A Little Sharing Goes a Long Way: The Case for Reciprocal Wifi Sharing

Jinghao Shi, Liwen Gui, Chunming Qiao, Dimitrios Koutsonikolas, and Geoffrey Challen
University at Buffalo
{jinghaos,liwengui,qiao,dimitrio,challen}@buffalo.edu Paper #5

ABSTRACT

Widespread deployment of private home Wifi access points (APs) can result in uncoordinated and overlapping wireless networks that compete with each other for limited bandwidth. We expect this suboptimal arrangement to only get worse, particularly in the dense urban environments that house an increasing fraction of the world's population. Broadband penetration and the demand for high-speed Wifi throughout the home will lead to more private APs, which will generate more interference for neighboring networks, resulting in even more private APs and additional interference, and so on.

In this paper we investigate whether we can prevent this vicious cycle by using *reciprocal Wifi sharing* to make better use of existing private home APs. We define reciprocal Wifi sharing as cases where two users both improve their network performance by connecting to each other's overlapping private Wifi networks. Compared to previous approaches that attempted to use private APs to create large-scale open-access Wifi networks, reciprocal Wifi sharing relationships more closely mirror existing human relationships and can be maintained without elaborate reputation mechanisms.

To evaluate the potential for reciprocal Wifi sharing, we analyze 21 M Wifi scans collected from 254 smartphones over 5 months. Our results show that even in a sparsely-populated suburban area, reciprocal Wifi sharing can be beneficial. And surprisingly, we detected several reciprocal Wifi sharing opportunities even within our tiny user sample. Motivated by these results, we present the design of WISEFI, a system enabling reciprocal Wifi sharing.

1. INTRODUCTION

Two trends are combining to create increasingly crowded and uncoordinated home Wifi environments. First, increasing broadband penetration is creating larger numbers of private home access points (APs). Strategy Analytics estimated that by the end of 2014, 451 M households worldwide (25%) would have home Wifi and that this number will continue to grow [7]. Second, an increasing percentage of the world's population resides in dense urban environments: 54% today and climbing to 66% by 2050 [6]. Together these two trends create a future where more people will operate private home APs that overlap with other nearby private home APs.

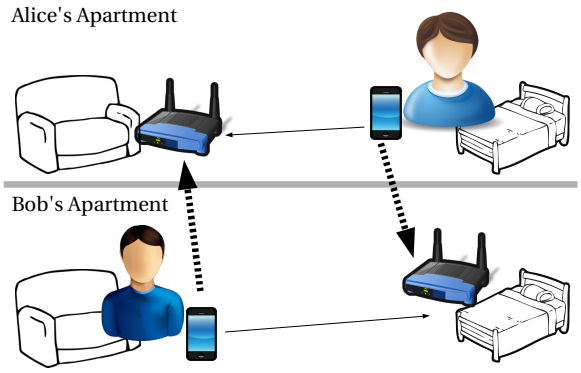


Figure 1: **Example of Reciprocal Wifi Sharing.** Solid arrows represent weak connections, while dashed lines represent strong connections.

Unfortunately, uncoordinated deployment of overlapping private networks can create interference that degrades performance, which may then cause users to respond in ways that further exacerbate the problem. Consider Alice's/Bob's apartment shown in Figure 1. Alice/Bob has deployed her/his AP in her/his living room/bedroom. Due to the proximity of their apartments, Alice/Bob receives a stronger signal from Bob's/Alice's router when she/he is in her/his bedroom/living room. But because Alice/Bob cannot connect to Bob's/Alice's router, she/he must either use the lower-bandwidth connection to her/his existing AP or deploy an additional AP in her/his bedroom/living room. Both options generate additional wireless interference for her/his neighbors, including Bob/Alice.

Ideally, Alice/Bob would allow Bob/Alice to use her/his router. Obviously this solution requires less hardware. But it also improves performance while reducing interference and client energy consumption, both by allowing the APs to coordinate overlapping transmissions and by allowing clients to achieve higher bitrates at lower transmission powers. We refer to this mutually-beneficial arrangement as *reciprocal Wifi sharing*.

Reciprocal Wifi sharing has benefits compared to attempts to use private APs to establish community networks such as FON [1] or OpenWireless [2]. Reciprocal Wifi sharing opportunities are more likely to align with existing human relationships, such as this example involving two neighbors, rather than requiring users to open their private networks to strangers. And because reciprocal Wifi sharing involves only pairwise cooperation, agreements can be established and monitored without the elaborate reputation systems or credit mechanisms required to prevent freeloading in large communities. Once Alice notices that the sharing agreement with Bob is no longer beneficial—either because she no longer needs his connection or because he is degrading her service to the point where it is no longer useful—she can immediately terminate it.

Begin	11/7/2014
End	4/3/2015
Duration (Days)	147
Participants	254
Device Type	Nexus 5
Scans	21,192,417
Observed APs	1,197,522
Used APs	15,668
Wifi Sessions	466,032

Table 1: **PHONELAB Wifi Dataset Summary.** Used APs refers to the subset of total APs that were used by the devices participating in the study.

But how often is reciprocal Wifi sharing beneficial and possible in practice? To explore these questions, we begin in Section 2 by analyzing a dataset collected on the PHONELAB smartphone testbed containing 21,192,417 Wifi scan results from 254 smartphones over 5 months. Despite the fact that the geographic extent of the dataset is suburban Buffalo, which as a city has a population density an order of magnitude lower than densely-populated areas like Manhattan, we still find that many users would benefit from being able to connect to neighboring private networks. Even more surprisingly, despite monitoring only several hundred users we were still able to identify several reciprocal Wifi sharing opportunities in our tiny sample. Motivated by these results Section 3 presents the design of WISEFI, a system addressing the practical challenges of establishing and monitoring reciprocal Wifi sharing agreements. We conclude by identifying some open challenges in implementing such a system as future work in Section 4.

2. INVESTIGATION

To investigate reciprocal sharing opportunity in real life scenarios, we obtained a Wifi scan result dataset from PHONELAB[1] (§2.1). We first discuss some heuristics to identify the home AP for each device (§2.2). Then we show the RSSI comparison between a user's home and neighbor APs (§2.3). Finally, we explore the reciprocal sharing relationships in the dataset (§2.4).

2.1 PhoneLab Wifi Dataset

PHONELAB[5] is a public smartphone platform testbed operated at the University at Buffalo. Several hundreds of participants carry instrumented Nexus 5 smartphones as their primary device. In particular, the smartphone platform was modified to log each Wifi scan result and Wifi connection events naturally generated by the Android system. Note that from data collection point of view, platform instrumentation is not necessary, and the same information can also be logged by applications with appropriate permissions. A Wifi scan result represents the device's network visibility, and consists of multiple entries—each corresponds to one Wifi AP the device observed. The content of one entry includes: (1) beacon timestamp, (2) AP SSID and BSSID, (3) AP channel and (4) RSSI. The timestamp when the scan was performed is also logged. Table 1 summarizes the PHONELAB Wifi dataset.

2.2 Home AP Detection

We focus on home Wifi networks which are more likely to reveal stable and immediate reciprocal sharing opportunities. For this purpose, we first developed several heuristics to identify the home AP for each device in the dataset. The intuition is that the devices are most likely connected to their home AP at night. More specifically, to identify the home AP for a device, we look at Wifi sessions that happened during 12 AM and 4 AM and count the number of days that the device connects to each AP during this time period. We then identify the AP which has the largest day count as the device's home AP, provided that the day count is larger than a threshold (30 days) to further filter out false positives.

After applying the above heuristics, the home AP information of 107 devices are identified, including 101 unique BSSIDs. There are 6 BSSIDs that are identified as home APs for two devices. After further investigation and clarification with PHONELAB administrators, we found this is because some participants are family members, and certain participants had device replacements during the data collection period. In both cases, multiple devices may be associated with the same home AP.

[1] http://www.phone-lab.org

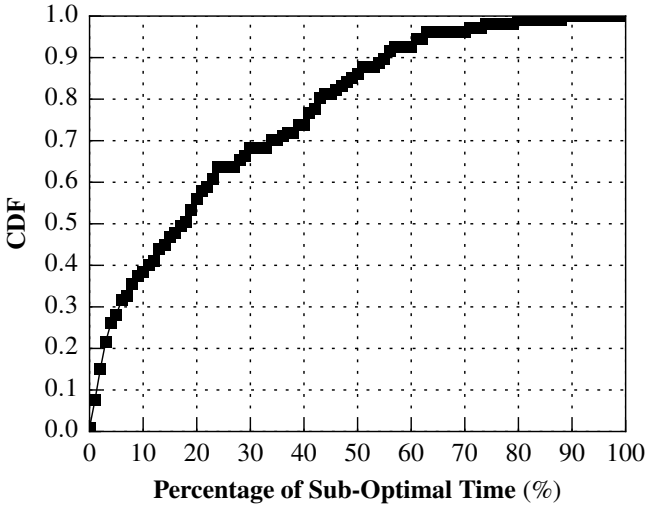


Figure 2: **CDF of Sub-Optimal Connection Time.**

2.3 Wifi Session Signal Strength

After identifying the home AP for each device, we ask two questions: (1) When the device is connected to its home AP, how often does it receive a better signal from neighbors' APs which it does not have access to? and (2) When the home AP fails to provide the best signal, are there dominant neighbor APs that provide better signal most of the time?

To answer the first question, we inspect scan results that are reported during Wifi sessions with home APs. For each such scan result, we identify the currently associated home AP, AP_{home}, and the AP with best RSSI, denoted as AP_{best}. We are particularly interested in *sub-optimal* cases, where: (1) $AP_{home} \neq AP_{best}$ and (2) the device never connects to AP_{best} in the dataset. Such cases indicate that the device could potentially improve its Wifi performance by connecting to a neighbor AP which has a strong signal yet it does not have access to that AP. Note that here we consider RSSI as a hint in determining the *optimal* AP and it is well understood that RSSI does not directly translate to Wifi performance, which we will discuss in Section 3.3. Also note that the cases when the device is not connected to APs with the strongest signal due to bad roaming strategies are not interesting in the context of this paper, and are excluded by the second condition.

We classify all scan results reported during home Wifi sessions into two categories: sub-optimal and the rest. For each device, we calculate the percentage of time when the scan results indicate sub-optimal association. Figure 2 shows the CDF of this percentage for the 107 devices. We make several observations. First, for 60%

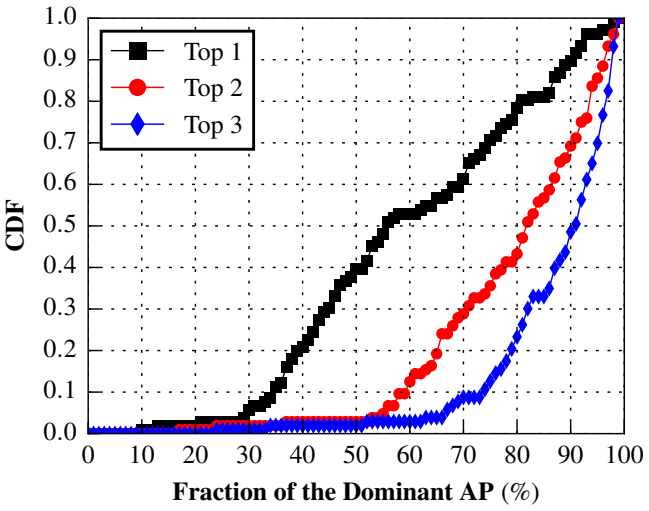


Figure 3: **CDF of Dominant AP Fraction.**

of the devices, their home APs usually provides best signal (sub-optimal percentage less than 20%). This result is not particularly surprising considering that home APs are usually carefully positioned to provide good coverage. Second, we notice that for certain number (15%) of devices, their home APs failed to provide best signal for more than 50% of the time, suggesting that these users may benefit from sharing the Wifi access of neighbor APs.

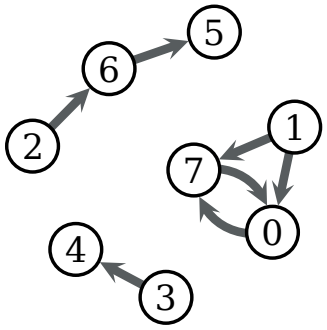
Next, we want to answer the question when the device is in a sub-optimal association with its home AP, are there *dominant* neighbor APs that usually provide the best signal among other neighbor APs? If such dominant neighbor APs exist, then by just sharing access of several particular neighbor APs, the device's sub-optimal association time can be largely reduced. To this end, we look at all the scan results in the sub-optimal category, and count the number of times that each neighbor AP appears as AP_{best}. For each device, we calculate the fraction of the top $n(1 \leq n \leq 3)$ dominant neighbor APs. Figure 3 shows the CDF of dominant AP fraction. By sharing 1, 2 or 3 neighbor APs, half the device's sub-optimal connection time can be reduced by 55%, 82% and 90% respectively.

2.4 Reciprocal Sharing Opportunities

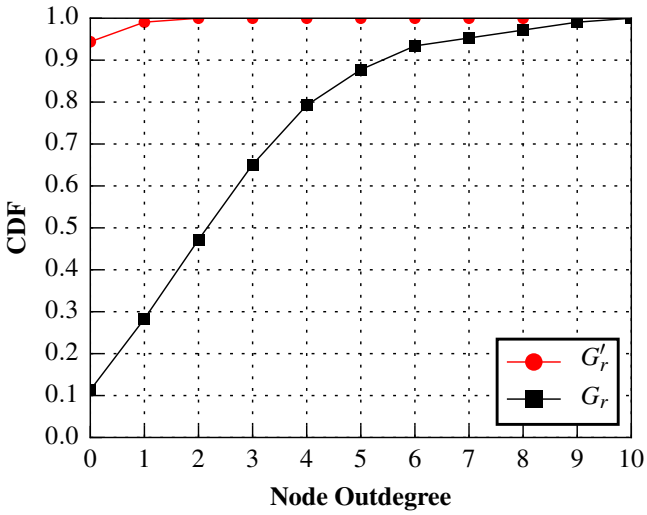
Finally, we investigate the cases where two devices can obtain better signals from each other's home AP, i.e., reciprocal sharing opportunities. For this purpose, we build a reciprocal sharing graph $G_r = (V, E)$, where V is the set of APs, and $\langle AP_i \rightarrow AP_j \rangle \in E$ if AP_i's clients receive better signal from AP_j, that is, AP_j appears as AP_{best} in the scan results of AP_i's clients. Note that according to the definition, AP_i is one of the identified home APs, while AP_j could be other arbitrary APs. Loops in G_r represent reciprocal sharing opportunities.

To capture the reciprocal sharing relationships among PHONELAB participants, we further construct a subgraph of G_r, $G'_r = (V', E')$, where $\langle AP_i \rightarrow AP_j \rangle \in E'$ only if both AP_i and AP_j are identified home APs of PHONELAB participants. Figure 4a visualize G'_r, where nodes without outgoing edges are omitted for clarity. Sharing opportunities are sparse but exist. In particular, we observe one pair of home APs, node 0 and 7, which exhibit reciprocal sharing relationships.

We must point out that PHONELAB participants reside sparsely among the vast Buffalo area, and the above analysis is further restricted to those participants that we can detect their home APs using heuristics described Section 2.2. The consequence of such sparsity is that most of the neighbor APs which can provide better



(a) **Reciprocal Sharing Graph Among PhoneLab Participants.**



(b) **CDF of Node Outdegree in Reciprocal Sharing Graph.** Only outdegrees of identified PHONELAB home APs are counted.

signal are not one of the identified home APs, thus are not shown in Figure 4a. To quantify the spatial sparsity, Figure 4b shows the CDF of node outdegree in G_r and G'_r. While the median node outdegree in G_r is 2, 95% of nodes in G'_r has no outgoing edges. The fact that reciprocal sharing opportunities exist at all in such a sparse dataset is quite surprising, and motivates the need for a system to detect and enable such reciprocal Wifi sharing.

3. SYSTEM DESIGN

Inspired by the results of the investigation in Section 2, we design a system called WISEFI to detect reciprocal sharing opportunities (§3.1), enable Wifi sharing (§3.2) and monitor the Wifi performance to ensure the sharing remains reciprocal (§3.3). Figure 5 shows the overall work flow of the WISEFI system.

3.1 Detection

To detect reciprocal sharing opportunities, two information are required: the home AP of the device, and neighbor APs' signal strength during Wifi sessions with the home AP. A smartphone application can be deployed through app market to collect these information. In particular, the home AP information can be learned over a period of time using the heuristics developed in Section 2.2, or be inputted directly by user. Once the home AP information is identified, Wifi scan results during sessions with home APs can then be logged to identify the neighbor APs that can potentially provide better network performance. Finally, these information are uploaded and fused in WISEFI server to identify reciprocal sharing opportunities using the methods described in Section 2.4.

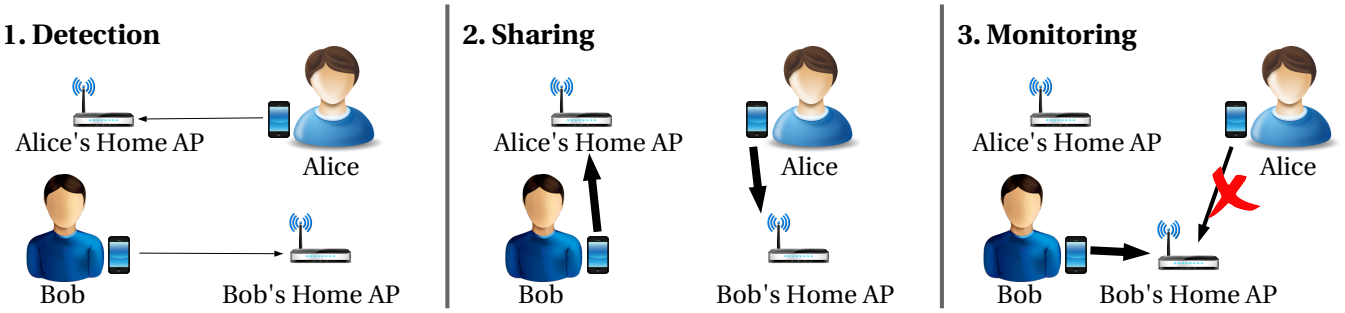


Figure 5: **WISEFI System Work Flow.** (1) Reciprocal sharing opportunities are detected by WISEFI smartphone apps; (2) Wifi sharing is enabled through coordination of WISEFI server; (3) Wifi usage and performance are monitored by WISEFI app to ensure the sharing remains reciprocal.

3.2 Sharing

Once the reciprocal sharing opportunities are discovered, the WISEFI server distributes such information to the WISEFI application on smartphone, which prompts user to establish Wifi sharing. The sharing mechanism must meet two goals: *control* and *protection*. First, the system should be able to control the sharing, including granting the access of home AP to other WISEFI users, and more importantly, revoking the access when needed. Second, the system should protect the home network from other WISEFI users by sharing access only to the Internet, and protecting private resources such as home network printers or storage.

Some mid-to-high end wireless routers support the *virtual network* feature, where multiple virtual Wifi networks are emulated by a single router hardware, and different network parameters, such as SSID, bandwidth cap, access permission, can be enforced separately for each virtual network. This feature is typically used to set up a guest Wifi network to provide network access to temporal visitors yet isolate them from home clients. For home APs with such feature, Wifi sharing can be achieved by only distributing the credential of guest network to other WISEFI users. Access and bandwidth policies can then be enforced on the guest network to achieve control and protection. Additionally, such isolation and enforcements are mostly likely already enabled by default for guest networks, so that even inexperienced user can configure the Wifi sharing through guest network.

For APs without guest network feature, however, cumbersome AP configurations may be required by user, such as MAC black or white list, routing table modification, etc. Such configurations are most likely too complicated for average users to perform. However, simply sharing the Wifi credential of user's home AP to other WISEFI users is not only dangerous, but also making it difficult to revoke the access in the future. In worst case scenario, a user may be forced to change the home AP password and reconfigure the Wifi credential on all his/her devices just to revoke the access of the other WISEFI user. Although most commodity APs support client MAC black or white list feature, configuring them properly is difficult for average users. Furthermore, the sharing relationship should be built between users instead of devices: once the sharing is established, one user should be able to connect any of his/her devices, not only the smartphone, to the other user's home AP. Even the system can directly share each other's Wifi credential, manually configuring it on all devices is still tedious.

To overcome this challenge, we propose a dynamic Wifi AP configuration API with two simple interfaces: `getAuthClients` and `setWhiteList`. The semantics of the interfaces are as follows. `getAuthClients` returns all the MAC addresses of clients that are currently associated with the AP through normal authentication. In home Wifi network scenario, this interface shall return only the MAC addresses of user's own Wifi devices. On other hand, `setWhiteList` sets a list of white list MAC addresses that the AP should accept their association requests regardless of possible authentication errors (e.g., due to incorrect Wifi password). Finally, these requests will only be accepted by the AP when they are sent by devices that are associated through authentication, not through white list. The API can be implemented on top of existing SNMP protocols, or be provided in form of RESTful API through the HTTP server that is already integrated in most commodity APs.

With the help of these configuration APIs, the Wifi sharing process can work as follows. Suppose the WISEFI system has discovered the reciprocal sharing opportunity between Alice and Bob, here are the steps to grant Bob's device to Alice's home AP. First, the WISEFI app on Bob's smartphone (which is associated with Bob's home AP through proper authentication) sends a `getAuthClients` request to Bob's home AP, retrieving the MAC addresses of all Bob's devices. These MAC addresses are uploaded to WISEFI server and then forwarded to the WISEFI app on Alice's smartphone, which sends a `setWhiteList` request to Alice's home AP to add all Bob's devices to its white list. At this point, Bob can connect his any of his devices to Alice's home AP using a dummy password[2]. Later on, when the reciprocal sharing opportunity no long exists, the WISEFI server instructs Alice's smartphone to perform another `setWhiteList` request to revoke Bob's access to Alice's home AP by removing the MAC addresses of Bob's devices from the white list.

There are several advantages of this sharing approach. First, note that throughout the grant and revoke process, the Wifi credential of Alice's home AP is not shared with Bob or the WISEFI server, thus remains confidential. Second, revoking access of other WISEFI users simply requires a `setWhiteList` request, without needing to change the user's home AP password. Furthermore, the WISEFI app can list other WISEFI users who are in a reciprocal sharing relationship and provide interfaces to let user manually revoke access of other users if needed. Finally, this mechanism does not require modifications of Wifi clients (except for installation of WISEFI app) and only requires software updates at AP side, making it easy to deploy. Once the sharing is established, protection and isolation can be enforced at the AP side by differentiating two type of clients: authenticated clients (user's own devices) and while list clients (WISEFI devices). Therefore, such sharing mechanism meets both the control and protection goals.

[2]Here we assume all Bob's devices are associated with Bob's home AP when the `getAuthClients` is sent. In practice, the grant process could be repeated several times to gradually including all Bob's devices.

3.3 Monitoring

After the sharing is established, the system needs to monitor both Wifi *usage* and *performance* of both parties to ensure that the sharing remains reciprocal. There are two reasons why this is necessary: one is obvious and another is obscure.

First, it is obviously important to ensure that the sharing remains reciprocal to provide incentives for both parties to participate the sharing. For instance, suppose after the system has established reciprocal Wifi sharing between Alice and Bob, and Bob decides to deploy an extra AP at his home which makes him no longer benefit from sharing Alice's home AP. The system should monitor Bob's Wifi usage to detect the termination of the reciprocal relationship and revoke Alice's access of Bob's home AP accordingly.

Second, the not so obvious reason is that, as mentioned in Section 2.3, Wifi signal strength is used as a hint to identify potentially better APs. And it is well known that signal strength does not directly translate to Wifi performance. Other factors, such as AP load, modulation, interference, or Wifi generation, also affect the link quality yet can not be easily detected by the smartphone. Furthermore, last hop Wifi link quality does not necessarily determines clients' overall end-to-end network performance. In fact, there is no way to predict whether the neighbor AP can indeed provide better network performance than user's home AP until the sharing is actually established.

To measure the reciprocity in terms of network performance, standard performance benchmarks, such as download/upload throughput, `ping` latency, or DNS lookup, can be performed periodically by the WISEFI client. However, it is not trivial to monitor the network usage aspect of reciprocity from the vantage point of a single client: the smartphone's association time may not be representative of user's other wireless devices. For this purpose, we argument the AP configuration API proposed in Section 3.2 with one new interface, `getWhiteListClents`, which returns the MAC addresses of clients that associated with the AP through white list mechanism. These are the clients of other WISEFI users that actively use the home AP. The WISEFI app can then periodically issue `getWhiteListClents` requests to measure the sharing usage of other WISEFI users to ensure reciprocity.

4. OPEN QUESTIONS

Enabling Wifi sharing between neighbors both touches known open issues of cooperative Wifi access and brings new challenges.

As discussed in Section 3.2, user's privacy and security can be preserved through isolating either at network level (virtual networks) or client level (white list vs. authenticated clients). However, it is still an open question that whether or to what extent the user is liable to the illegal actions, most notably copyright infringement, of the peers who share the network.

Another challenge in establishing reciprocal Wifi sharing is the bootstrap process. It is expected that during early stages of deployment, the sharing opportunity will be sparse. Therefore, It is important to provide additional incentives other than the benefit of Wifi sharing to increase the penetration of system. One possible feature that can be added to the WISEFI app is to help the user find better Wifi channels for their own APs. Uses who are willing to install the app for this feature are more likely not satisfied with their Wifi performance and thus have the desire of improve their network experience by joining the reciprocal sharing relationship.

Finally, the immediate and stable sharing relationship brings new challenges to traditional reputation or credit based peer to peer sharing mechanisms, most of which are developed under the assumption that peers are strangers and the mutual beneficial relationship is transient. For instance, the fairness metric of the sharing may need to be considered over a longer time window.

5. RELATED WORKS

OpenWireless movement [2] is a community effort for ubiquitous Internet access. Volunteers configure their Wifi network with open access and a special SSID, `openwireless.org`, to advertise free access. Another goal of OpenWireless is arguably preserving user's privacy by blending the user's network activity among all other users who share access to the open Wifi network. On other hand, FON [1] is a commercial Wifi sharing network, where registered users can roam over FON-supported Wifi networks. WLAN owners share their Wifi network either for small money compensation, or to get Wifi access to other users when they are way from home (roaming). FON aims at providing global Wifi sharing community where users want to connect to others' Wifi network because they are way from home and have no WLAN access.

Both OpenWireless and FON aim at sharing Wifi access between strangers either through volunteering or financial incentives. Whereas in our proposal, users share Wifi network locally (within neighbors) for better network performance, and the sharing relationship is immediate (between two parties) and stable (physical neighbor relationship).

There are also rich literature on cooperative Wifi sharing. Dimopoulos *et al.* [4] propose a reciprocal Wifi sharing mechanism and later extend it to a large scale peer-to-peer Wifi roaming framework [3]. They mostly focus on the reciprocal manner of sharing: each user who share his/her WLAN will obtain digital proof service (*receipts*), which represent a "I-owe-you" relationship. These receipts can later on be consumed to get reciprocal Wifi access from other users. Such reputation mechanisms can also be applied to WISEFI, although they can be simplified since the sharing is between two immediate peers with physical colocation relationship.

6. CONCLUSIONS

To conclude, we explore the reciprocal sharing opportunities through extensive analysis of the PHONELAB Wifi dataset, and show that such opportunity does exist despite the spatial sparsity. Inspired by the analysis results, we present the design of WISEFI, a system that detects reciprocal sharing opportunities, enable Wifi sharing and monitor the Wifi usage and performance to ensure the sharing remains reciprocal.

We are currently implementing a WISEFI system prototype, which includes a WISEFI Android application, dynamic AP configuration API support on OpenWRT router platform, and WISEFI server powered by Django.

7. REFERENCES

[1] FON Wireless. Ltd. `https://corp.fon.com/en`.

[2] Open Wireless Movement. `https://openwireless.org/`.

[3] E. G. Dimopoulos, P. A. Frangoudis, and G. C. Polyzos. Exploiting super peers for large-scale peer-to-peer wi-fi roaming. In GLOBECOM Workshops (GC Wkshps), 2010 IEEE, pages 1990–1994. IEEE, 2010.

[4] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos. Controlled wi-fi sharing in cities: A decentralized approach relying on indirect reciprocity. Mobile Computing, IEEE Transactions on, 9(8):1147–1160, 2010.

[5] A. Nandugudi, A. Maiti, T. Ki, F. Bulut, M. Demirbas, T. Kosar, C. Qiao, S. Y. Ko, and G. Challen. Phonelab: A large programmable smartphone testbed. In Proc. 1st International Workshop on Sensing and Big Data Mining (SenseMine 2013), November 2013.

[6] U. Nations. World urbanization prospects. `http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf`.

[7] Strategy Analytics. Global broadband and wlan (wi-fi) networked households forecast 2009-2018. `https://goo.gl/IUKVfD`.