Three Applications for Mobile Epidemic Algorithms

Paul Tennent, Malcolm Hall, Barry Brown, Matthew Chalmers, Scott Sherwood

Department of Computing Science
University of Glasgow
17 Lilybank Gardens
Glasgow, UK, G12 8QQ
+44 (0) 141 586 7192

{pt, mh, barry, matthew, sherwood} @dcs.gla.ac.uk

ABSTRACT

This paper presents a framework for the pervasive sharing of data using wireless networks. 'FarCry' uses the mobility of users to carry files between separated networks. Through a mix of ad-hoc and infrastructure based wireless networking, files are transferred between users without their direct involvement. As users move to different locations, those files are then transmitted on to other users in the new location. We examine three applications utilising this framework that depend upon this sharing. Each of these exploits the physically proximate nature of social gatherings. As people group together (such as in business meetings or cafés) this can be taken as an indication of similar interest (e.g. groups interested in the same presentation or type of music). MediaNet allows users to share media files between strangers or friends, MeetingNet shares business documents in meetings and NewsNet shares RSS feeds between mobile users. NewsNet also develops the use of pre-emptive caching – collecting information from others not for oneself, but for the predicted later sharing with others. We draw observations developing this system in a mobile, multi-user, multi-device environment.

Categories and Subject Descriptors

H.5.3 [**Group and Organization Interfaces**]: Collaborative Computing

General Terms

Design, Human Factors.

Keywords

Wireless, ad-hoc networking, file sharing, peer-to-peer networks, sociable sharing, proximity-based sharing.

1. INTRODUCTION

Designing mobile systems presents distinct challenges when compared to stationary technologies, as well as offering new opportunities. A topic of recent interest has been the use of mobile networks as a way of distributing information between mobile and stationary users. One of the earliest systems of this type was Pollen [11], a system that used mobile individuals as data carriers, exchanging information as they moved around.

In these models the mobility of users allows data to be physically carried and then exchanged on an opportunistic basis. More broadly, epidemic algorithms support the spreading of information opportunistically between proximate hosts. These algorithms have shown their utility for the dissemination of information in non-mobile contexts, such as synchronising information between distributed databases [4].

In terms of applications, however, it is unfortunate that the most successful application of these algorithms has been computer viruses. In this paper we explore more beneficial applications of epidemic algorithms in a mobile context. While previous work has focused on technical questions, we introduce three user-focused applications that use mobile epidemic algorithms to support sharing data between mobile users. Each of these applications makes use of 'FarCry' - a framework which uses serendipitous self-configuring 802.11 networks to spread information. Currently running on PDAs and laptops FarCry automatically exchanges data between devices as they become physically proximate. Our applications use this framework to provide to users the ability to share data and files as needed. The mechanism can be controlled by users so as to decide what data to share, or to only share files from other users on request.

2. RELATED WORK

There has been considerable discussion in the literature on the dissemination of data over mobile peer-to-peer networks, yet most discussion has remained at the level of technical or system descriptions, or alternatively simulations of data propagation. Su et al. [12] discuss opportunistic Bluetooth ad-hoc networking modeling the distribution of messages across mobile distant networks. [7] and [8] present efficient algorithms for data distribution over mobile ad-hoc networks using, respectively, tornado coding and epidemic algorithms. Hayes and Wilson examined an application of the Gnutella protocol in a mobile ad-hoc environment [6].

In terms of applications, Beaufour et al. propose a system of data dissemination between fixed sensor networks based on Bluetooth enabled smart tags [2]. Their application area involved visitors to a national park spreading information between fixed environmental sensors. Esbjörnsson et al.'s Hocman [5] demonstrates how URLs and user profiles can be exchanged using serendipitous ad-hoc networking between motorcyclists. However, neither of these applications are strictly epidemic, since information would only be passed between pairs of nodes, rather than supporting an epidemic model of carriers spreading information between multiple nodes.

While not mobile, the work of Sandler et al. [10] is of interest, advocating the use of peer-to-peer based systems to reduce the

bandwidth overhead created by RSS feeds. RSS feeds work on a 'retrieve and store' model for accessing web content using a peer-to-peer algorithm here has some similarities with the mobile context (in particular, our third application described below).

3. TECHNICAL OVERVIEW

FarCry is a C# assembly, a library of code that can be easily by used by other .NET applications on mobile devices, PCs or Smartphones. While it currently works over wi-fi its functionality is simple enough to be used over any TCP/IP network, such as a network connection set up over Bluetooth. As an important distinction from previous systems, FarCry is able to work alongside user's existing wireless network use. It operates both on infrastructure networks, such as a user's own wireless network, or will create its own network if necessary.

FarCry allows applications to select files to be shared, specifying which files can be received from other FarCry enabled devices, as well as providing an interface for dealing with the user-initiated spreading of files between devices.

When running, FarCry spawns a background task that searches for other FarCry peers. If the device is currently on a wireless network, a search is made for other peers using a lightweight service discovery mechanism similar to Apple's *Bonjour* protocol, but more robust to changes at the physical network layer. All FarCry clients broadcast their existence over UDP to the subnet, allowing listeners to become aware of them.

If no infrastructure networks are available, or the client is unable to obtain a connection, FarCry will create an ad-hoc network to which other clients can connect. This ad-hoc network has a fixed SSID of which all FarCry clients are aware. FarCry listens for this ad-hoc network even while connected to infrastructure networks, changing to the ad-hoc network if necessary. When FarCry uses its own ad-hoc network, IP addresses for devices are obtained using the same approach as ZeroConf (www.zeroconf.org). This is an advancement over previous systems, where normally it is assumed that a network connection is already configured.

When FarCry devices discover and are connected at the session level, a file exchange system is set up using a simple personal web server running on both devices. Devices automatically connect to each other's web server, download a list of all available files from other peers, and transfer files (subject to an application defined filter). Files that are stored on both devices have their timestamps compared, with the newest file propagated. FarCry also supports an interactive mode where users are notified that a peer is nearby and an interface provided for users to browse other's devices and select files for download. FarCry keeps a record of transferred files, so does not re-transfer files that have been previously transferred. As a protection against viruses, the FarCry assembly will only exchange documents or media, and will not exchange program code.

In epidemic algorithm terms FarCry works on a device-by-device and file-by-file basis. Devices are 'susceptible' when they have not seen a particular file. When devices have files they become 'infectious', in that they can spread that file to other devices. Lastly, when a user or application deletes a file the device is 'removed' or immune – it can no longer be infected with that file.

4. APPLICATIONS

We have used the FarCry framework to develop three applications using mobile epidemic algorithms. Each of these applications exploit the ways in which users mobility coincides with their likely interests. That is to say that collections of people often share similar interests – or at the very least are likely to share interests more than the general population.

4.1 MediaNet

In Brown et al.'s exploration of music sharing [3], which examined the difference between peer-to-peer file sharing networks like napster, and the traditional 'mix tape' method of music sharing, we see how the former lacks the sociable aspects of the latter. More recently, Voida et al. have examined the use of iTunes file sharing [13] showing a return these traditional values, through the removal of anonymisation. We propose to further intimate this process by developing a proximity-based media sharing application.

MediaNet is a media sharing system, designed to disseminate media files across a network of friends. Although controversial, media sharing is a popular persuit - some estimates put the amount of Internet traffic taken up by media sharing as high as 60% [14].

The FarCry framework depends on location, and thus facilitates sharing amongst people who meet regularly, generally, friends, colleagues, and 'familiar strangers' [9]. MediaNet allows users to view, stream or download available files from any present peers - excluding those protected by digital rights management. Media can be automatically swapped – supporting the unobtrusive sharing of media between friends. This exploits the fact that social groupings often share tastes in music, film etc, allowing individuals to browse new acquisitions at leisure. An alternative mode allows users to be alerted when other users come into view, and to browse users' files while still connected.

Figure 1. PDA Screenshots of MediaNet. Notifying the user that another user is nearby (left). Browsing and downloading files from another user's device (right).

Since these exchanges are triggered simply by network range, files are exchanged not only between friends but between strangers who are physically proximate. This allows a cross-pollination between distinct social groups. Groups who go to the same social settings (such as the same bar) would exchange files more often than those who do not. The nature of MediaNet might

also allow the transfer of files between two individuals who do not know each other, but with similar tastes through a third party with connections to both.

MediaNet allows streaming as well as direct downloading, meaning those using devices with lower storage capacities, such as flash based PDAs can also be supported. This part of the application is particularly suited to commuter-style environments, where users maintain proximity with strangers for long periods of time. MediaNet stores a history of streamed files, allowing the user to browse this later, locating and downloading them from the Internet when more time or storage is available.

4.2 MeetingNet

As an application, MediaNet is primarily concerned with entertainment, but the FarCry framework is not restricted to this area. Our second example applies FarCry to use in a workplace environment. MeetingNet coordinates a network connection between all the wi-fi enabled devices present at a meeting. Within the meeting a folder on users' machines is dynamically set up and all files in that folder shared between participants. Users can then distribute electronic files to all attendees, such as to pass PowerPoint files around. Attendees simply place the files into the folder (either in advance) or during the meeting, and files will be exchanged between all the participants.

Technically, this system is very similar to MediaNet, differing only in details of its interface. One added complication over MediaNet comes from the private nature of the files likely to be exchanged. In our current application MeetingNet is only practical for use with non-confidential files. Since files are automatically shared, it is possible that those who are within the vicinity but not actually at the meeting can share files. A planned extension to this system involves the use of a passcode to initiate sharing amongst meeting participants. In this extension a code would be entered by the participant who would all have to enter the same code to share the files.

The second area of functionality provided is that of instant messaging. It can be useful to interact silently with one's peers at a meeting (so called 'backchannel' communication), however colleagues may not all be subscribers to the 'buddy' system used by most instant messenger systems. Again, the geographical boundaries of FarCry's local networking are turned to positive use, by restricting the messaging system to those within range of the network, and running the MeetingNet Application - in practice; those present at the meeting. Of course, both these features can be replicated using other tools, if a suitable network is set up, however the automation of FarCry aims to make this process painless.

4.3 NewsNet

NewsNet combines FarCry with the use of a recent popular technology: RSS. Unlike MediaNet and MeetingNet, NewsNet depends on the user having had a connection to the Internet. It examines a user's bookmarks for those based on RSS feeds, then creates time-stamped caches of those pages. When the user meets or passes another NewsNet user, FarCry coordinates a network connection, and each device compares its list of feeds with that of the other. If any match is found then the older page is updated with the additional articles from the newer.

In this manner, a user is able to receive news updates without actually connecting to the Internet. Like MediaNet, NewsNet exploits social groupings, depending on the premise that friends share similar interests, thus have a better chance of matching feeds than complete strangers. In this way NewsNet allows users who are outside Internet range to be updated with new feeds from others passing by who have recently accessed the Internet.

NewsNet has also been designed to predict which feeds other users may request and cache these, even if the current user has no interest in them. This is a form of 'pre-emptive caching' of news for other users. The decision of which feeds to cache is based on a ranking system. If two devices A and B discover each other over the network, device A sends requests for all the news feeds it requires, a list of requested feeds is built up on device B, with a count of requests attached to each. These counts are then used to select the top ten most-requested feeds, which are then updated whenever an Internet connection is available. This simple technique proves to be very efficient as it, like MediaNet, utilises social networking to mediate the ranking system - the rankings are stored locally on client devices, and requests are made every time two devices discover, meaning that devices which regularly discover will increase the rankings of each others' requested pages. The high ranked feeds will thus vary with social interaction; for example, a group of technologists is likely to have several technology sites in their rankings, while a group of musicians may have more musically relevant sites stored.

If a user wishes, they may browse the news feeds available on another device visible over a FarCry network. As with the practice of iTunes-sharing based 'musical voyeurism' [13], NewsNet allows a 'news voyeurism', a sort of electronic equivalent of reading over someone's shoulder. In certain situations, such as commuter environments, this may prove an enlightening diversion, while its use among friends may lead to the same kinds of judgements described in [13].

Of the three systems described, NewsNet is the one most likely to benefit from the serendipitous meeting of strangers. While specialist news-feeds are likely to be confined to those with similar interests, those of more general interest, such as local news, may have more universal appeal. Additionally the size of the files used by NewsNet are likely to be considerably smaller than those of MediaNet, so downloading content from passing strangers is more plausible.

5. DISCUSSION

As mentioned above, FarCry applications exploit the geographical proximity of users to support file sharing. Of course, the clustering between location and interest is a very weak one – every day we walk past many people who we have little in common with. However, as Boden puts it, despite our use of Internet technologies, we still have a 'compulsion of proximity' [1]. In aggregate, physical proximity can correspond with much clustering of interest. Our social spaces are often inhabited by similar others, not only friends or familiar strangers [9], but those who work in the same organization as us or live in the same area.

In our experiments with FarCry files can be reliably exchanged at a distance of around 100 meters. This may be too far to effectively support the sort of social situations that FarCry is designed for. Certainly for MeetingNet the wifi network extends far outside one meeting room to econompass adjacent rooms. We

are therefore currently experimenting with lowering the power of the wireless network to support smaller social networks, so that only those who are physically proximate will have files shared. Using FarCry with Bluetooth, or other near field technologies is another possibility that we are investigating.

It is important to note that FarCry is still a potentially useful technology if there is no clustering of interests, and exchanges take place soley between strangers. In this case FarCry works at the level of a sharing 'zeigeist' files – files that are popular in a particular area or organisation. This would mean that, for example, in MeetingNet files from all meetings are exchanged and with MediaNet a geographical area's files are exchanged.

We plan to trial FarCry with groups of users to explore further the propagation of files. In particular we are interested in how successful our preemptive caching of data will be at supporting information exchange. In future technical work we plan to expand FarCry to work over Bluetooth as well as wi-fi, and to be compatible with more devices than the restrictions of its current .NET incarnation allow. We are also looking at the option of allowing the system to function across a VPN - this would allow a tunnel to connect together discrete and separate FarCry networks. This is particularly applicable to MeetingNet.

6. CONCLUSION

FarCry takes advantage of the mobile and social nature of individuals, providing a framework for mobile, data sharing. Set-up overhead and bandwidth restrictions do not adversely affect the system, thanks to a dependency on social gathering as a means of determining compatibility. Sharing of information using FarCry exploits proximity and face-to-face contact, rather than attempting to overcome distance, as do most internet based application. In this way FarCry has the potential to be integrated into existing social networks, such as groups of friends, in turn spurring its further use.

The three applications discussed each show how this technique can be adapted to new domains. While we are cautious due to the possibility of viruses, in our future work we plan to explore how these techniques could be applied to the other types of information, such as software updates. More generically we see much potential in applications that work with geographical distance instead of attempting to overcome it.

7. ACKNOWLEDGMENTS

8. REFERENCES

[1] Boden, D., and Molotch, H. L. (1994)b. *The Compulsion of Proximity*. pp. 257-286 in NowHere: space, time and modernity, edited by R. Friedland, & Boden, D, London & Berkeley CA: University of California Press.

[2] A. Beaufour, M. Leopold, and P. Bonnet (2002) *Smart-tag based data dissemination*. In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA-02), pages 68-77, New York, Sept. 28 2002. ACM Press.

[3] Brown, B. Geelhoed, E., and Sellen A. (2001) *Music Sharing as a Computer Supported Collaborative Application*, In Proc. of ECSCW'01, pp. 179-198, Bonn, Germany, Kluwer Academic Publishers

[4] A. Demers, D. Greene, C. Houser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart and D. Terry, *Epidemic algorithms for replicated database maintenance*, ACM SIGOPS Operating Systems Review, 22 (1988), pp. 8-32, ACM Press

[5] Esbjörnsson M., Juhlin O. and Östergren M. (2003) *Motorbikers Using Hocman – Field Trials on Mobile Interaction*. In Proceedings of the 5th International Mobile HCI 2003 conference, Udine, Italy, Springer-Verlag.

[6] A. Hayes and D. Wilson (2004) *Peer-to-Peer Information Sharing in a Mobile Ad Hoc Environment*, In Proceeding s of the Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'04), pages 154-162, Lake District National Park, United Kingdom, IEEE Computer Society.

[7] S. Goel, M. Singh, D. Xu and B. Li, (2002) *Efficient Peer-to-Peer Data Dissemination in Mobile Ad-Hoc Networks*, 2002 International Conference on Parallel Processing Workshops (ICPPW'02), IEEE Computer Society, Vancouver, B.C., Canada, p. 152.

[8] A. Khelil , C. Becker , J. Tian and K. Rothermel (2002) *An epidemic model for information diffusion in MANETs*, Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems, pages 54 - 60 , September 28-28, 2002, Atlanta, Georgia, USA, ACM Press

[9] E. Paulos and E. Goodman. (2004) *The familiar stranger: anxiety, comfort, and play in public places*. In Proceedings of the 2004 conference on Human factors in computing systems, pages 223--230. ACM Press

[10] D. Sandler, A. Mislove, A. Post, P. Druschel (2005) *FeedTree: Sharing Web micronews with peer-to-peer event notification*, to appear in 4th International Workshop on Peer-To-Peer Systems, Ithaca, New York.

[11] Dave Snowdon, Natalie Glance (1999) *Pollen: Virtual Networks that use people as carriers*, In proceedings of Handheld and Ubiquitous Computing (HUC'99), pp 362-364, 27-29th September 1999, Karlsruhe, Germany.

[12] J. Su, A. Chin, A. Popivanova, A. Goel and E. de Lar (2004), *User Mobility for Opportunistic Ad-Hoc Networking*, In Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'04), pp 41-50, Lake District National Park, United Kingdom, IEEE Computer Society.

[13] A. Voida, R. Grinter, N. Ducheneaut, K. Edwards and M. Newman, *Listening in: practices surrounding iTunes music sharing*, Proceeding of the SIGCHI conference on Human factors in computing systems, ACM Press, Portland, Oregon, USA, 2005, pp. 191-200.

[14] Anonymous, Cachelogic (2005), *The true picture of peer-to-peer filesharing*, presentation available online at: http://www.cachelogic...om/research/index.php