connectivity, GPS localisation capability, a wide range of social networking applications and HTML browsing ability on large touch LCD displays, there is a fertile market for targeted and personalised advertising. Naturally, handset manufacturers have recently launched a series of advertising platforms which leverage the users' choice of websites, activities, music and social activities to present them with targeted ads.

There are a large number of technical, legal and user-related obstacles to overcome on the path to a successful mobile advertising strategy. Individuals are much more *attached* to their mobiles than to their laptops and personal computers. Hence the use of sensitive, personal information kept on the phones can raise privacy concerns. Successful and accurate profiling and personalisation of ads will depend strongly on ad networks assuaging consumers' privacy concerns over targeted ads. Mobile phones in general have also less bandwidth, processing power and screen size when compared to ordinary computers. Hence the ads must be smaller, downloaded less frequently and have low processing requirements. The profiling tasks must also require limited computation and storage access in order to preserve battery life.

In this paper we present MobiAd, a first proposal for personalised, localised and targeted advertising on smart phones. Utilising the rich set of information available on the phone, MobiAd presents the user with local ads in a privacy preserving manner. The ads are selected by the phone from the pool of ads which are broadcast on the local mobile base station or received from local WiFi hotspots. In this manner, the user only needs to download ads which are relevant to his interests, and are for items and services in his locality. The information about the ad views and clicks are then encrypted and sent to the ad channel via other mobile phones and intermittent WiFi hotspots, in a delay tolerant manner. In this system, other nodes and the network operator can not find out what ads were viewed. Likewise, the ad provider cannot determine which users viewed which ads and only receives aggregate information. MobiAd al-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MobiArch'10, September 24, 2010, Chicago, Illinois, USA.
Copyright 2010 ACM 978-1-4503-0143-5/10/09 ...\$10.00.

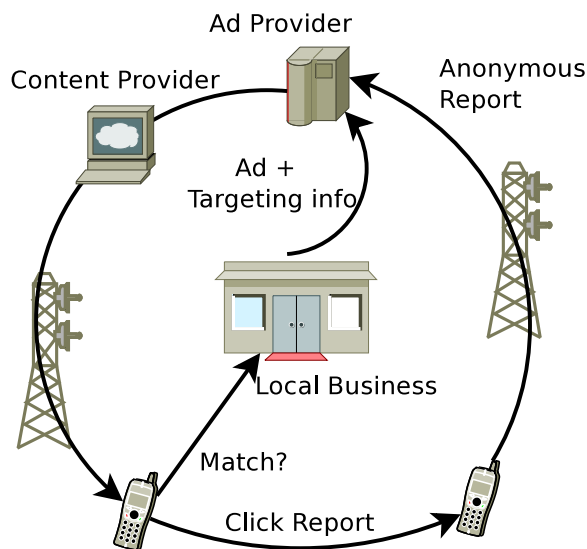


Figure 1: Targeted localized advertising.

lows businesses, local and global, to target users narrowly and directly, without compromising users' privacy. It also improves the scalability of advert distribution by using a local broadcast frequency with geo-targeted adverts.

The rest of this paper is organised as following. In Section 2 we present the overall MobiAd system architecture. Section 3 presents some techniques and tools for user profiling. We discuss ad dissemination and report collection in Section 4. We then discuss privacy concerns and issues in Section 5. We discuss the limited related work in Section 6 and discuss future work and avenues for further research in Section 7.

2. OVERALL ARCHITECTURE

In this section we present an overview of the MobiAd system architecture. Figure 1 presents the an example of some of the components of the MobiAd advertising system. The main components of the system are:

- *Advertisers*: The ad providers aim to reach a specific groups of users based on requirements such as sex, age, interests and location. They provide the ad texts, targeting information, bidding budgets and potentially a landing page for the clicks¹.
- *Network Operator*: The network operator provides the infrastructure for disseminating the ads, collecting reports and locating users. In return they receive a share of revenues.
- *Content Provider*: Content providers, such as news sites and blogs, provide online services and materials which are of interest to users. Alongside their main content, they provide ad boxes where personalised ads could be displayed to the user. Social networking sites such as Facebook are a particular type of publisher,

¹We elaborate in Section 5 why a landing page is not essential

with access to more detailed profile information on their users.

- *Ad Provider*: The ad providers are the interface between the advertisers, operator and content providers. They gather ads from advertisers, provide ads for the users in the publisher websites, collect view and click reports, bill the advertisers and compensate the publishers and the network operator.
- *Profiling Agent*: The agent gathers relevant information for profiling the user. It also downloads and filters relevant ads, displays them to the user at appropriate and convenient times and prepares click and view reports for billing purposes.

Advertisers such as local businesses wish to sell their products or services through ads. Content providers (e.g., news and review websites, personal weblogs, mobile phone applications) provide opportunities to view ads, for instance by providing space for ad banners. Clients are the users of the handset. Ad providers (e.g., Google or Microsoft) bring together advertisers, publishers, and clients. They provide ads to users, gather statistics about what ads were shown on which publisher pages, collect money from the advertisers, and pay the publishers. In traditional advertising systems, the advertisers specify their ads and bids (how much the advertiser is willing to pay for views and clicks of the ads) to the ad providers. When a publisher provides banner space to the client on a web page, a request goes to the ad provider asking to fill in the banner space with appropriate ads. The ad provider makes the decision as to which ads to place based on a number of criteria such as the keywords for the web page, personalisation information about the client (usually based on persistent cookies on the client machine), the keywords of the ad, and the bid associated with the ad. It then delivers the ad to the client, informs the advertiser of the ad view and clicks, and charges the advertisers and compensates the content providers accordingly.

By using detailed profiling and data mining technics in addition to the user location, MobiAd provides new opportunities for localised and personalised advertising. In terms of privacy protections, some of these components are also similar to traditional advertising systems (such as Google's AdWords program) or newly proposed privacy-aware systems such as Adnostic [17] and Privad [9]. However the key difference here is the fact that mobility and use of local ad distribution and Delay Tolerant Networks (DTN) [7] provide a simple and scalable ad distribution and privacy preserving click report mechanism, while providing numerous challenges for profiling and ad placement on a mobile device with limited screen size and battery life. The network operator also plays a more central role as it needs to broadcast adverts in a localised manner and collect and forward reports. The lower bandwidth, battery life and display size of mobile phones prevent us from downloading, sorting and showing a large number of ads on the user's phone. Hence in MobiAd we focus on a lower number of ads to be displayed but with higher targeting and a focus on local ads that would particularly benefit from the user's location information.

In the next sections we expand on the key individual components, their roles and operation strategies.

3. PROFILING AND INCENTIVES

The most important objective of MobiAd is to serve relevant and interesting ads to the user. Since the mobile phone's battery life and display size and general usage time is less than the average personal computer, it is crucial to use the ad display opportunities effectively. In order to do this, users' interests and profiles should be maintained on user handsets, while allowing the user to configure and delete their interest categories. This is also in compliance with requirements and recommendations of most regulatory organisations and privacy advocates.

3.1 Maintaining the user profile

There are rich sources of information on a typical smartphone, from email and browsing activities to social networking and shopping sites. This information is in essence an aggregation of information from the user's web history, browser cache and keyword extractions from activities on social networks and email. Users are likely to have different privacy sensitivities regarding these data sources, and should be allowed to control which are included in profiling activity. Browsing behaviour can be used to update profiles at lower processing cost using server-side pre-categorisation of URIs into interest segments [17].

The profile and the associated software work in cooperation in a similar manner to Gmail or persistent cookies from search engines and ad providers. However in MobiAd the profile does not leave the user's handset and the software platform picks up the appropriate ads from the broadcast channel.

The user profile must solely be kept securely on the handset. The profile must be visible to the user but unobtainable by other applications. The isolation of information between different applications is readily available on popular smart phones. Profiling tasks can be done while the phone is idle. The extent and depth of categorisation is dependant on the different regions and users, e.g., Google keeps 700 categories in a 3-level hierarchy, but Amazon has over 65k categories. We envisage that a MobiAd client can maintain an extensive database of interests, locations, mobility patterns and daily habits. Such detailed information would enable the relevant ads to be easily filtered and directed to the user. In next section we discuss the privacy mechanism of MobiAd.

3.2 User Incentives

MobiAd system is without a doubt beneficial to advertisers and network operators, but why would users install such an application? Users have an incentive to install and utilise most applications if there is a marginal entertainment or financial benefit for them. iPod touch users download an average of 12 apps a month and spend 100 minutes a day using apps. Android and iPhone users download a similar number of apps every month and spend a similar amount of time using the apps [3]. On a new iPhone app, users have been reported to be searching daily for money saving vouchers and local promotions.² Hence the intention is that useful services would encourage the users to download the client which could also act as a privacy information centre on their phone.

For the MobiAd system, we are considering looking at a range of advertisement benefits to the user, location-based

and independent. Location-based benefits could include offers and coupons for local businesses and retailers. Independent long-term benefits could include informative applications, such as suggesting events and activities which could be off interest to the user and are not necessarily advertised. In addition, network operators may pre-install this type of software on handsets, or offer incentives to users (such as discounted monthly fees) for them to use MobiAd. In this way the costs of carrying other user reports can also be compensated by the *availability* of a user's handset for carrying traffic and hence contributing to the anonymisation process. Another incentive could be a small percentage cut payment from the ad click revenue for the report carriers, in an aggregate manner, in order to avoid the network operator or the advertiser to be able to trace the origin of the clicks.

4. DISSEMINATION AND REPORTING

4.1 Ad Dissemination

Ad dissemination in a mobile environment is different from the desktop environment. In MobiAd, the focus is on local ads that are relevant to the user. Location information can be obtained using GPS position or network provider information from the handset. Users roam in and out of mobile cells on a regular basis. It has also been shown that there are limits to predictability of location of users at given times [14]. We therefore do not rely heavily on prefetching all the relevant ads to the user, apart from at locations such as home and work where they appear frequently.

The optimal data dissemination strategy should avoid constant data download, but be ready for unpredictable arrival of the user into new areas. The MobiAd agent on-handset should be able to classify locations that are frequently visited (using a list of GPS positions most frequently visited), such as the route from home to work, weekend hotspots and such like. The ads for these locations could be prefetched when there is wireless connectivity and stored for longer periods, in order to minimise the data transfer costs and battery utilisation on the handset.

When a user enters a new location where the ads are not already prefetched, it can receive all local ads using technologies such as Multimedia Broadcast and Multicast Services (MBMS) [4]. MBMS is a new service offered on GSM and UMTS networks and uses multicast distribution in the core network which enables an interaction between the handset and the network which can be used for distributing ads and collection of reports. MBMS enables network operators to distribute all the local ad texts simultaneously to all cell phone users within each transmitter's coverage area using a single shared transmission broadcast. As the cell coverage is expected to be in order of few hundreds of meters, the text ads within each cell should not exceed a few kilobytes (a few hundred local ads, each having around 100 characters of text) which is a reasonable amount of data transfer for all modern smart phones to deal with. If one channel is used at each cell tower to broadcast locally-relevant ads, all phones could listen to all channels and just select relevant ads without revealing which ads are of interest and shown to the user. If more privacy is required, we could add protocols such as SlyFi [8] which would provide anonymous sniffing capabilities for downloading ads from local WiFi hotspots. However since all the local ads can be downloaded from WiFi hotspots, the hotspot service provider is not able to classify

²<http://www.pocket-lint.com/news/34077/deals-moneysupermarket-launches-iphone-app>

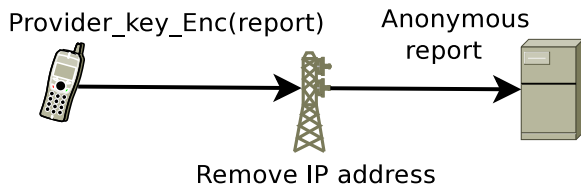


Figure 2: Encrypting click reports.

the users, as they cannot find out which ads were displayed. The number of broadcast ads even in busy metropolitan areas could be limited by a combination of network operator and ad provider using an auction mechanism to limit the number of location-targeted ads through raising their price. Hence we opted for local flooding for the current design.

It is also possible for the ad network to suggest a short-list of relevant adverts within specific advert frames, resulting from centrally-available context and pricing information [17]. One may also consider using Tor³ for ad dissemination or report collection, however Tor requires a real-time interactive channel that consumes significant amounts of power. MobiAd’s ad-report transmission does not need a real-time interactive anonymous channel. By relaxing this requirement, we can reduce power use.

4.2 Billing

At the end of each billing cycle, advertisers are billed by the advertising network for advert displays and click-throughs. MobiAd uses a cryptographic protocol developed by Toubiana et al. that allows clients to notify the network of advert impressions without leaking user interest information [17].

Figure 2 provides an overview of the Public Key encryption stages of the click reports. The ad report will be encrypted using the ad provider’s public key, so only the ad provider can open the report. Ad clicks will then be anonymised, as the ad provider can identify the ad clicked on, but does not know who clicked on the ad. Likewise, the network operator knows a report was received, but does not know what ad was clicked on. MobiAd also uses a one time pseudorandom number in order to avoid replay clicks. This is similar to the reporting mechanism used in Privad [9]. We avoid using more sophisticated methods such as Tor due to the complexity of running such CPU and data intensive systems on mobile phones.

4.3 Report collection using DTN

As advertisers are generally billed using information on cost-per-impression or cost-per-click, there needs to be a return path for clients to report this data (without leaking information on user interests). To further protect users against attempts to link reports to user behaviour, we are taking a similar approach to onion routing [6] using the DTN paradigm.

DTN was originally designed for interplanetary communication, where the delay is up to a few minutes [5], and then it was adapted to solve intermittent connectivity prob-

lems in daily life. Furthermore, recently it has been shown that by leveraging the delay of wireless transmission, DTN can improve the anonymity of wireless communication from physical localisation (e.g. triangulation) [12]. Onion routing is an approach to achieve anonymous communication by routing the message through several intermediate relays before reaching the destination, hence the probability of revealing the source node of the message is significantly reduced. As shown in Figure 3, the MobiAd agent system is designed to report on ad views and clicks, while preserving the privacy and anonymity of users.

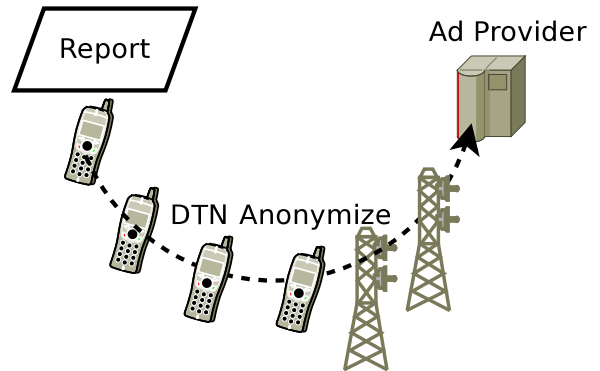


Figure 3: Collecting reports via DTN.

In MobiAd, we use DTN to route ad reports to several intermediate relays before they are finally passed to the cellular network. DTN relies on mobile peer-to-peer store-and-forward (using WiFi or Bluetooth connections) and hence there is no additional monetary cost on top of the cellular network cost. Here for further privacy consideration we have three requirements: 1) the relays should have certain social in-correlation with the social network, which prevents identity reverse engineering from the social relationship, 2) if possible, the final location of the final hop to the cellular network should have certain geographical distance from the original location of the report, 3) we want a certain delay (but not too long for billing purpose) between the time when the report is first sent out from the source and the time when it is finally sent to the network.

For a better guarantee of successful delivery, we use two-copies forwarding instead of a single copy [15] for the report, which means that the source will make a duplicate copy of the report and send them separately to two different immediate relays. The report will not be further duplicated during the multiple-hop transmission. To achieve the social in-correlation criteria, we are taking an anti-social network approach as opposite to the social-based approach introduced in BUBBLE Rap forwarding [11], where a mobile device will periodically scan the environment and detect the devices belonging to its social community. But here we intend to choose random people, including friends and strangers, as relays instead of socially close nodes. In this way the social network of a node can not be easily identified by an attacker which monitors all the forwarded packets in a cell network where a node is frequently present.

In order to preserve the location and temporal privacy, we will set the number of hops before the last hop to the cellular network to be 3 (so in total 4-hops). Based on the seminal work on 6-degree of separation by Milgram et al. [13], 4-

³<http://www.torproject.org/>

hops should be a reasonable distance in order to scramble the social correction, and long enough for the message to have enough temporal delay and geographical distance from the source. There may be energy consumption issues due to excessive wireless scans for efficient DTN routing, but since delay is not a main concern for the delivery of the ad reports, we do not need to scan the environment so frequently.

While taking all these measures into consideration, it is theoretically possible for an advertiser or the network operator, through long term monitoring of the mobile user, to determine which ad reports have a geographical correlation with the user's location. This is due to the user's routes following a specific home-work-home pattern for most of the days. In order to overcome this, MobiAd can employ a system where base stations follow a similar approach to the DTN system proposed before forwarding the reports for, for example reports from a specific region or town could be forwarded all over the country, or they could be presented to the ad provider in aggregate form. In this way the ad provider cannot build an accurate estimate of number of phones and their geographic correlation in specific regions. We are currently working towards categories of attack scenarios by the advertisers, ad provider, network operator and content provider and plan to address these issues in future work.

5. SECURITY AND PRIVACY

MobiAd enhances user privacy by keeping the user profile used to target adverts on the handset and minimising the user data exposed to advertisers or ad providers. The client pre-fetches adverts using the inherently anonymous broadcast channel [16] being developed for GSM and 3GPP, reporting client impressions and possibly clicks using a cryptographically-protected report and Delay-Tolerant Network to minimise the possibility of this data being linked back to individuals.

The profile is an aggregate view of user interests rather than a detailed history, reducing the risk of information leakage. It excludes information about "sensitive" matters such as medical interests, trade union membership and religious beliefs. This builds user trust in the system, reduces the potential for this information to be accessed for unauthorised purposes, and enables easier compliance with data protection laws such as the European Union's Data Protection Directive [1].

An open question is whether users that click on adverts should be taken directly to an advertiser URI; redirected to an advertiser site via an intermediate URI hosted by the ad provider for click-through measurement and fraud protection, as commonly happens in today's advertising networks; or to content also distributed using an anonymous channel, to further limit the potential for linking users to specific interests. In general usage the click-through rate for adverts is extremely low, so sending users directly to advertiser sites is much less privacy-intrusive than building detailed server-side user profiles. Users may anyway voluntarily provide further information to advertisers at this point, particularly if they make a purchase. However, particularly privacy-sensitive users may make use of a service such as Tor to reduce linkage of their browsing behaviour to any long-term identifier (such as an IP address). Care needs to be taken to reduce the ability of malicious advertisers to gain information on users who click-through an advert that

is targeted at extremely small numbers of individuals – both in terms of interests and in frequently-visited locations such as homes and work places.

Careful attention also needs to be paid to client-side implementation details to prevent information leakage. Adverts need to be carefully isolated within display pages using mechanisms such as identically-sized iframes, to prevent client-mediated communications between publisher and advertiser. This may preclude the inclusion of active content such as Flash ads [17].

Mobile handsets are less frequently shared than PCs, and hence information is less likely to leak between users of the same equipment. However, care must be taken to protect profiles using a PIN or password from access by other people with physical access to a handset. The possibility of coerced access – such as by parents to their children's handset profile – must also be considered, which is a further reason for storing only aggregate information and excluding sensitive personal data categories.

An issue outside the scope of MobiAd is user reaction to highly-targeted adverts, even with guarantees that behavioural profiles remain entirely private to the individuals they describe. Advertisers may need to tread carefully in targeting adverts for products such as low-fat foods that to some users may raise concerns that they have been unfairly categorised, or suggest lifestyle problems. A possible mechanism to address the first concern would be transparency in explaining to users why they had been shown any given advert. Many countries also have laws that ban discriminatory treatment of individuals based on certain characteristics that might be inferred from behavioural profiles. For sensitive ads we envisage that no reports need to be collected in order to minimise any privacy leaks. Even the landing pages of such ads could be provided using a Content Distribution Network (CDN), or they can be pre-fetched using the DTN system. We are dealing with the privacy issues in more detail for future work.

MobiAd could also use Bluff Ads [10] in order to reduce the level of targeting of ads by displaying random ads from the pool of ads without actually using targeting information. Inclusion of Bluff Ads reports could also make it more difficult for the ad provider to profile individual users, even in the absence of any identifying information.

6. RELATED WORK

Despite a fertile market for advertising, there are not many dedicated ad networks for mobile phones. There are a few services for serving ads on mobile websites. For example, AdMob is a service which provides ads for more than 15,000 mobile Web sites and applications around the world. AdMob stores and analyses the data from every ad request, impression, and click and uses this to optimise ad matching in its network [3]. However the methods used are in no way privacy-aware or localised. This limits the scalability of the system as ads have to be served individually at the time of browsing. This is not an issue in general for desktops, but on a mobile phone numerous HTTP connections could slow down the browsing experience.

Adnostic [17] and Privad [9] are also newly proposed private advertising systems for ordinary browsers. They work on the basis of downloading all the relevant ads offline and showing them at appropriate times. The core ideas of these systems is similar to MobiAd from a privacy perspective.

However operation in a mobile environment brings a range of challenges on dissemination of ads, capturing reports and scalability. We have attempted to address these issues by using a range of solutions such as DTN for report collection and 3G broadcast channel for ad dissemination. MobiAd is also resistant to collusion between advertisers and network operators, as the DTN anonymisation strategy would prevent the origin of the clicks being easily traced.

Recently, Apple and Microsoft have also entered the mobile advertising market. Apple have launched the *iAd* service⁴, on which they will perform a range of standard targeting options on the iAd Network include demographics, application preferences, music and movies choice and location. All these information will be kept by Apple and will be used to target ads to relevant customers. Microsoft also envisage a similar service on the Windows mobile platform. Having such detailed profile information at a content provider or handset provider's disposal is a clear threat to users' privacy.

7. FUTURE DIRECTIONS

In this paper we presented the MobiAd system architecture, a system for personalised, localised and private yet scalable mobile advertisement. In this system, ads are locally broadcast to users within mobile cells, appropriate ads are shown to the user and view and click reports are collected using a DTN system, preserving the privacy and anonymity of the user. MobiAd provides opportunity for using the vast amount of information on users' smart phones for targeted advertising while protecting privacy.

We are at early stages of defining the protocol for MobiAd. We are working on building a prototype for Apple iPhone, Google Android and Microsoft Windows mobile platforms in order to carry on a pilot study. We are aware that there are a great number of research questions on user privacy, scalability, user incentives, user profiling and information security. In future work we aim to present an extensive analysis of these challenges and deploy prototype solutions. We believe that mobile advertising is an important market for revenue generation and systems such as MobiAd are a step towards providing an advertising system which allows great targeting potential without jeopardising user privacy.

Acknowledgment

We wish to acknowledge Tristan Henderson, Joss Wright and anonymous reviewers for constructive feedback on the security and privacy strategies.

8. REFERENCES

- [1] Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281 pp.31-50, Nov 1995.
- [2] Google investor relations, financial tables, http://investor.google.com/fin_data.html, 2008.
- [3] Admob mobile metrics report, <http://metrics.admob.com/wp-content/uploads/2010/02/AdMob-Mobile-Metrics-Jan-10.pdf>, 2010.
- [4] Multimedia broadcast/multicast service (mbms); stage 1, 3gpp specification detail <http://www.3gpp.org/ftp/Specs/html-info/22146.htm>, 2010.
- [5] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss. Delay-tolerant networking: an approach to interplanetary internet. *IEEE Communications Magazine*, 41(6):128–136, 2003.
- [6] R. Dingleline, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *In Proceedings of the 13th USENIX Security Symposium*, pages 303–320, 2004.
- [7] K. Fall. A delay-tolerant network architecture for challenged internets. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 27–34, New York, NY, USA, 2003. ACM.
- [8] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services*, pages 40–53, New York, NY, USA, 2008. ACM.
- [9] S. Guha, A. Reznichenko, K. Tang, H. Haddadi, and P. Francis. Serving ads from localhost for performance, privacy, and profit. In *Eighth ACM Workshop on Hot Topics in Networks (HotNets-VIII)*, New York City, NY, 2009.
- [10] H. Haddadi. Fighting online click-fraud using bluff ads. *ACM Computer Communication Review*, 40(2), 2010.
- [11] P. Hui, J. Crowcroft, and E. Yoneki. Bubble rap: Social-based forwarding in delay tolerant networks. In *MobiHoc '08: Proceedings of the 9th ACM international symposium on Mobile ad hoc networking & computing*, May 2008.
- [12] X. Lu, P. Hui, D. Towsley, J. Pu, and Z. Xiong. Anti-localization anonymous routing for delay tolerant networks. *To Appear in Elsevier Computer Network*, 2010.
- [13] S. Milgram. The small world problem. *Psychology Today*, (2):60–67, 1967.
- [14] C. Song, Z. Qu, N. Blumm, and A.-L. Barabasi. Limits of predictability in human mobility. *Science*, 327(5968):1018–1021, 2010.
- [15] T. Spyropoulos, S. Member, K. Psounis, and C. Raghavendra. Single-copy routing in intermittently connected mobile networks. In *In Proceedings of IEEE SECON*, 2004.
- [16] F. Stajano and R. J. Anderson. The cocaine auction protocol: On the power of anonymous broadcast. In *Information Hiding*, pages 434–447, 1999.
- [17] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas. Adnostic: Privacy preserving targeted advertising. In *NDSS 2010*, San Diego, California, USA.

⁴<http://advertising.apple.com/>