Popup Networks: Creating Decentralized Social Media on Top of Commodity Wireless Routers

Chaya Hiruncharoenvate, Wesley Smith, W. Keith Edwards, Eric Gilbert
School of Interactive Computing & GVU Center
Georgia Institute of Technology
{chaya, wersmith}@gatech.edu, {keith, gilbert}@cc.gatech.edu

ABSTRACT

Recent news has made social media notorious for both abusing user data and allowing governments to scrutinize personal information. Nevertheless, people still enjoy connecting with friends and families through social media but fail to use it to connect to local communities where we live our daily lives. In this paper, we present *Popup Networks*, a new platform for building hyper-local social computing applications, running on home wireless routers via an underlying mesh network. Summative interviews illustrate interests in using Popup Networks to create new local ties and as a backup in the case of Internet disruption. By utilizing locality to ward off external risks, Popup Networks provide alternative privacy, visibility, and economic models compared to traditional social media. While deploying Popup Networks would be an ideal evaluation, we argue that the technical tests and user interviews we conducted are suitable for socially complex systems such as Popup Networks—advocating an agenda moving forward for social computing systems research.

CCS Concepts

•**Human-centered computing** → *Social networking sites;*

Keywords

social computing; mesh networks; internet censorship; social capital

1. INTRODUCTION

Modern social computing systems play an important role in keeping friends and families connected—often over great geographical distances. Beyond simply being fun and engaging, social media use can have important benefits for the people and communities that use it. For example, social media use is associated with having a larger and more diverse network of relations [31], which can in turn be important for job searches and other activities [26]. Sharing photos and reading/posting comments on Facebook help build social capital in geographically-distributed social networks [15], but a larger Facebook audience may not find the post about new neighborhood police patrols very relevant [12]. In short, social media enriches our social networks and makes social ties more accessible than in the past [45]. It's important to note, however, that social media gives little design priviledge to local communities—the places where *local* social capital is generated and *local* ties are created [44].

GROUP '16, November 13 - 16, 2016, Sanibel Island, FL, USA

ISBN 978-1-4503-4276-6/16/11…$15.00

DOI: http://dx.doi.org/10.1145/2957276.2957285

However, current social media architectures exhibit a number of profound issues. First, the recent outcries of governments' surveillance over social media [29] and questionable practices surrounding user data by social network site operators [33] raise significant questions about privacy via these systems. Second, beyond the U.S., citizens in some countries live under the watchful eye of repressive governments who limit access to the Internet based on what the lawmakers deem appropriate. Part of this problem is the centralization in the Internet's client-server model [13], where control of a few centralized servers is easier than controlling multiple decentralized nodes [21].

We argue that properties around scale, privacy, and economics in today's centralized social media architectures remove users from their local communities, leave services vulnerable to disruption (such as in times of natural disasters), and expose user data to governments and marketers. While decentralized social systems such as Diaspora adopt federated infrastructure to mitigate the problem of a single failure point, they require users to purchase and set up expensive, always-on servers, creating a technical barrier for everyday users. Yet, most households now own and operate a powerful always-on, always-connected servers—*their wireless routers*—within their homes and under their control.

In this paper, we present a novel technical platform called *Popup Networks* intended to address part of this problem. We designed the system around goals that emphasize sustainability, repurposing of existing infrastructure, distributed identity, trust, ownership, and privacy—an approach we call *hyper-local social media*. Our system runs on top of common, consumer-grade wireless routers that are linked via an underlying wireless mesh network, thereby separating the network from the global Internet. A Social API embedded in the system allows developers to easily build applications to support social interactions in the network. Popup Networks use a socially distributed trust protocol called *vouching* to protect privacy and security of user data. Since everything *lives on* and *runs on* the routers, this system is perfect for neighborhood communication where the hyper-local scope communication is not suitable for the global scale of social media. Furthermore, we believe activists and disaster relief efforts can also quickly deploy this system in their local areas where the Internet is no longer a suitable venue, or not available.

To evaluate the system, we conducted two lab tests to understand the technical capabilities of home wireless routers and mesh networks. We also interviewed 13 people to gauge initial impressions for Popup Networks. Participants saw the system as a way to increase social capital among neighbors by acting as an ice breaker

to reduce social barriers in meeting new neighbors—primarily ones who share interests. Also, Popup Networks would be a viable communication platform during times of Internet disruption, according to our interviews.

This paper is organized as follows. First, we review the social capital theories and empirical studies that underpin this work. Next, we introduce the design principles that frame Popup Networks. Finally, after describing how theories and architecture drove the Popup Networks design, we present our interview participants' reactions to the system. In summary, this paper's contributions are threefold:

1. A novel social computing technology that provides alternate *privacy, visibility*, and *economic* models relative to traditional social media;

2. An evaluation of this system, incorporating technical tests and user interviews, finding Popup Networks are both feasible and useful;

3. A brief argument for why these methods are appropriate for new social computing technologies, suggesting an agenda moving forward for social computing systems research.

2. LITERATURE REVIEW

In this section, we review three bodies of literature. First, we relate the rich social science literature surrounding social capital to the design goals of Popup Networks. Next, we present current work on distributed social network platforms and the use of wireless mesh network and distinguish how Popup Networks build from them. Finally, we conclude this section by visiting recent events of Internet disruption and censorship caused by political governments and natural disasters, along with the means that researchers and activists presented to get around them.

2.1 Social Capital and the Importance of Local Ties

We know that social communities are strong communities. Through simple, informal activities, communities build social capital [43]. Based on the work of Coleman [17], Bourdieu [14], and Lin [39], social capital is most commonly conceptualized as the sum of the resources embedded in social structure, or the ability to access resources in social networks for some purposeful action; social capital is a resource that plays a pivotal role when communities face challenges requiring collective action, through the means that increase community attachment [47] and empowerment [24], and reduce crime rate [48] and fear and mistrust [46].

While most Americans have few strong ties at the neighborhood level [52], local ties are still important. Neighborhood ties are the source of very specific types of individual support, such as help with child-care, emergency aid, and home improvements [53]. At the community level, social capital available through weak social ties may be more valuable than a network of close, densely-knit cliques of strong ties as weakly bound neighborhood connections are necessary for successful collective action [27].

There is a growing body of research on exactly how and why social media translates into social capital [15, 25]. In this line of research, studies look for the specific features that create social capital. For example, in Facebook certain affordances matter more than others, such as wall posts accounting for more accumulated social capital than simple status updates [15]. However, a gap exists where social network sites often do not provide functionality to discover new local connections—an important factor in building new ties.

While these studies focus on social capital created at a distance over Internet-based social media, the idea that online communities can help local communities is not new. A number of studies from the field of community informatics and others have attempted to design and evaluate Internet interventions for social capital at the neighborhood level [30]. Due to this need to facilitate new tie creation at the local level, new online communities such as Nextdoor[1] and iNeighbors[2] have flourished. However, previous research showed that audience scope and scale can be a problem in community-oriented social media [20, 41].

Despite largely encouraging results of these interventions and the recent boom in social media use, national studies have found that only 4% of Americans use the Internet for neighborhood-level interaction [32]. Together, these findings indicate an opportunity for new approaches to social media, focused on the local level. We believe *Popup Networks can lead to new tie formation and increased bridging capital in local communities*.

2.2 Distributed Social Network Platforms and Mesh Networks

Popup Networks are distributed social network platforms because of how data is separately stored in different nodes. In many cases, distributed social network platforms have arisen in response to the privacy and security concerns inherent to centralized social network sites [20, 55]. Platforms such as Diaspora[3], Friendica[4], and OneSocialWeb[5] are examples of such systems. Some, such as Safebook [19], leverage real-life trust relationships in order to establish privacy in the online system, while others, such as DECENT [35], employ advanced cryptography to preserve the privacy and security of user content and relationships. Virtually all of these decentralized social network platforms use a federated architecture, in which users' data is spread across multiple servers that work together in cooperation via the Internet. From our perspective, these Internet-based platforms rely on a single point of failure—*the Internet*. Additionally, the Internet still leaves these systems vulnerable to malicious acts from hackers and surveillance by ISPs and government.

Perhaps the most important idea of an Internet-free network is the near-ubiquitous presence of residential Wi-Fi. Recent data suggests that over two thirds of U.S. households have broadband connections, with over half of these having a home network [34]. Importantly, in high- and medium-density areas (in other words, both urban environments and many suburban ones), the density of networks means that at any given point multiple Wi-Fi networks are visible and allowing for the creation of *wireless mesh networks*.

The idea of neighborhood and metropolitan wireless mesh networks is not new. Researchers have started to demonstrate the technical feasibility of neighborhood mesh networks in the 2000s [4, 7]. In practice, the Athens Wireless Metropolitan Network (AWMN) began in 2002 when Athenians were fed up with poor Internet service provided by telecommunication companies. Currently, AWMN has more than 1,000 users in the network, serving the connection speed up to 30 times faster than the Internet connection provided by ISP [37]. Researchers have also set up several testbeds such as MIT Roofnet [10] and SMesh [3] to explore and improve on several issues with wireless mesh network. However, most of them utilize

[1]https://nextdoor.com/
[2]https://www.i-neighbors.org/
[3]https://diasporafoundation.org
[4]http://friendica.com
[5]http://onesocialweb.org

specialized equipment, making them inflexible and hard to replicate for general household users [42].

Mesh networks have a fundamentally different structure from traditional wireless networks (as well as wired local area networks). In contrast to traditional network topology, each node in mesh networks must not only deal with its own data, but also potentially serve as a relay for the data of other nodes in the network [56]. This topology means that wireless mesh networks are self-organizing, self-healing, and self-configuring, as nodes automatically connect to each other and determine how to route data as the topology evolves [1]. The unique property that separates Popup Networks from other mesh networks is *Popup Networks repurpose existing home wireless routers as the network infrastructure instead of asking users to install rooftop antenna or other expensive equipment*.

2.3 Internet Freedom and Communication Disruption

Recently, Internet privacy has been jeopardized by increasing surveillance of Internet communication from governments, telecommunication providers, and website providers. The National Security Agency (NSA) has reportedly obtained personal Internet communication data such as email and social networking details from communication providers such as Verizon and AT&T and website operators and communication hubs such as Google and Apple [29]. Furthermore, citizens in several countries also experience Internet censorship where only content deemed appropriate by the governing body is available. Several researchers have explored content censorship in countries such as China and Iran and found that most social network sites that are popular in the western world such as Facebook and Twitter are not fully accessible from those countries [5, 6, 49]. Rather, localized versions are popularized to allow governments to maintain censorship control over "inappropriate" content.

While the First Amendment of the US constitution prohibits Internet censorship by all levels of the government, private entities can allow or deny services as they wish. Amazon removed Wikileaks from its hosting service when political pressure arose in 2010 [40]. The issue of freedom of communication was also brought up when the Bay Area Rapid Transit (BART) decided to shut down cell phone services on August 11, 2011 to prevent protests coordinated via mobile devices at some of its stations [18]. Under repressive governments, it is especially easy for the leaders to disconnect their citizens from the global Internet [21]. Several projects have attempted to use mesh network as an alternate channel for the Internet. In 2011, in the wake of the Stop Online Piracy Act (SOPA), Reddit users spawned a new subgroup to discuss the possibility of a city-wide mesh network to provide a version of the Internet that would not be subjected to government control [28]. Similarly, a group in Oakland, CA is testing a mesh network, called People's Open Network, to reduce the technological gap in the city by providing free Internet through volunteer mesh nodes [51].

Not only do wireless mesh networks provide citizens an advantage in limiting government censorship, but these networks are also useful in the aftermath of natural disasters. The Red Hook Initiative provided Internet connection to Superstorm Sandy survivors during the days that Internet and cell phone connections were not fully restored [36]. In 2013, the Boston mobile networks were highly congested due to chaos surrounding a bombing. Open Garden[6] were shone spotlight because it allows computer and Wi-Fi devices, including cell phones, to share Internet connection using wireless mesh network [2]. While these systems and applications offer similar functionality to Popup Networks, *Popup Networks accelerate the set up process during time intensive disasters by not relying on current communication infrastructure and not requiring extra equipment to be purchased by users or volunteers*.

[6]https://opengarden.com/

3. POPUP NETWORKS DESIGN

Drawing from the literature, we define four high-level design goals for Popup Networks that distinguish it from other social media and mesh network platforms.

Goal 1. Repurpose existing infrastructure. One of the oft-cited downfalls of federated social systems is that they require non-technical users to administer their own, always-on servers. A key insight underlying Popup Networks is that people all over the world already have relatively powerful servers always connected in their homes: their routers. By sitting on top of this infrastructure, we limit the technical burden of federated services on everyday users.

Goal 2. Sustainability and adaptability. Popup Networks is designed to operate independently of other infrastructure. The self-organizing, self-healing, and self-configuring properties of mesh networks do the work of maintaining paths within the network. The decentralization nature of Popup Networks will both allow the system to be independent from communication infrastructure and resistant to service disruption and government censorship.

Goal 3. Locality-based privacy. By default, Popup Networks function at much a smaller scale as our natural, proximity-based scoping mechanism providing different *visibility* by limiting communication exclusively to nearby nodes. Popup Networks application data is forwarded hop-by-hop via neighboring nodes in the network. Applications can specify the limits on information propagation, including the set of nodes that can receive it. To provide different *privacy* than current social media, each router houses all of its own application data locally, which others can request access if or when they choose, strengthening the idea that users do not have to worry that a global or unauthorized audience may see the information they share.

Goal 4. Distributed identity, trust, & ownership. Without a central arbiter handing out accounts and verifying identities (as Facebook or Twitter would), Popup Networks use a decentralized model of identity. Popup Networks use a *vouching* mechanism to indicate trust between users, similar to the vouching system used by the site Couchsurfing. Since Popup Networks offer a different *economic* model in which each user distributively owns and controls her own technical infrastructure and personal data, vouching information allows users to make judgment whether to share their information. Because data is stored locally on each user's node, copies of data are no longer available for mining once a user decides to delete it.

4. POPUP NETWORKS

To achieve the design goals, Popup Networks comprise three major subsystems running on top of residential routers:

1. A **customized router firmware** distribution with mesh networking, web servers, and databases all running on top of the router hardware.
2. A social **API on the router**, implemented via HTTP endpoints, enabling developers to build hyper-local social applications quickly and easily.
3. A socially **distributed model of trust** called *vouching*, permitting users to vouch for others and infer trust signals at the social level.

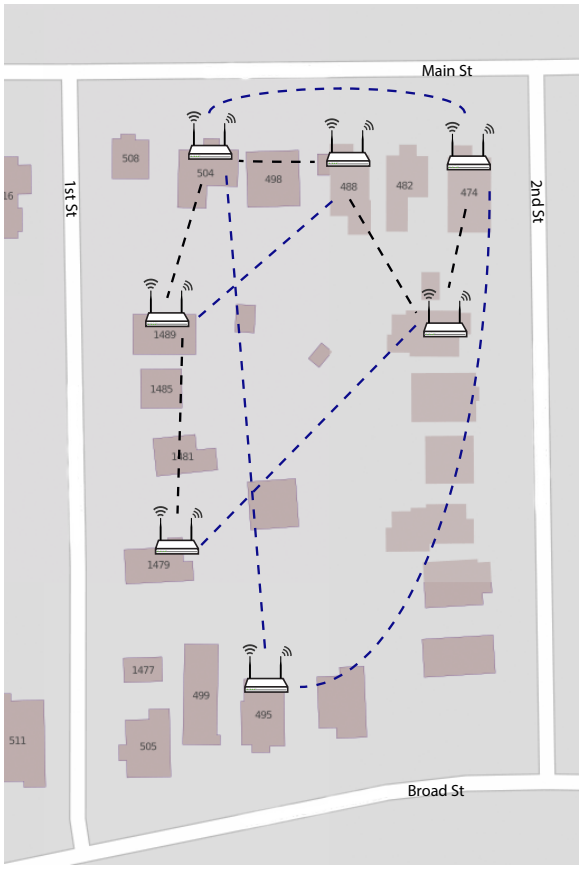

Figure 1: An example residential Popup Networks mesh network. Dotted lines represent wireless mesh network connections between routers; black for direct connections, blue for multi-hop connections. Note that the graph is not fully connected, just as there are missing links in social networks. Nodes adaptively find paths to other nodes with whom they wish to exchange information.

4.1 Implementation

Popup Networks run a customized build of OpenWRT-compatible router. OpenWRT[7] is an open-source Linux distribution for embedded devices, primarily home routers, and enjoys an active support community. For low-level mesh networking, Popup Networks use the Optimized Link State Routing (OLSR) protocol [16]. OLSR is an IP routing protocol optimized for mobile ad hoc networks, which allows nodes to discover and disseminate link state information through the network. The protocol allows Popup Networks to proactively discover routes to all reachable nodes visible in the network. We chose OLSR over other protocols because of its extensive community and its history of production use. (A full discussion of the network performance characteristics of OLSR is beyond the scope of this paper, but see [50] for more detail.) The software has been successfully deployed, for example, on community networks with thousands of nodes, such as the Athens Wireless Metropolitan Network.

On top of OLSR, Popup Networks run a customized LAMP (**L**inux, **A**pache, **M**ySQL, **P**HP) software stack, a common web application server environment. Optimizing for our router's embedded platform, we selected lighttpd, a small memory footprint web server[8] instead of Apache because of its efficiency; our platform also uses the FastCGI interface of PHP for performance reasons.

Our hardware platform leverages multi-radio access points, which are increasingly commonplace in the consumer market. Generally, the multiple radios in these devices are used to provide separate networks on different frequencies (2.4 GHz and 5GHz). Popup Networks repurpose the 5GHz radio solely for communication among other nearby routers running Popup Networks using ad hoc connections. We choose to use the ad hoc mode rather than alternatives (such as Bridge or Wireless Distribution System modes) because ad hoc connections do not require a fixed hierarchy of nodes in the network. OLSR creates a mesh routing layer atop these ad hoc wireless networks, providing a self-organizing and self-healing topology. The 2.4GHz radio is used for its original purpose, allowing clients to connect through it to access the Internet or the mesh. This approach provides a transparent mechanism to create a local neighborhood mesh network at high speed, while also maintaining constant connectivity of other devices inside the home to the Internet. Due to the performance of modern wireless standards, homes can potentially communicate with each other *much* faster than they can with Internet-hosted services; 802.11n networks, for example, have a theoretical maximum speed of 600Mbps, compared to common home Internet speeds in the U.S. of 1.5-12Mbps.

Specifically, we implemented Popup Networks on the D-Link DIR-825 wireless router, using a USB flash drive for extra storage, the software stack, and the database.

4.2 Social API

Popup Networks implement a core social API that allows developers to create hyper-local social media applications quickly and easily. For example, a developer might bring together these API endpoints to recreate Twitter as a hyper-local Popup Networks application. Popup Networks' social API provides basic social application primitives, such as following and vouching (i.e., trust), as well as data storage, communication, identity management, and discovery. It also transparently handles communication with the underlying mesh substrate.

The API follows the REST API model[9], a common design pattern familiar to modern web developers that uses the HTTP verbs (e.g., GET and POST) to wrap API calls. Popup Networks categorize its social API endpoints into six groups based on their purpose and functionality:

Applications API provides a mechanism to determine which applications are installed on a given node, allowing applications to find peer nodes in the network with which they can communicate (applications communicate with other instances of the same application). Not all nodes are assumed to have the same applications installed.

Users API provides information about the human users of the system, a key element in social applications. This API allows applications to both query and update profile information about users, both at the local and remote routers.

Message API supports basic messaging functionality among application instances. Applications can optionally specify a fixed set of authorized recipients of the message, or can allow messages to be public—meaning that they can be seen by all nodes. This API hides the low-level details of the mesh, such as routing and message delivery.

Relationship API provides functionality for establishing the social relationships that exist within the network. Popup Networks use

[7] http://www.openwrt.org

[8] http://www.lighttpd.net

[9] http://en.wikipedia.org/wiki/Representational_state_transfer

"following" relationship to connote a one-way social relationship between users. These are *application-specific*, and applications can use these relationships to manage increased levels of trust and sharing among users. If the application design relies upon bi-directional social connection, the API provides mechanisms to establish both following and followers relationships.

Database API provides a way for applications to store persistent data. Each application has access to a unique, sandboxed data storage area. The API provides a NoSQL-style database rather than a relational database to allow application authors to easily persist custom data structures expressed using JSON or XML. All data resides locally on the router itself; a common Popup Networks design pattern has routers querying the mesh network for data held locally at each node.

Vouching API endpoints allow users to assert that a given Popup Networks person/node pair is trusted, a process we call *vouching*. The API allows users to vouch for each other, and for applications to query whether a user is vouched for (and by whom). Note that this is distinct from following relationships; following relationships exist at the application level, whereas vouching is *global* and transcends particular applications. We design vouching and following relationships to be separated because different applications might have different meanings for following, and vouching is unique and universal throughout the Popup Networks system.

4.3 Vouching

4.3.1 Security Model

Popup Networks implicitly link routers to identities at the social level. However, this presents a core problem: How can I be sure you are who your router says you are? Adopting a worst-case scenario lens, we have to worry about "van attacks" where a villain joins the Popup Networks mesh network and spoofs an identity—either a new or existing one. While clearly an edge case, it may not be as farfetched as it first appears[10].

Leveraging existing relationships, we have re-appropriated the idea of "vouching" from the site Couchsurfing[11]. Couchsurfing is a travel network where participants stay on one another's couches while traveling and host travelers of their own. Vouching is essentially a distributed reputation model where participants put their own reputations on the line to assert that a user is trustworthy. Despite the inherent risks Couchsurfing clearly presents, it is remarkably safe [38]. Analogously, Popup Networks provide high-level APIs that allow users to vouch that the router on the network truly belongs to the person presented at the application layer.

4.3.2 Privacy Model

To preserve privacy of users and their data, privacy in Popup Networks is protected by multiple layers of technical and social infrastructures, fundamental to Popup Networks platform.

The technical infrastructure of Popup Networks helps ensure privacy in two ways. First, the local scope of connections through the wireless mesh network makes snooping harder because the packets are transferred between nodes directly without the need of a hub or switch. Second, encryption protocol can be put in place to prevent eavesdropping. Although encryption is not currently implemented in this version, Popup Networks can be easily extended through the API. We leave the extension of encryption in Popup Networks as future work.

The social infrastructure of Popup Networks also adds an additional layer of privacy protection. When a new or susceptible user joins the network and requests access for personal data, the vouching mechanism can provide social information about the trustworthiness of the questionable user. For example, Bob sees that Alice has vouched for Charlie. Since he trusts Alice, he uses his own judgment to decide that Charlie is trustworthy and allow Charlie to access his information. However, if Bob did not trust Alice, her vouch for Charlie would be meaningless to him. The vouching mechanism acts as another layer of privacy protection on top of the layers from technical infrastructure mentioned earlier.

[10]cf. http://en.wikipedia.org/wiki/Wardriving

[11]https://www.couchsurfing.org/

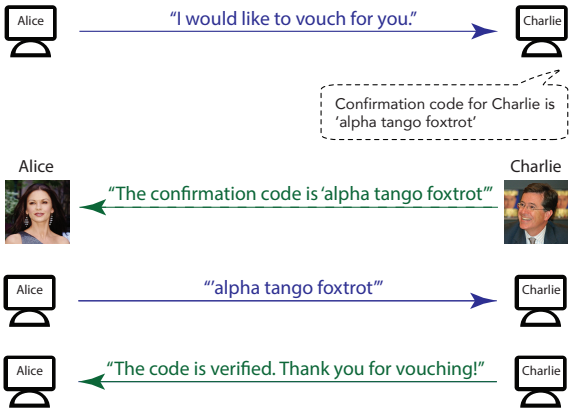

Figure 2: Popup Networks reference vouching implementation. Solid lines represent communication through Popup Networks' mesh network; dotted lines represents *out-of-band* communication, presumably over the phone or in-person.

4.3.3 Example Protocol

Popup Networks ship with a reference implementation of vouching that we consider to be one best practice. Developers can create new vouching mechanisms to suit their specification. At a high level, we have implemented a vouching protocol that forces Popup Networks users to verify one another's identities socially out-of-band. Figure 2 outlines the protocol, which we also describe in detail next.[12]

Alice, Bob, and Charlie are three Popup Networks users. Alice would like to vouch for Charlie who is new to the network. Popup Networks ask them to follow this protocol:

1. Alice visits Charlie's profile page and clicks a button to indicate that she wants to vouch for Charlie. Alice's vouching state for Charlie now changes from **notvouch** to **waiting**, an indication that Alice is waiting for a confirmation from Charlie.

2. Charlie's own router now notify him that Alice would like to vouch for him and generates a random string of words, such as "alpha tango foxtrot." Charlie now needs to give this string to Alice through another channel (e.g., face-to-face, email, phone) where she can verify his identity.

3. Alice receives the string from Charlie and enter to string to Charlie's profile page to confirm his identity. Alice's router checks it against Charlie's router database and changes her vouching state for Charlie to **vouched**.

[12]All images of persons used in this paper are photographs of celebrities from http://www.flickr.com/photos/shankbone/sets/72157623925606177, available under a Creative Commons license.

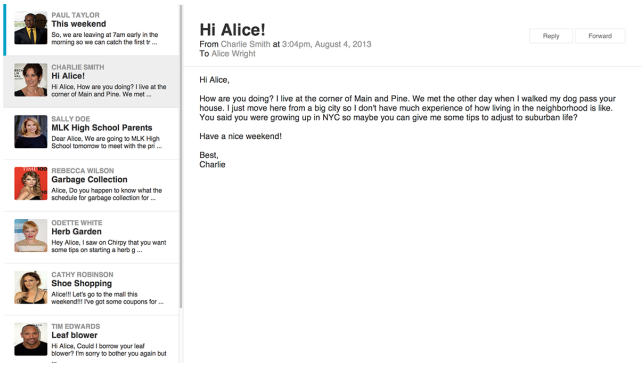

Figure 3: Messages main page. Messages permits one-to-one messaging between Popup Networks users.

Now, any time someone pings the Popup Networks network for who vouches for Charlie, Alice's router will respond affirmatively, while Bob's router will not. In this way, vouching information is distributed across the entire Popup Networks network; no single point holds it all. While not impossible to fake, Popup Networks' vouching signal carries a significant cost; this tends to make signals valuable in social systems [22].

4.4 Popup Networks Application

Popup Networks are designed to be an open platform[13] that developers can leverage to build hyper-local social computing applications. Developers can use the core APIs to send messages around the network, manage data and caches, as well as to manage social constructs like following (application-specific) and vouching (global-scope). Per-application data-bases on individual routers allow applications to keep their data accessible, yet sandboxed from other applications.

To illustrate the capabilities of Popup Networks, we present *Messages*, a replica of the most popular social application—email—rewritten as a hyper-local version using Popup Networks' social API. We present this application to emphasize the design goals presented earlier in this paper and illustrate how Popup Networks provide full support for common social media features.

Messages is a hyper-local clone of email. Like email, it allows point-to-point text messages between users, but in this case without ever leaving the Popup Networks network. Users simply enter the name of the recipient (a plugin progressively prompts nearby nodes for available users), in the "To:" field.

Messages manages its own tablespace through the database API. Conforming to the typical email standard, Messages stores the email it sends at the database of the recipient. When Alice sends an email to Bob, Alice's router contacts Bob's router via the database API and asks Bob's router to store the message for him. (OLSR guarantees that the nodes visited in transit cannot compromise the messages, so only Bob can read it.) Via the database API, Messages stores information such as the sender's name, sender's IP address, recipient's name, recipient's IP address, email subject, email body, and sent date, using JSON encoded objects. In the prototype version of the application we developed, we did not employ encryption on the message, but developers could extend Messages to include encryption at the application level.

[13]Our code is also open source, and made available under MIT license at http://comp.social.gatech.edu/papers

Up\Down	x.4	x.5	x.6	x.7	x.8
x.4		7.56	8.91	5.55	26.81
x.5	12.18		4.13	18.51	20.82
x.6	8.69	5.30		4.05	13.74
x.7	6.24	24.11	3.03		8.42
x.8	25.97	14.91	13.23	8.01	

Table 1: Upload/Download speed test result (Mbps). White indicates direct connection. Blue indicates weak direct connection. Yellow indicates 2-hop connection. Green indicates 3-hop connection.

5. TECHNICAL EVALUATION

We evaluated whether the mesh-based framework and the processing power of consumer-grade wireless routers would sustain the computational and network communication requirement of Popup Networks. As a proof of concept, we conducted two tests in lab settings to evaluate the performance of the consumer-grade wireless routers and the connections over mesh networks.

The first test to evaluate the performance of our routers. We performed 10,000 rounds of a basic PHP function that inserts and deletes a row to a MySQL table on the DIR-825 wireless router with Popup Networks software stack. Our benchmarks indicated that the router completes said operations in 360 seconds. For comparison, an Amazon AWS EC2 instance with a similar software stack took 225 seconds to complete the same task.

The second test evaluated connections over a wireless mesh network. Five DIR-825 wireless routers connected through Popup Networks were placed in different locations across 2 floors of a building. Each router was placed close enough to have a direct link to at least one other router (about 20-30 meters apart, in our test) and far from at least one other router to force multiple-hop connections. Out of 10 possible pairs of connections, our test mesh network topology had 1 pair of weak direct connection, 3 pairs of 2-hop connections, and 2 pairs of 3-hop connections. A speed test was conducted for a transfer of a 2 MB file between every router pair. We measured the average of the download speed in megabit per second (Mbps) over 10 rounds of such transfers.

Table 1 shows the results of the average speed over 10 transfers of 2 MB files for every pair of connections. Note that since all transfers are ultimately between two nodes, the downstream speed of one node is the upstream speed of the other node. In general, 3-hop connections are slower than 2-hop connections, which are slower than direct connections. Weak direct connections are also significantly slower than regular (strong) direct connections. However, multiple-hop and weak connections still provide downstream speed close to the 4 Mbps and upstream speed over the 1 Mbps "broadband connection" defined by the FCC [23].

The two performance tests proved that consumer-grade routers and mesh-based framework can provide resources to sustain a hyper-local social media platform. Although the first test showed that our wireless routers performed with much lower efficiency than a traditional web server, the local scope of Popup Networks will not require as much computational power as social network sites on the Internet, where thousands of users are online at the same time. Our wireless mesh network speed test proved that users will not notice much different in the connection speed between Popup Networks and broadband Internet connections.

6. INITIAL USER IMPRESSIONS

We conducted semi-structured interviews with 13 participants (7 female, age 18-52) to gather initial reactions from potential Popup Networks users. Participants were recruited from campus mailing lists and the neighborhood-centric social network site, Nextdoor. Each interview was approximately 30-45 minutes and was conducted either in person, over telephone, or Internet voice call, and each participant was compensated with $30.

We first asked participants about their use of social media to connect with neighbors and local communities. 10 of our participants reported that in addition to face-to-face contacts, phone calls, and texting, they also used some sort of social media (mailing list, Facebook, Nextdoor) to connect with their neighbors. This large proportion bias is due to the platform (Nextdoor) from where the participants were recruited. Two of our participants expressed that they might have different experiences due to Internet censorship and blocking against social media in their home countries. Then, we showed participants the concept of Popup Networks and the mesh network (Figure 1) and asked about the potential uses of Popup Networks and their privacy and security concerns. Finally, we asked participants about their opinions regarding Popup Networks serving as an alternative solution for Internet connection during service disruption and government censorship.

6.1 Local Communication

Participants see profile information that other people would share as an ice breaker to get to know new neighbors, especially ones who share interests or common characteristics.

> *If I have a neighbor who also goes to [the same school] then probably it's easier to kind of communicate saying "ok my school is here" that might be a good start. (P4)*

> *I think I'd be interested to see [which of] their kids are my kids age or can babysit, and also which schools they go to, which temple, so I could see who's got more in common with me. . . . I would look for like-minded people or people with the same kind of things that I have. (P10)*

Regardless of making new connections, participants believe that profiles of their neighbors could act as the "Facebook" of the neighborhood.

> *It would provide, while we have social gatherings, it's kind of nice to be able to have a picture and name because obviously when you are walking around the neighborhood, you don't really know if the person lives in the neighborhood or is just walking around the neighborhood and so this would be a way to put a name and a face together and high level detail around them, as much as they gave out. (P5)*

6.2 Privacy and Security

Participants have similar privacy concerns with Popup Networks as other social network sites. In general, they are willing to share information which might be useful to their neighbors and often compare what information they are willing to share on Popup Networks with what they already put on Facebook or Nextdoor. However, participants who live in an apartment complex have no problems with sharing their apartment number through Popup Networks because their neighbors usually already know which room they reside in.

> *Maybe one piece of additional information would be apartment number because it would just be in your apartment so there would not be a problem with security with the apartment number. (P4)*

> *[I would share to my trusted neighbors] my particular room number. These people will be the ones I know well enough to tell them where I am. A potential use is neighbors borrow stuff from each other so people could do that kind of stuff with this info. (P8)*

However, some participants are concerned that since Popup Networks operate at a hyper-local scope, it is easier for other users to pinpoint their real identity.

> *I won't post [some pictures I post on Facebook] on Popup Networks because sometimes I guess my audience cannot identify me easily on other social media, but in Popup Networks, I'm more identifiable. Maybe, I won't post some things like personal photos or more personal information on Popup Networks. (P11)*

> *I feel a little bit more concerned with [privacy on] Popup Networks because the fact that people are so near to me, and the fact that people stalk me or follow me, but for Facebook, the likelihood of this kind of thing can happen is not as much because people might not be in close proximity. (P13)*

Even for the neighbors that they know, the relationship and trust structure is complex. Our participants do not want a one-size-fit-all privacy policy when coming to sharing personal information.

> *The privacy setting [would be] a great [addition]. Maybe I can show certain posts to certain people. Like Google+ has circles, maybe I can create circles. (P1)*

Participants wish Popup Networks had a more transparent privacy model than traditional social network sites.

> *If each individual has a better control of their privacy and they can choose who to have access to the [information], and make it be upfront unlike Facebook where you have to go in and opt out, where they suddenly make everything open and you have to go back in and make it more private. I think it's better to be private up front and you have a better feature of choosing who to share in the network. (P7)*

6.3 Communication Disruption

While participants see Popup Networks as a promising platform to get around Internet censorship, the limited scope of Popup Networks also limits the variety of content available.

> *[I think Popup Networks can help alleviate the limited connection during censorship], but I think the scope will be limited to the local community not the global community because the issue I have experienced was the global censorship. . . . I don't know how Popup Networks can extend the network to other network beyond the neighborhood network. If it could do that, that would be a great thing because we don't even need to connect to the Internet so we don't have any censorship. (P11)*

Popup Networks could also become an infrastructure where people who have access to blocked content can share the content with the network.

> *[M]aybe Popup Networks users could get the content from other social media, other sources which are censored or blocked and put them on Popup Networks and share them with the neighbors who are not well connected to the other social media. Most of people may have limited access to the information resources. Other people who also have the connections to other social media can put useful information in Popup Networks. . . . I [also] would share [VPN and proxies] with someone that I know [over Popup Networks], could be my neighbors or relative who may not be my neighbors but live in the same town. (P11)*

Participants also view Popup Networks as an appropriate platform for a quick restoration of communication infrastructure during the time of disasters when traditional communication infrastructures are destroyed.

> *If Popup Networks [are] available during the Internet blockage, I think it would be important in the circumstance of emergency like if there's flood or hurricane, then it would be good. One time, the fire alarm went off and people didn't know what to do and someone need to come out so this kind of thing might be good. (P13)*

7. TOWARDS AN EVALUATION AGENDA FOR SOCIAL SYSTEMS RESEARCH

We did not deploy Popup Networks. This raises the vexing problem of evaluating social computing systems [8]. In this context, a successful evaluation of Popup Networks might resemble seeing it used by the Red Cross after they move into a disaster area, or a small group of neighbors who want to share their Internet connections among one another, or protesters either in the U.S. or abroad. While we would certainly welcome such a use case—and have promoted it or are working to promote—we argue that such standards (common to the UIST community, for example) no longer make sense for social computing research.

It is no accident that the majority of innovation happening around social computing systems takes place in industry (via the startup community and incumbents such as Facebook, primarily), or within the small group of academics working in crowdsourcing. Regarding the former, while we have seen wonderful systems emerge from startups, we would argue that ceding innovation solely to industry would be a path towards irrelevance for social computing. Regarding the latter, we look up to crowdsourcing work such as Soylent [9] and VizWiz [11]; yet, at the same time, it is evidently more straightforward to evaluate those systems because you can plug the software into online micro-labor markets such as Amazon Mechanical Turk.

Where does that leave us with *more social* social computing research systems? We cannot compel people to "be social" the way a typical "systems-style" evaluation might (by compensating participants for their participation). Nor can we plug into a willing and able group of participants as crowdsourcing researchers might with a crowd. Instead, we advocate for a third approach, exemplified by the work we have just presented. As social computing researchers, we think the field should strive for both technical innovation and human-centered relevance. The methods we have employed in this paper reflect that belief, and we hope that this work may serve as a guidepost for future evaluations of innovative social computing systems.

8. LIMITATIONS

The front-line hurdle that can prevent adoption of Popup Networks is the complications in setting up the software architecture of the system. While the Popup Networks software can be deployed as a simple one-step installation package, those who want to install Popup Networks onto their own routers must own wireless routers that are compatible with the custom firmware OpenWRT, and install the firmware on their routers. However, users with moderate to advanced technical skills can easily accomplish this task with the help from the extensive OpenWRT online documentation and support groups.

Regarding Popup Networks' infrastructure, the main technical limitation of using a mesh network to provide underlying communication infrastructure of Popup Networks is the limited reach of the network, as pointed out by participants from our interviews. However, if the network contains a large number of nodes, it can span a large area, as the Athens Wireless Metropolitan Network spans the city of Athens and nearby municipalities[14].

While mesh network systems like Popup Networks can help quickly restore communication infrastructure during disasters, electricity is still needed to power equipment, wireless routers in our case, to facilitate construction of the network. Thus, if there is no electricity, such systems cannot be useful for the affected population. However, wireless routers usually consume little power and can be run off of power generators. Furthermore, further research can utilize the advanced capabilities of smartphones in such a way that smartphones can become nodes in Popup Networks, eliminating the needs of electricity since smartphones can run off of battery power.

We did not conduct a large-scale deployment of Popup Networks. As argued in the previous section, a successful evaluation of Popup Networks relies on specific circumstances that, while possible, do not occur on a daily basis. We believe that the evaluations we performed and the argument we presented justify the novelty of Popup Networks and its contribution of the HCI community.

9. FUTURE WORK

As discussed in the Implementation section, security in Popup Networks can be enhanced with encryption. However, given the significant usability problems known to plague these systems [54], this may present an entire research undertaking on its own. We plan to start by extending the vouching protocol with a distributed public-key infrastructure and propagate this infrastructure throughout the system. Not only this infrastructure will help secure communications, but will also emphasize the concept of distributed identity, trust, and ownership in Popup Networks.

10. CONCLUSION

We presented Popup Networks, a platform for building hyper-local social computing application using home wireless routers. Popup Networks are built on top of a residential mesh network, leveraging their physical proximity; thus, it removes the need for data transfer to the Internet. Popup Networks provide different privacy and security, and a different economic model than traditional social computing platforms.

Popup Networks are composed of three major subsystems: a social API that allows developers to quickly implement applications to extend Popup Networks, a distributed trust model—*vouching*—that facilitates users' trust-making process, and a customized OpenWRT with mesh networking and software stack running on top of a consumer-grade router's firmware. Our performance evaluation proved that Popup Networks' infrastructure has abundant resources to provide high bandwidth connections between nodes. We presented an application—Messages—using Popup Networks' social APIs as a demonstration of its capabilities.

Our interview participants suggested that Popup Networks are a feasible communication platform during the time of Internet disruption such as government censorship and disasters. Furthermore, they showed interests in using Popup Networks to connect with their local ties and meet new neighbors. Exploiting locality allows Popup Networks to achieve its goals to provide a sustainable infrastructure for social computing applications that facilitate communications in hyper-local context.

Finally, we argue that while a deployment would be a perfect evaluation of Popup Networks, the nature of this system presents a great challenge in deploying into suitable communities and cir-

[14]https://wind.awmn.net/?page=nodes

cumstances. Instead, we present this work as an example of how to evaluate innovative social computing systems.

11. REFERENCES

[1] I. F. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. *Computer networks*, 47(4):445–487, 2005.

[2] A. Al-Akkad, L. Ramirez, S. Denef, A. Boden, L. Wood, M. BÃijscher, and A. Zimmermann. Reconstructing Normality: The use of infrastructure leftovers in crisis situations as inspiration for the design of resilient technology. In *Proc. OzCHI*, pages 457–466. ACM, 2013.

[3] Y. Amir, C. Danilov, M. Hilsdale, R. Musaloiu-Elefteri, and N. Rivera. Fast handoff for seamless wireless mesh networks. In *Proceedings of the 4th international conference on Mobile systems, applications and services - MobiSys 2006*, page 83, New York, New York, USA, 2006. ACM Press.

[4] P. Antoniadis, B. Grand, A. Satsiou, L. Tassiulas, R. Aguiar, J. Barraca, and S. Sargento. Community Building over Neighborhood Wireless Mesh Networks. *IEEE Technology and Society Magazine*, 27(1):48–56, jan 2008.

[5] S. Aryan, H. Aryan, and J. A. Halderman. Internet censorship in iran: A first look. In *Proc. of the 3rd USENIX Workshop on Free and Open Communications on the Internet*, 2013.

[6] D. Bamman, B. O'Connor, and N. Smith. Censorship and deletion practices in chinese social media. *First Monday*, 17(3), Mar. 2012.

[7] J. P. Barraca, P. Fernandes, S. Sargento, and R. Rocha. An architecture for community mesh networking. In *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2008.

[8] M. S. Bernstein, M. S. Ackerman, E. H. Chi, and R. C. Miller. The trouble with social computing systems research. In *Proc CHI EA*, pages 389–398. ACM, 2011.

[9] M. S. Bernstein, G. Little, R. C. Miller, B. Hartmann, M. S. Ackerman, D. R. Karger, D. Crowell, and K. Panovich. Soylent: a word processor with a crowd inside. In *Proc. UIST*, pages 313–322. ACM, 2010.

[10] J. Bicket, S. Biswas, D. Aguayo, and R. Morris. Architecture and Evaluation of the MIT Roofnet Mesh Network.

[11] J. P. Bigham, C. Jayant, H. Ji, G. Little, A. Miller, R. C. Miller, R. Miller, A. Tatarowicz, B. White, S. White, et al. Vizwiz: nearly real-time answers to visual questions. In *Proc. UIST*, pages 333–342. ACM, 2010.

[12] J. Binder, A. Howes, and A. Sutcliffe. The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites. In *Proc. CHI*, pages 965–974. ACM, 2009.

[13] M. S. Blumenthal and D. D. Clark. Rethinking the design of the internet: the end-to-end arguments vs. the brave new world. *ACM Transactions on Internet Technology (TOIT)*, 1(1):70–109, 2001.

[14] P. Bourdieu. The forms of social capital. In *Handbook of Theory and Research for the Sociology of Education*, pages 241–258. Greenwood Publishing Group, New York, 1986.

[15] M. Burke, R. Kraut, and C. Marlow. Social capital on facebook: Differentiating uses and users. In *Proc. CHI*, pages 571–580. ACM, 2011.

[16] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot. Optimized link state routing protocol (OLSR). *The Internet Society*, 2003.

[17] J. S. Coleman. Social capital in the creation of human capital. *American journal of sociology*, pages S95–S120, 1988.

[18] T. Collins. BART cell phone shutdown: Safety issue or free speech violation?, Aug. 2011.

[19] L. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine*, 47(12):94–101, 2009.

[20] A. Datta, S. Buchegger, L.-H. Vu, T. Strufe, and K. Rzadca. Decentralized Online Social Networks. In *Handbook of Social Network Technologies and Applications*, pages 349–378. Springer US, Boston, MA, 2010.

[21] J. Dibbell. The shadow web. *Scientific American*, 306(3):60–65, Mar. 2012.

[22] J. S. Donath. Identity and deception in the virtual community. *Communities in cyberspace*, 1996:29–59, 1999.

[23] FCC. Sixth broadband deployment report. Technical report, July 2010.

[24] K. J. Geis and C. E. Ross. A new look at urban alienation: The effect of neighborhood disorder on perceived powerlessness. *Social Psychology Quarterly*, pages 232–246, 1998.

[25] E. Gilbert and K. Karahalios. Predicting tie strength with social media. In *Proc. CHI*, pages 211–220. ACM, 2009.

[26] M. Granovetter. *Getting a job: A study of contacts and careers*. University of Chicago Press, 1995.

[27] M. S. Granovetter. The strength of weak ties. *American Journal of Sociology*, 78(6):1360–1380, May 1973.

[28] A. Greenberg. Wary of SOPA, reddit users aim to build a new, censorship-free internet, Nov. 2011.

[29] G. Greenwald and E. MacAskill. NSA prism program taps in to user data of apple, google and others. *The Guardian*, June 2013.

[30] K. Hampton and B. Wellman. Neighboring in netville: How the internet supports community and social capital in a wired suburb. *City & Community*, 2(4):277–311, 2003.

[31] K. N. Hampton, L. S. Goulet, H. Rainie, and K. Purcell. *Social networking sites and our lives: How people's trust, personal relationships, and civic and political involvement are connected to their use of social networking sites and other technologies*. Pew Internet & American Life Project, 2011.

[32] K. N. Hampton, L. F. Sessions, E. J. Her, and L. Rainie. Social isolation and new technology. *Pew Internet & American Life Project*, 2009.

[33] A. Hern. OKCupid: we experiment on users. everyone does. *The Guardian*, July 2014.

[34] J. Horrigan. Home broadband adoption 2009. *Pew Internet & American Life Project*, 2009.

[35] S. Jahid, S. Nilizadeh, P. Mittal, N. Borisov, and A. Kapadia. DECENT: A decentralized architecture for enforcing privacy in online social networks. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 326–332. IEEE, mar 2012.

[36] B. Kazansky. In red hook, mesh network connects sandy survivors still without power, Nov. 2012.

[37] J. Kloc. Greek community creates an off-the-grid internet, Aug. 2013.

[38] D. Lauterbach, H. Truong, T. Shah, and L. Adamic. Surfing a web of trust: Reputation and reciprocity on couchsurfing. com. In *Computational Science and Engineering. International Conference on*, volume 4, pages 346–353. IEEE, 2009.

[39] N. Lin. Building a network theory of social capital. *Connections*, 22(1):28–51, 1999.

[40] E. MacAskill. WikiLeaks website pulled by amazon after US political pressure | media | the guardian, Dec. 2010.

[41] C. A. Masden, C. Grevet, R. E. Grinter, E. Gilbert, and W. K. Edwards. Tensions in scaling-up community social media: A multi-neighborhood study of nextdoor. In *Proc. CHI*, pages 3239–3248. ACM, 2014.

[42] P. H. Pathak and R. Dutta. A Survey of Network Design Problems and Joint Design Approaches in Wireless Mesh Networks. *IEEE Communications Surveys & Tutorials*, 13(3):396–428, 2011.

[43] R. D. Putnam. Bowling alone: America's declining social capital. *Journal of democracy*, 6(1):65–78, 1995.

[44] R. D. Putnam. *Bowling alone: The collapse and revival of American community*. Simon and Schuster, 2000.

[45] H. Rainie, L. Rainie, and B. Wellman. *Networked: The new social operating system*. The MIT Press, 2012.

[46] C. E. Ross. Neighborhood disadvantage and adult depression. *Journal of Health and Social Behavior*, pages 177–187, 2000.

[47] R. J. Sampson. Local friendship ties and community attachment in mass society: A multilevel systemic model. *American Sociological Review*, pages 766–779, 1988.

[48] R. J. Sampson and W. B. Groves. Community structure and crime: Testing social-disorganization theory. *American journal of sociology*, pages 774–802, 1989.

[49] I. Shklovski and N. Kotamraju. Online contribution practices in countries that engage in internet blocking and censorship. In *Proc. CHI*, pages 1109–1118. ACM, 2011.

[50] A. Tonnesen. *Impementing and extending the optimized link state routing protocol*. University of Oslo, Department of Informatics, 2004.

[51] B. Valentine. Oakland's sudo mesh looks to counter censorship and digital divide with a mesh network, July 2014.

[52] B. Wellman. The community question: The intimate networks of east yorkers. *American journal of Sociology*, pages 1201–1231, 1979.

[53] B. Wellman and S. Wortley. Different strokes from different folks: Community ties and social support. *American journal of Sociology*, pages 558–588, 1990.

[54] A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proc. of the 8th USENIX Security Symposium*, volume 99, 1999.

[55] C.-m. A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners-lee. Decentralization : The Future of Online Social Networking. *Artificial Intelligence*, 2:2–7, 2006.

[56] Y. Zhang, J. Luo, and H. Hu. *Wireless mesh networking: architectures, protocols and standards*. CRC Press, 2006.