Offline Social Networks: stepping away from the Internet (Position paper)

Anne-Marie Kermarrec, Erwan Le Merrer

Offline Social Networks: stepping away from the Internet (Position paper)

Anne-Marie Kermarrec
INRIA Rennes Bretagne Atlantique
anne-marie.kermarrec@inria.fr

Erwan Le Merrer
erwanlemerrer@no-log.org

Abstract

Online social networks have been revolutionary in the way people interact over the Internet today. Typically in online social networks the information is ephemeral while the relationships between users are sustainable. While they have been very successful, they usually do not leverage the notion of physical proximity. In addition the sustainable nature of the connections does not leave any room for sporadic and fleeting social relations. In this position paper, we explore the concept of **offline social network** considering geographical locality as a first-class citizen. Offline social networks do not aim at capturing long-standing relationships and in that sense are very complementary to online ones. Being implemented off the Internet, they avoid privacy breaches that users start to complain about. An offline social network relies on a hardware device, plugged in some location, to which anyone can freely connect. In an offline social network, while the relationships between users are ephemeral, the information can be temporary or permanent depending on the application scenarios. We believe that such a concept matches a wide spectrum of usages today that are not covered by online social networks. In this position paper, we describe the concept, the potential applications, the underlying technologies as well as the associated exciting research agenda.

1 Introduction

Online Social Networks (OSN) have conquered the digital world over the past five years and literally revolutionized the interactions between people over the Internet. Facebook counts today more than 800 million users. Every single event is instantaneously Twitted though thousands of different paths. Yet, it is hard to believe that online social networks match everyone needs and all situations. In addition the popularity of current social networks is not without having an impact on their functionality. First of all, a key notion in an online social network is the fact that relationships are sustainable while the information delivered through posts is clearly ephemeral. This represents an issue since giving up a connection on an online social network represents a negative statement about people. Yet, it might just reflect the fact that although you enjoyed talking again to your old primary school buddy, it did not take long to realize that you might not want to be permanently connected to him. Similarly, information posted a long time ago is almost impossible to dig out, several scenarios can be thought of where a permanent access to information can be desirable. Finally, privacy is a recurrent issue in OSNs. While the mere presence of a 800 million user network does not seem to convey any fear from the Internet users, users might be more and more reluctant to give away so much information about themselves[1]. In addition, while some knobs are available to adjust the privacy settings, there is anecdotal evidence that nobody bothers changing the parameters for every post. While this might not be perceived as a drawback, and is indeed a clear asset in many situations, the wired and global nature of online social networks, together with the huge information overload they are under, does not ease the leveraging of physical locality. Other secu-

[1]The value of Facebook is mostly due to the enormous amount of personal data that the company holds.

rity and privacy concerns for online social networks include information leak, user de-anonymization, phishing and spamming [7].

Interestingly enough, physical proximity is not without having a clear impact on social networks and this is conveyed by the growing number of Foursquares users. Yet, introducing the physical locality in current social networks (Foursquare is integrated to Twitter or Facebook) has not yet entirely fulfill its promises and there is hardly any new functionality emerging from it. In this paper, we propose a novel and orthogonal way to implement a social network, entirely stepping away for the Internet. We present here the **Offline Social Network** (OffSN). An OffSN is simply a hardware device which acts as a rendez-vous point between various users located in the area of reach of that device, who can potentially form a social network, exchange data, store their own data, use the local data stored, while potentially enjoying all the standard functionalities of OSN, such as chat, walls, etc. The fact that there is no connection to the Internet and that the accesses to that box are anonymous by default (depending on the users and the parameters), the users privacy is preserved (provided the box is trusted). The users may interact through the OffSN and create an ephemeral social network, reflecting the fact that they are at the same location at the same time while not implying any long-standing digital relationships in the future. The information stored on the OffSN can be temporary as a guarantee that the data durability is limited over time and that no user can be traced. It can also be permanent for instance when associated to a specific location.

Recent approaches such as Vanish [8] have made the case for time limited data durability (as e.g. emails or wall messages), proposing a solution for self-destructing data. The rationale is that some interactions between users, made possible by the use of electronic resources, have an acceptable lifetime and are not meant to be accessible by possibly third parties *ad vitam aeternam*. There has been some notion of location-aware or context-aware social networks such as Lovegety (a social network for dating services based in Japan) or office-based networks. Yet those approaches rely on a connection to the Internet to manage the relationships while exploiting the physical proximity to enhance the user experience. Opportunistic networks, also called pocket-switched networks, do not rely specifically on the Internet to operate. Yet, they focus on leveraging the mobility patterns of users to carry (route) information [11]. One of the closest approach is the PirateBox [6], which is designed to provide a totally mobile box for file-sharing, therefore running on battery. We seek to offer an enhanced service by providing additional social communication and interaction tools, possibly over a short to medium time span. Finally, another interesting work [5] aims at providing friend recommendations, as well as acquaintance information, for people located nearby in an office, through workplace resources. We discuss in this paper the opportunity and the benefits of exploring such proximity-related interactions.

The goal of this position paper is to introduce the concept of Offline Social Network, to discuss some possible application scenarios and to expose the research challenges associated to OffSNs. We do not aim at that stage at providing a complete solution but rather to convince the community that this novel concept can be of great interest both from the users and researchers standpoints. The rest of the paper is organized as follow: we first present some application scenarios of OffSNs in Section 2, we then present the technical details of the proposed solution in Section 3 before setting up the research agenda ahead in Section 4.

2 Application scenarios

In this section, we introduce a number of potential applications for offline social networks, that would be difficult to cover with traditional online social networks.

2.1 Local information sharing

Online social networks represent a great way to share information, but the very temporary nature of the information in OSNs is such that if should someone want to share some data on the long term, he/she has to place it on his/her account and periodically generates notifications targeting the new comers. Additionally, when data is meant to be shared among geographically close people, in reach of a local area network for instance, there is no reason nor need for that data to first be uploaded to

the Internet (at the often low WAN bandwidth), to be then downloaded again locally. This would rely on the Internet infrastructure while the LAN infrastructure is perfectly adapted and sufficient here. Yet such situations happen all the time.

Promoting local content Consider a location to which context-aware information is associated (for instance an art gallery located in some city). Targeting the right set of people, *i.e.* the people who might be able to visit the gallery, might be very difficult. As a complementary solution to traditional ways of advertising, offline social networks plan to leverage the physical proximity of people to some specific location and target a wide audience over time. The basic idea is to install an offline social network in specific places, *e.g.* an art gallery. Such a feature could both attract visitors, walking in the area as well as augment the users' experience within the gallery. In addition to the traditional exhibition paintings on the gallery's walls, a sharing device can offer artists' work in a numeric format, for example through a web page exhibiting (other) pictures. The difference with an online web page is precisely what makes the scenario of particular interest: accessing the additional content requires the people to be physically in the gallery to connect to the offline device (simply using a tablet or a smart phone and Wi-Fi connectivity). The visitors can then post back some appreciations on the artist wall present on the same device, making the exhibition more interactive, and *de facto* creating a social interaction between the artists and their visitors, and possibly between visitors themselves.

While an online social network could be used here, it will not provide the exact same interaction and would serve the different purpose of providing a more global event, but removing the local interest of people and artists reunion in a dedicated area.

Discovering music Another potential scenario is related to discovering and sharing music among a large-set of people gathered in a concert hall for instance. Clearly, the Internet has completely changed the way music is shared, discovered and even converted into cash in the world. While music can be instantaneously shared over the world, one of the thing that professionals try to leverage is the added-value of going to a concert. An interesting application of an offline social network in such a setting could be to share information both ways. Consider a band, having a concert where fans would pay for the concert and in return would get some of the music tracks for free. The Offline social network could be used to download the music tracks without requiring an online password/verification procedure. The rationale is very simple: if you are in the room attending to the concert, you get the music track. In addition, even in concerts, it is well known that all the attendees are using their phone, tweeting away, taking pictures, etc. The very same device implementing the offline social network could be used to upload this material and share it with the people collocated at the concert and typically interested in the very same event. Note that this does not prevent anyone to also share some of the information online on traditional OSN as people do today. Privacy-wise this is riskless, there is no control of who is posting what, people download from the OffSN what they are interested in. The information on the box is as ephemeral as the concert, as well as the interaction between attendees.

2.2 Ephemeral social network

Beyond the simple information sharing, the same device can be used to create a real social network, the vocation of which is not to last over time.

Remote meeting Consider the following scenario of a professional meeting held in a specific city, gathering some people who happen to know each other, some are friends, some are not, who meet for a specific reason (for instance a European Project meeting, or a physical program committee meeting). This is typically a scenario where people can interact, potentially socially. While they have lunch or dinner, they might talk over about various things: work, papers, music, restaurants, etc and are in a somewhat close relationship for a few days; that is not meant to last. An offline social network here could be used to share information over this period of time, without leading to any future obligation. We conducted a very-small scale experiment in a work-related meeting recently among twenty people. The experiment showed that many of the participants happily shared content

and the nature of the content was of a very different nature: work-related documents, pictures of the place of the meeting, pictures and music as well as other text document not particularly related to the meeting. All the posts were anonymized. This shows that the social circumstances of any work-related meeting may be leveraged to implement a short-term social interaction.

Family sharing Being a friend on Facebook of your teenager is always an issue on both sides. Now consider a family reunion, such as a wedding for instance or a party. It is unclear that all those people are indeed connected through an OSN. There is definitely some value to have a hardware support in order to share anything related to the event of the reunion, pictures for instances or videos. It is a well-known fact that the people you have not seen for 10 years and to whom you promise to send your pictures of the day will never get them. An offline social network can easily serve that purpose without generating the need of maintaining sustainable relationships on an online social network.

2.3 Locality-aware personalized recommendations

Going even further, there is a very promising application of offline social networks that would address an unsolved issue. While the greatest efforts have been devoted to recommendation systems and ubiquitous computing, the integration of both is yet to come. As surprising as it might seem, today, at the 21st century, finding a restaurant, in an unknown city, adapted to your habits, tastes, standards is still and issue for most of us. We end up, browsing the Web on the tiny screen of our phone, in the night and cold, trying to decrypt the recommendations, potentially controversial, of remote people, before finally deciding almost at random. Yet, each of us, could very easily advise a good restaurant in our own city that would be relevant for people resembling us or sharing similar tastes. The offline social network could be used to implement such a local recommendation system. Ideally when wondering in search of a restaurant, by connecting to the offline social network of the vicinity, one could benefit from restaurant recommendations depending on his/her profile. This could potentially be used for many other areas (clothes, shoes, etc, art, movies). While we believe this is a great application of OffSNs that poses many technical challenges that we will enumerate later in this paper.

3 Building OffSNs with Widrop

The *dead drops* project, by the German artist Aram Bartholl, received in 2010 a considerable media coverage. This project consisted in promoting the insertion of USB keys in city walls in order to provide *an anonymous, offline, peer to peer file-sharing network in public space* [3].

Widrop [1] (standing for WIreless dead DROP) is the pragmatic extension of such a concept, providing at once a more resilient and more convenient technology for such a sharing scenario. Widrop places mini-servers in the cityscape in order to provide an easy way to drop files and is easily accessible by anyone through a standard Wi-Fi connectivity. Concomitantly the fully mobile counterpart was introduced in the form of the so-called PirateBox [6]. Our novel concept of OffSNs relies on widrop, enhancing it with additional functionalities to fit the scenarios we contemplate in this position paper. Below we provide the details of the widrop along with the guidelines for its social extension.

3.1 The basic widrop layer

We now briefly describe the widrop mini-server we have built, that will then be used in discussions as a basis for implementing OffSNs.

Model and operations

As initially imposed by the basic capabilities of the USB dead drop devices, widrop follows the philosophy of a publicly accessible device in full read/write mode. This deliberately gives a full control of any user on the whole content of the shared storage space. This might be considered as an obvious opportunity for attackers to block any action on a particular widrop. Yet, we believe that in a geographical space probably occupied by people knowing each other or at least here, to share some common interest, this has a lower chance to occur that on

Figure 1: A widrop prototype with Wi-Fi and USB dongles, based on a Linksys NSLU2 flashed with Linux/Debian (2.1 x 9.1 x 13cm dimensions, for a 5 Watts consumption)

large scale networks. We come back on those issues in Section 4. Among the benefits of the widrop, is the opportunity for users to manage themselves the content (e.g. remove inappropriate insertions), but also remove a part of the responsibility of the widrop provider regarding what is hosted or done on the box. The other benefit of widrop over the dead drop is that the storage space can be much larger on such a server allowing for multimedia content for instance. Finally, the widrop can be hidden of the users in some secured space (as accessed through Wi-Fi), and thus cannot be directly localized nor disrupted.

A 5 Watts, Linux-based prototype

We have build a prototype on a cheap network-attached storage (or NAS) unit (as presented on Figure 1), initially meant to plug USB hard drives and make them accessible at any time on a local Ethernet network. This Linksys's NSLU2 original interface, accessible through HTTP, only permits basic NAS related operations; this device can be hacked by flashing and upgrading to a full Linux/Debian install[2]. The device is formed of a ARM Intel CPU (at 266MHz), with simply 32MB of sdram and 8MB of flash. There are 2 USB slots (to originally plug hard drives), so that one can be used for increased memory to host the OS and the storage space, and the remaining one to add an USB Wi-Fi dongle, to allow wireless connectivity.

The widrop application is then build from this Debian basis, installing lightweight packages that will propose the targeted service. The first service (*Hostapd*) turns the server into a Wi-Fi hotspot (essid is set to "Widrop"). *DNSMASQ* is then used as a DHCP server to provide an IP address in the local network to the interested user; this service also redirects any web traffic from the browser to a predefined local address (i.e. implements a captive portal). *Lighttpd* then provides the local web-server to display the welcome page where the user is automatically redirected, explains the widrop concept, and provides a link to the shared storage space (accessible via a simple HTTP listing or FTP with *vsftpd*) and a button calling an upload form that may be used to send a piece of data. While by default data remains in the shared space until wiped out by users, *cron* jobs can then be activated by the widrop operator to periodically flush data.

Widrop installation footprint on NSLU2's CPU is below 3% while idle, and showing peaks at up to 60% due to the ftp server *vsftpd*, while a large file is downloaded. The performance bottleneck is related to the I/O system, with around 1MB/s of available throughput for large files.

The crucial vector allowing physical-proximity only interactions is the Wi-Fi dongle, that covers a pretty limited area[3]. As this proof of concept is more low consumption than performance oriented, its scalability is limited and more adapted to a "stationary" usage. *FatDrops*, i.e. their flash-crowd resilient counterparts are currently considered.

3.2 A social enabled extension

The widrop provides the storage basis and a very simple device to implement data sharing, so that no technical skills are required to use the device and share data. Obviously for the widrop to offer users

[2]see `http://www.cyrius.com/debian/nslu2/`

[3]Several widrops are currently deployed in the city of Rennes.

the functionalities of an offline social network, we need to extend it with additional features.

The widrop basis, aimed at providing an anonymous data-depot, can be extended in order to provide a more complete platform for local interactions. There are several popular open source social network frameworks available on the Internet. Elgg [2] is one example, distributed under GNU GPL and MIT licenses, providing a tunable social networking engine and allowing multiple plugins to be added. The required setup is a classical Apache/MySQL/PHP on the server side. Such a layer may constitute an easy startup to develop and integrate location and event specific boxes: for instance, OffSN can implement a basic message wall for communication and posting of data, as well as add right management. Data inserted may progressively vanish with time; the interface would just display last messages, and delete them all when the box is turned off. We are currently investigating such an extension.

4 Challenges

In this section we review the various research challenges associated to the concept of Offline Social Network that we introduced in this paper.

4.1 Privacy

Privacy is one of the first issue that comes up to mind when introducing any new concept in the area. We believe that the concept of offline social network, due to the fact that there is no connection with the Internet, provides potentially better guarantees than online social networks with respect to privacy. Yet, OffSNs need to account for such guarantees while being designed.

When being connected to the Internet, the public IP address (given by an ISP) accurately identifies the associated user[4]. On the contrary, moving offline has the advantage of removing such a hard-coded mapping between a device being connected and an user identity: local IP addresses are non unique. The accessible information at an OffSN is only the MAC address of the device connected to the system. While MAC addresses are unique, identifiers originally hard-coded in each physical network interface, they are not tied to specific users in providers databases. Therefore they can not be used to identify the person carrying a specific device. Regardless, MAC addresses can be trivially masked at OS runtime (*e.g.* with a simple `# ifconfig eth0 hw ether 12:34:56:78:12:34` under Linux), adding easy plausible deniability in the balance. Additionally, such a privacy-oriented device should also purposely remove all logs that will allow to infer generic user's behavior, as for instance patterns of access to that box; this will avoid further investigation from "out of the box" trying to breach privacy.

Another step to avoid data leaks and investigations, preserving user's privacy, is to consider on the fly encryption of the box's disk. This ensures that the system configuration, logs and more importantly user's data become unexploitable by an external attacker, thus preserving users privacy. A complete audit on this very sensitive privacy question is yet to conduct.

4.2 Trust and security

Beyond privacy, a key for adoption and success of an application is the trust that users can put on the service provider. While trust clearly relies on variable metrics, even feelings from one user to another, being able to provide a provable means that privacy and security are respected and that the server follows the initial announcement is definitely an advantage for a wide adoption.

Open source approaches clearly provide this advantage over closed and proprietary software that code can be checked out by anyone, and that privacy breaches can be detected and patched earlier, due to the potential amount of people interested in a given project. When relying on a single central point to implement the local social service, as in the widrop device example, the question comes down to who is operating it, and what the device is actually doing. Security-checking procedures as SWATT [9] allow remote applications to challenge a specific server to assess if it is running the legitimate code, and thus prove that no malware has been inserted in it. This is made possible by verifying memory contents of the device, using randomly generated challenges that require legitimate checksums of server's actual memory. Adaptation

[4]Organizations such as Hadopi or Acta precisely leverage this mapping.

of this solution in our particular context constitutes a challenge, as currently, the whole OS code must be audited (not only the widrop application on the server). Such a security add-on, specifically targeting the widrop server code itself, can then greatly participate in making the public confident about those local networking applications.

Another frequent feedback from widrop users is the fear that such a box becomes a virus vector. There is probably no other generic answer than highlighting the fact that a proper antivirus is nowadays more than recommended, while using a widrop or the Internet. Widrops may be running antiviruses checking each insertion in storage space, but the very offline nature of this box would prevent virus databases to be updated, then making such a process useless.

4.3 Scale and flash-crowd

It is clear that several of the application considered in this paper would require OffSNs to be able to sustain peaks of load as well as a potential large number of users in permanent regime. For instance, in the concert experience, the hardware should be able to store a large amount of information (read and write). The hardware should also be able to handle flash-crowd to sustain a large number of users simultaneously.

Several alternatives can be considered to solve this issue. Firstly, the standard widrop, whose emphasis is on low power consumption, could be replaced by *fatdrop* supply, using trucks with extensive hardware and communication means and coverage, as done with satellite or TV trucks. A second alternative is to connect several widrops, thus increasing both the storage and the connectivity capabilities. This requires to provide a shared virtual space between multiple widrop, revisiting traditional distributed systems issues such as maintaining coherence, providing a shared interface, to which should be added some networking issues.

Finally, in order to cope with extremely large scale dissemination requirements such as the music track dissemination in a concert hall, we can envision a peer to peer dissemination protocol assisting the OffSN. This requires the user devices to get connected not only to the OffSN but among them as well, introducing the need for users to install a local client for that purpose. Again, the fleeting nature of such a network and the lightweight requirements of the associated client, represents a challenging large-scale distributed setting.

4.4 Local recommendations

Using OffSNs for personalized and local recommendations is one of the most promising applications as well as the most challenging one. The idea behind such an application is to associate to each user, connecting to an OffSN, a set of users sharing similar tastes as in [4]. This set of users can be used to compute the recommendations for that users. Obviously this requires to be able to compute some form of similarity between users. Two scenarios can be considered. The easiest one is to compute recommendations accounting for users who are currently connected to the OffSN. A second solution is to store on the OffSN the anonymized profiles of users that have been connected in the past and use those profiles for the recommendations.

The main question in this application is to clearly define the notion of a user profile, such that it can be leveraged for recommendations without hurting the users profile. Also building up a profile for each user might actually require the users themselves to carry their profile, built up over their actions on the Internet. Dealing with the relationships between interaction between an OffSN and information harvested on the Internet is a very interesting question.

4.5 Towards a collaborative widrop

Finally, the notion of a collaborative widrop, that we briefly mentioned when discussing scalability, is clearly an interesting perspective to OffSNs. Indeed, increasing the level of privacy may come from distributing the responsibilities, as opposed to a standard client/server model. A challenging implementation of an OffSN may take place on user devices themselves, connected altogether. The aggregation of storage on devices would form a virtual and unified space, where users can interact and share data.

The fact that no specific participant has a particular role may also be leveraged to enforce the limited durability of the exchanges: a protocol based on *secret sharing* [10] would allow to control the number of people needed in a room for the shared

space to be "active". Indeed, using such a protocol, no participant has the secret key, but just a part of it; the aggregation of those key parts allows to control the number of users that are required to be able to access the service. Should the number of people in the room drop beyond a given threshold, the share may then become unreadable; this ensures that the platform and the data it contains provides a service that is timely-related to the event itself and its participants. In other words, the share is technically forced to disaggregate. The question of how to bootstrap the protocol (key fragment generation and parameter setting), as well as the reliability of such a system may constitute a challenge for a practical application.

5 Conclusion

The goal of this position paper was to make a case for the concept of offline social network. While we do not claim to provide a complete solution, we presented the networking capability of OffSNs, the basic technology, the potential exciting applications and some preliminary thoughts about the associated challenges. We really believe that while online social networks have a place of choice in order to maintain long distance contacts among people, offline and temporary networks can directly leverage the notion of proximity between users, favoring a new (local) usage of social networks. Two decades after the publication of the essay on Temporary Autonomous Zones (TAZes) by Hakim Bey, in which people escape control by forming temporary communities, we presented challenges and means to implement offline social network systems, that may be a support of choice for TAZes of collaborating people. This would push users' interactions far away from the big brother and ultra centralization syndrome.

References

[1] The wireless dead drops project. `http://widrop.bzhack.org/`, 2011.

[2] elgg. `http://www.elgg.org/`, 2012.

[3] Aram Bartholl. dead drops. `http://deaddrops.com/`, 2010.

[4] Marin Bertier, Davide Frey, Rachid Guerraoui, Anne-Marie Kermarrec, and Vincent Leroy. The gossple anonymous social network. In *Middleware*, 2010.

[5] Alvin Chin, Hao Wang, Bin Xu, Ke Zhang, Hao Wang, and Lijun Zhu. Connecting people in the workplace through ephemeral social networks. In *IEE Privacy, Security, Risk and Trust*, 2011.

[6] David Darts. The piratebox. `http://wiki.daviddarts.com/PirateBox`, 2011.

[7] Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, and Yan Chen. Security issues in online social networks. *Internet Computing, IEEE*, 15(4):56 –63, july-aug. 2011.

[8] Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, and Henry M. Levy. Vanish: increasing data privacy with self-destructing data. In *USENIX security*, 2009.

[9] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. Swatt: software-based attestation for embedded devices. In *IEEE Security and Privacy*, pages 272 – 282, 2004.

[10] Adi Shamir. How to share a secret. *Commun. ACM*, 22:612–613, November 1979.

[11] Zhensheng Zhang. Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges. *IEEE Communications Surveys Tutorials*, 8(1):24–37, 2006.