Collaborative Municipal Wi-Fi Networks - Challenges and Opportunities

Tobias Heer, René Hummen, Nicolai Viol, Hanno Wirtz, Stefan Götz, Klaus Wehrle
RWTH Aachen University
Distributed Systems Group
Aachen, Germany
{heer, hummen, viol, wirtz, goetz, wehrle}@cs.rwth-aachen.de

Abstract—**Municipal Wi-Fi networks aim at providing Internet access and selected mobile network services to citizens, travelers, and civil servants. The goals of these networks are to bridge the digital divide, stimulate innovation, support economic growth, and increase city operations efficiency.**

While establishing such urban networks is financially challenging for municipalities, Wi-Fi-sharing communities accomplish good coverage and ubiquitous Internet access by capitalizing on the dense deployment of private access points in urban residential areas. By combining Wi-Fi communities and municipal Wi-Fi, a collaborative municipal Wi-Fi system promises cheap and ubiquitous access to mobile city services. However, the differences in intent, philosophy, and technical realization between community and municipal Wi-Fi networks prevent a straight-forward combination of both approaches. In this paper, we highlight the conceptual and technical challenges that need to be solved to create *collaborative* municipal Wi-Fi networks.

I. Introduction

The technological advance in wireless communication technology allowed for the creation of almost ubiquitous city-wide broadband networks. Many communities all over the world are trying to leverage these developments and install municipal Wi-Fi (Muni-Fi) networks (In January 2008, *http://www.muniwireless.com/* reported 395 planned and completed Muni-Fi projects in the US alone.) Their goals include ubiquitous Internet access, localized services (e.g., city and event guides, traffic information, etc.), and simplified data collection (e.g., traffic monitoring and meter reading). It is hoped that these goals help bridging the digital divide, stimulate innovation, support economic growth, and increase city operations efficiency [1].

However, the cost of deploying and operating such networks has hampered or prevented their proliferation in many cases. Even previously highly successful Muni-Fi deployments are facing serious financial problems. A recent example is the free public Wi-Fi network in St. Cloud, Florida [2]. Despite its great public success and its high popularity, the network that initially cost USD 2.6 million was shut down to annually save USD 600.000 in costs of operation. But not only small Muni-Fi networks are struggling with financing: prestigious projects like the *Wireless Philadelphia* project [3] have to undergo deep structural changes in order to reduce deployment and maintenance costs and to stay operational and economically attractive.

As an alternative, Wi-Fi sharing communities have evolved in many cities and represent a more cost-effective approach for providing wireless access, as the financial burden is split among all members. Its concept emerged from grass-root movements such as Freifunk [4] and was later adopted by companies such as FON [5] and Elisa (Wippies community) [6]. The members of a Wi-Fi sharing community provide Internet access to each other via their privately owned Wi-Fi access points (APs), thereby creating a widely-distributed Wi-Fi access network. Thus, the whole Wi-Fi network infrastructure is provided, operated, and maintained by the community members.

Although there are certain similarities between Wi-Fi communities and municipal Wi-Fi (both provide Wi-Fi in urban areas), the intent, philosophy, and technical realization of these networks differ. The main difference is that Wi-Fi communities provide wireless access in an unplanned and non-orchestrated way. Consequently, such networks have varying characteristics regarding coverage, range of an access point, availability, and performance. Moreover, fundamental goals of established Muni-Fi networks, such as bridging the digital divide or reliably supporting civil servants, are more difficult to reach or become even impossible to achieve because of these varying characteristics.

In this paper we highlight the opportunities and challenges that collaborative Muni-Fi networks yield from a conceptual and technological point of view. In Section II, we first discuss the roles and structures in Wi-Fi communities and Muni-Fis in more detail. Section III addresses the real-world properties of Wi-Fi networking. Based on these results, Section IV elaborates on how a collaborative approach fits the goals and uses of Muni-Fis. The main technical challenges of a collaborative Muni-Fi system and possible solutions are discussed in Section V and Section VI concludes.

II. Municipal Wi-Fi Networks

A Muni-Fi network consists of three logical entities: a wireless access provider, a local service provider, and the

This work is supported by the Ziel2.NRW program and the ERDF fund of the European Union.

users. Depending on the actual network architecture, some of these logical entities may fall into the responsibility of a single physical entity. Before proceeding to *collaborative* municipal networks, we introduce these entities and discuss possible forms of operation for city-wide and municipal networks.

Wireless Access Provider: A wireless access provider (WAP) offers its existing uplink to the city-wide network to nomadic users. The WAP can be a company, a non-profit organization, or a private person sharing a Wi-Fi access point at home.

Local Service Provider: A local service provider (LSP) offers services (possibly with local scope) in the Muni-Fi network. Services can be WWW-like content and information services as well as communication services. An LSP may be identical to a WAP when the network merely provides Internet access as a service. LSPs can be the city administration or companies providing pedestrian navigation, tourist guides, or internal services to city workers.

Users: Users access the services provided by the LSP via the Wi-Fi infrastructure provided by the WAP. A user can be a person (e.g., a tourists, accessing information through their PDA) or an automated end-system (e.g., a traffic sign that retrieves information from a traffic control system).

These three logical roles can be distributed among any number of entities. In special-purpose Muni-Fis, the municipality can even inherit all roles (e.g., for Wi-Fi networks that are solely built for supporting civil servants).

A. Forms of Organization

City-wide Wi-Fi networks can be categorized by the interplay of the entities that build and maintain the wireless infrastructure as well as the back-end for municipal services. We discuss three forms of organization that differ in their technical realizations and characteristics: municipality-driven, provider-driven, and user-driven. Any combination of the above models is possible, i.e., municipality-driven networks with provider or user contribution. The collaboration between the parties can be at the WAP or the LSP level (horizontal separation) or it may be divided vertically so that one entity focuses on the wireless access, whereas another group focuses on services. Figure 1 shows how seven popular large-scale Wi-Fi and Muni-Fi networks and two concepts for collaborative Wi-Fi networks can be positioned between the three driving forces.

1) Municipality-driven Networks: When a city administration plans, commissions, and runs a wireless network, its usual intent is to provide wireless access to city staff, citizens, or tourists in certain areas. Examples for municipality-driven networks are Paris Wi-Fi [7] and the Cyber Spot network in St. Cloud [2]. In these networks, the interests of the municipality are the main driving force.

A municipality may reduce the deployment costs by contracting an Internet service provider to install and maintain the required infrastructure or by co-operating with and advertising an existing WAP. Hence, the distinction between a municipality-driven network and a provider-driven network is not always clear. An example for such a combination is panOulu [8], a joint project of four ISPs and the city administration aiming to provide free Wi-Fi access.

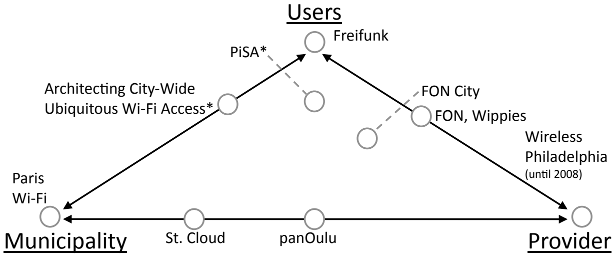

Figure 1. Organization of large-scale Wi-Fi networks. Concepts without deployment are marked with an asterisk.

2) Provider-driven Networks: Provider-initiated large-scale Wi-Fi networks may also serve the municipality and the citizens. However, the interest and business model of the provider often contradicts open competition at the Wi-Fi access and service level. Wireless Philadelphia, as originally initiated by Earthlink, is one of the most prominent examples for a provider-driven Muni-Fi, although the free Wi-Fi program was discontinued in May 2008. The project was financed and deployed by Earthlink [9], giving the company tight control over the network and the provided services.

3) User-driven Networks: In a user-driven Wi-Fi network, private users form a *Wi-Fi community* in which they share their broadband Internet access. Each member is responsible for and maintains its own AP, providing access for other community members as a WAP of the network.

The main advantage of this approach is the reduction of the deployment cost as well as of the cost of operation. Users install access points in their own homes and use their existing mains and Internet connection, obsoleting cost for wiring outdoor public access points. Moreover, the expenses for electricity and Internet access are paid by the AP owner, which limits the expenses of a Wi-Fi community to the cost of providing the authentication and service infrastructure.

The main drawbacks of user-driven networks are the sparse deployment of access points in sparsely populated areas and a lack of security (with regard to privacy and accountability) when using a community member's AP. The Freifunk initiative [4] is an example for a purely user-driven Wi-Fi network based on 802.11 mesh technology.

Combinations of user-driven and provider-driven models are also possible. FON [5], FON-City [10], and Wippies [6] follow a user-oriented concept in which users deploy and operate Wi-Fi access points, providing the Internet up-link via their existing wired connection. However, the companies behind these community networks use a provider overlay to control the access to the wireless network. The provider manages and controls all Wi-Fi access-related aspects of the network (i.e., user management, access control, and billing), giving it a position similar to an ordinary wireless Internet service provider. FON-City also involves the municipality. However, its role is limited to supplying the citizens with access points and providing Wi-Fi access in areas that are not covered by user APs.

In Figure 1, we also included two technical concepts that are not currently deployed. The Peer-to-peer Internet Sharing Architecture PiSA [11] and the work by Sastry et al. [12] allow for secure mobile Internet access without a dedicated Wi-Fi access provider by using tunnels. These tunnels form a virtual Muni-Fi network on top of any existing infrastructure. Without direct involvement of providers, the approaches can serve as an open platform for any service.

In contrast to the other provider-driven approaches, Wi-Fi communities must overcome a initial obstacle before they can be successful: The benefit to early adopters is small because the user-base and coverage is low. Hence, the community only becomes attractive to a wider audience after it reaches a critical mass of contributors.

B. From Wi-Fi Communities to Collaborative Muni-Fi

As discussed above, different forms of organization are possible when establishing large-scale city-wide Wi-Fi and Muni-Fi networks.

The term municipal Wi-Fi network is not clearly defined in literature. A common consensus is that a municipality is involved in some form [1]. This involvement ranges from a municipality purely advertising an existing Wi-Fi network to building and autonomously maintaining a Wi-Fi infrastructure and its related services. Furthermore, authors often use the terms *municipal Wi-Fi (Muni-Fi)* and *city-wide Wi-Fi network* interchangeably. However, a distinction between these two terms is useful and necessary for the discussion of the concepts and properties of Muni-Fi networks due to their different scopes.

The sole aim of a city-wide Wi-Fi network is to provide (ubiquitous) Internet access to a restricted group of users. Additional services specific to the network typically have a subsidiary role and should generate further incentives for the user to use the offered bandwidth. Examples for this category of Wi-Fi networks are Sonera Homerun [13] as an ISP-based Wi-Fi network and Freifunk [4] as a Wi-Fi sharing community.

In contrast to city-wide Wi-Fi networks, we speak of a municipal Wi-Fi network when the network infrastructure and the accessible services or applications therein pursue a public interest. These interests include publicly available services that are closely related to the network's location (e.g., electronic tourist guides or digital ordering in a cafe) or governmental applications facilitating the network as a communication infrastructure for municipal staff and in public facilities. These local services are the essence of why the Wi-Fi network is built and maintained in the first place. Hence, when referring to Muni-Fi networks, we address such a combination of wireless network access and local-scope services with a focus on the public interest. This definition is similar to the definition of *community network* in [9], however, we do not stress the economic aspect of the network because collaborative approaches often lack the business aspects.

As discussed in Section II-A3, user-provided Wi-Fi can reduce the financial challenges in establishing and operating a municipal Wi-Fi network. We use the term collaborative municipal Wi-Fi for a Muni-Fi in which users contribute to the network infrastructure or local services. Collaborative Muni-Fis can be seen as a combination of community Wi-Fi sharing networks and Muni-Fi networks. In contrast to pure Wi-Fi sharing communities, collaborative Muni-Fis put a stronger emphasis on providing a set of services that is characteristic for Muni-Fi networks.

III. Harnessing Unused Wi-Fi Resources

Wi-Fi access points in community Wi-Fi sharing models are typically placed inside buildings. Positioned to primarily serve the needs of their owner, the outdoor coverage of such APs is typically lower than the coverage of dedicated outdoor access points.

Thus, compared to a well-structured, professionally deployed and maintained network infrastructure, collaborative networks exhibit the following properties:

- Reduced or insufficient coverage in certain city districts because of an unplanned deployment of APs.
- Lower availability and reliability because the hardware is operated by users who may (accidentally) unplug a wireless router from its power or Internet link.
- Largely varying latency and throughput as well as small range because of suboptimal indoor placement of Wi-Fi access points.

Good Wi-Fi coverage is mandatory to provide mobile users with ubiquitous connectivity. This raises the question if a user-driven network is sufficient to provide city-wide outdoor Wi-Fi in urban areas. Without an existing collaborative Muni-Fi network, the answer to this question can only be an educated guess. However, the actual coverage in a city with private Wi-Fi access points gives an estimate of an ideal case in which all citizens are part of the community.

We conducted a war-walking measurement in the inner city of Aachen to estimate the feasibility of a collaborative approach under optimal conditions. We used consumer hardware to measure the possible coverage and range of Wi-Fi access points to reproduce the situation of a mobile user in the streets. During the measurement, we walked the streets just as a typical user would, stopping at crossings and taking turns every now and then. A visual trace of our route is available on our website [14].

Our test hardware is a notebook equipped with two Zydas zd1211 Wi-Fi USB device and a Sirf Star III GPS receiver.

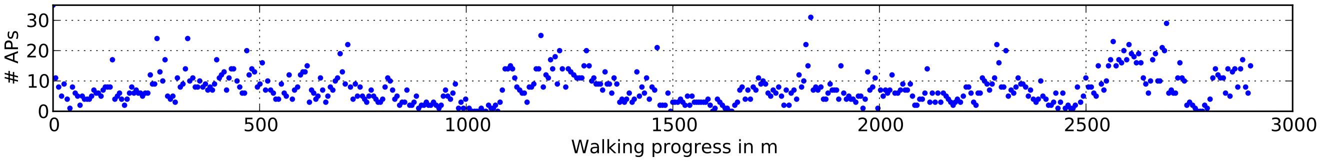

Figure 2. Number of visible APs per logical data point along a track of 2,898 m.

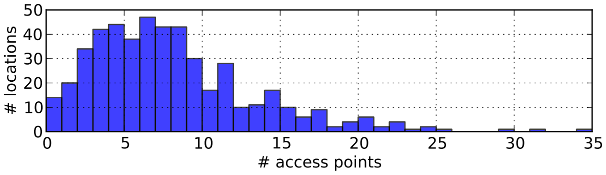

Figure 3. Histogram of the AP density for 580 locations.

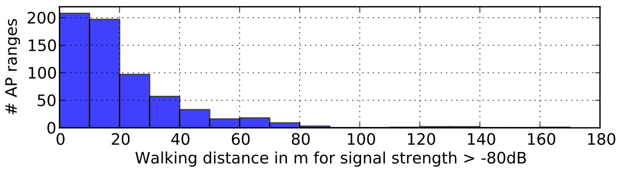

Figure 4. Distribution of the street-level walking distance for 882 discovered APs (signal strength ≥ -80 db).

We measured the signal strength of the AP beacons and the GPS position along the main streets around the city center. Similar to the behavior of an ordinary device, we cycled the frequencies in the 802.11 2.4Ghz band. To counter GPS jitter and irregularities caused by the frequency cycling, we aggregated all measurements within a range of 5 meters to a single logical data point.

In total, we observed 2,695 distinct access points during our 3 km walk. However, since we are only interested in Wi-Fi links of acceptable signal strength, we discarded all results with a signal strength below -80 dB, leaving us with 882 APs along the track. Figure 2 shows the number of access points per logical data point on the track and Figure 3 shows a histogram of the same results. About 97% of the track were covered by at least one access point, whereas 68% were covered by at least five access points. Figure 2 also shows 18 peaks with more than 20 access points. These peaks represent crossings and the market square, showing that Wi-Fi penetration is particularly high in places that are expected to be visited by many users. Overall, the results suggest that ubiquitous connectivity is possible with a collaborative approach, provided that the community can reach a sufficient number of users.

Besides total coverage, the range of the access points is an important factor for the perceived quality of service. Although range and coverage are closely related (higher range obviously leads to better coverage), taking into account only coverage neglects the needs of mobile users. Mobile users that connect to low-range APs have to expect sudden disruptions in connectivity and quality of service. Since metrics like the total range of an AP are of little practical relevance for mobile users, we measured the distance that a user can move before the signal strength of the AP drops below -80 dB.

Figure 4 shows the results for 771 ranges for 882 distinct APs. We did not consider APs that had only a single reading (path length 0), leading to the discrepancy in the AP and range counts. The results indicate that even moving a short distance often makes a handover to a different AP necessary. For example, 73% of all samples exhibit an effective range of less than 40 meters. Assuming an average walking speed of 1.4 m/s, we can expect a maximum connection duration of 28 seconds for these APs. Hence, a ubiquitous network with such a short outdoor range requires handover support for mobile clients to approximate the performance of an ISP-built outdoor Wi-Fi network.

Even for stationary clients (e.g., an environmental sensor or a restaurant patron), the mobility support is beneficial because of the best-effort nature of the Wi-Fi sharing network. Due to the unplanned AP deployment, we assume unreliable but often redundant AP coverage. In cases of AP outage or if the link quality drops, another AP within range can provide fail-over.

IV. Can Muni-Fis be Collaborative?

This section discusses whether collaborative networks can match the requirements of Muni-Fis and their typical services and applications. The best-effort character of collaborative Muni-Fi networks is acceptable for many but not all usage scenarios and goals of Muni-Fis (cf. [1]):

Bridging the Digital Divide: It is obvious that a community-based Wi-Fi approach cannot solely serve the purpose of providing Internet access to those who cannot afford it in order to bridge the digital divide. This is because a Wi-Fi community approach relies on a sufficiently large number of members to contribute their existing broadband Internet connection to the community for the network to be of any value. Still, commercial Wi-Fi community providers like FON have shown that an established Wi-Fi community can sustain a certain number of users who do not contribute to the network infrastructure (paying FON customers). However, to advocate collaboration, a balance between community members and pure Wi-Fi users needs to be assured, in order to keep the network attractive for contributing and joining users. Further incentives could be the installation of access points in well-frequented areas without community Wi-Fi coverage or the establishment of attractive municipal services.

Fostering Economic Development: Collaborative Muni-Fi can offer a platform for commercial applications. The local character of the network especially lends itself to the integration of locally relevant services and business offers. However, a user-deployed network may not achieve sufficient coverage in commercial areas. Hence, the municipality and companies should also contribute to the Wi-Fi network where network coverage is beneficial for increasing economic development (e.g., in shopping malls and pedestrian precincts). Moreover, the openness of collaborative Muni-Fis allows for healthy competition between independent service providers.

Improving Citizen Satisfaction: The pervasive nature of a collaborative Muni-Fi can serve as a platform to offer new and attractive services to citizens as well as a simplified communication path to the government. However, providing general access to services or permanent free Internet access to citizens at home without supplementary fixed wireless connections cannot be achieved with collaborative Muni-Fi. This is, as a collaborative Muni-Fi primarily relies on existing Internet uplinks at home and aims at enabling Wi-Fi access for *mobile* users.

Stimulating Tourism: Collaborative Muni-Fi is well suited to provide mobile users with access to local information services. However, due to the unplanned deployment of community access points, important touristic locations may not be covered (e.g., sights that are not surrounded by residential buildings). In such locations, the municipality needs a planned deployment of dedicated access points that augment the existing community-based infrastructure and enable a continuous network.

Improving City Operation Efficiency: Collaborative Muni-Fi cannot give any guarantees regarding the availability of a network. Hence, civil workers can not exclusively rely on it. For example, live-streaming of CCTV videos is not possible via a user-operated access point because of a higher failure probability and limited fail-over options compared to orchestrated networks. However, services that can also operate without permanent connectivity may very well benefit from a collaborative Muni-Fi network. A CCTV camera that stores its pictures for eventual analysis in case of fraud or an environment sensor that collects environment data for later use can send its data over the Wi-Fi network when connectivity is available. In the latter two cases, a civil worker can also collect the data manually from time to time, if the network is not available. Hence, the city can increase its efficiency in some places, but it has to expect network failure at any time.

In this non-comprehensive Muni-Fi service analysis, we showed that a collaborative approach is especially valuable and feasible when the services provided in the network either require sporadic and non-ubiquitous network connection by nature or can be restricted to fit these characteristics (e.g., as presented in the CCTV example). However, services demanding a fixed set of service guarantees are hard or even impossible to implement in a collaborative network environment.

V. Technical Realization

When using a city-wide network, a user expects to perceive the network as *one* single system. However, due to its underlying principles, a collaborative Muni-Fi resembles a patchwork of different networks, owned and operated by individuals. Hence, the software and hardware in the system must be programmed and configured in a way that hides this patchwork-like character from the users.

There is a wide range of possible technologies and architectural concepts that can be employed to create a collaborative Muni-Fi. This section discusses technical challenges and possible design choices regarding the wireless network access, the WAP back-end that provides the APs with Internet connectivity, and the access to local services.

A. Wireless Network Access

Depending on the usage scenarios, a Muni-Fi must feature certain access control mechanisms to support network access for a closed group of users, open network access, or both at a time. In the following, we highlight the three most-widely used access control mechanisms: Link layer network access control through 802.1X, network-layer access control via Virtual Private Network (VPN) approaches, and application-layer access control.

The eduroam project [15] is a prominent example for a network provider restricting access at the link layer. It employs 802.1X to authenticate users during their attempt to associate to the advertised network. With a hierarchical authentication structure with hundreds of institutions in Europe, eduroam shows that large-scale 802.1X authentication is feasible. With 802.1X it is possible to distinguish unauthenticated from authenticated users. Hence, both classes of users can be treated differently regarding the available services.

VPNs are suited to set up an overlay network over encrypted tunnels, thereby hiding the actual network structure from the user. Moreover, VPN solutions include authentication and access control features. A collaborative Muni-Fi could provide an open 802.11 network for publicly accessible services and require a VPN connection to a VPN server for accessing restricted services.

VPNs and 802.1X require special configuration and software that may not be available on every client platform. Especially special-purpose hardware (e.g., an environmental sensor) may not implement those features. In these cases, a completely open network with access control on the application layer may serve the purpose of the community. Service providers can implement their own authentication methods (e.g., https and passwords) for their restricted services. Such a setup is commonly used by ISP-based city-wide Wi-Fi networks like FON in form of a captive portal, requiring a user to authenticate before granting access to the Internet.

B. Wireless Internet Back-end

Each AP of the community must be connected to the community network providing the local services. In the absence of a single common WAP, the connection with the LSPs is typically performed over the Internet. There are two options for providing this Internet connection to the community APs: direct connections through a wired link (e.g., ADSL) or wireless mesh-based approaches with wired connection for few APs.

Examples for large-scale Wi-Fi networks based on direct uplinks are FON and Wippies. In this model, community members contribute their wireless router and their uplink capacity to the community. Its advantage is that this uplink capacity is (fully) available to the community members, while the network is simple to deploy and to administrate.

In mesh-based approaches like Freifunk and panOulu, not all APs are necessarily connected to a fixed network uplink but may merely forward data to a gateway node with an Internet connection over the wireless link. In large mesh networks, several wireless hops are traversed before a data packet reaches a gateway node. Mesh networks have the advantage that an Internet connection is not required at each AP, making it possible to install APs in places where only mains power is available (e.g., lamp posts and facades), thereby extending the coverage of the Muni-Fi. However, multi-hop forwarding and a heavily-shared Internet uplink may seriously decrease the available network bandwidth. The characteristics of additional backbone technologies, including 3G networks and Wi-MAX are discussed in [9].

C. Access to Services

Once a user has access to the network at the wireless access level, the WAP may allow access either to a *restricted set of well-known LSPs* or to *any service in the Internet*.

There exist several approaches to restrict access to a set of service, in order to achieve a walled-garden-like service environment. Firewall-based approaches define a set of IP addresses of allowed services and block all other traffic. These approaches can be applied at the ingress points to the community network and are simple to install. VPN approaches allow the user to connect to a single VPN server only that provides the desired set of services. Alternatively, the community WAP can connect to a VPN server over the Internet, thereby creating a huge virtual bridged network that makes the services directly accessible to the users.

The firewall-based approach has the advantage that the traffic can directly flow between the services and the APs, whereas the VPN-based approaches require the VPN gateway to route all traffic through the Muni-Fi network. However, the firewall-based approach requires the distribution of the set of firewall rules across all community WAP, while the VPN approach affords a central enforcement.

Depending on the authentication at the WAP layer, additional authentication may be needed at the service layer. Especially for Internet access, user authentication is a must to prevent the obfuscation of criminal activities.

VI. Conclusion

In this paper we discuss the concept and the feasibility of collaborative municipal Wi-Fi. Through user-provided networking, these networks promise to reduce the cost of Muni-Fi networks and simultaneously increase their coverage in otherwise unattractive yet beneficial city areas. Our measurements in the center of Aachen show a sufficiently high density of private indoor access points to indicate the practicability of collaborative networks. Thus, even at moderate adoption rates, these existing APs can form an important cornerstone for a collaboratively organized Muni-Fi and its services. However, the collaborative approach cannot cater to every goal of existing municipal Wi-Fi networks. Its applicability depends on the specific requirements and the intended use of the respective Muni-Fi network. User contribution offers a cost-attractive option to cities that strive to extend their digital services.

References

[1] L. van Audenhove, P. Ballon, M. Poel, and T. Staelens, "Government policy and wireless city networks: a comparative analysis of motivations, goals, services and their relation to network structure," *The Southern African Journal of Information and Communication*, vol. 8, 2007.

[2] St. Cloud, "St. Cloud CyberSpot," [Online] Available http://www.stcloud.org/index.aspx?NID=402, Jan. 18, 2010.

[3] Wireless Philadelphia Project, "Wireless Philadelphia Project," [Online] Available http://www.wirelessphiladelphia.org, Jan. 18, 2010.

[4] Freifunk Community, "Freifunk Website," [Online] Available http://start.freifunk.net/, Jan. 18, 2010.

[5] FON WIRELESS, Ltd, "FON Website," [Online] Available http://www.fon.com/, Jan. 18, 2010.

[6] Saunalahti Group Oyj, "Wippies Website," [Online] Available http://www.wippies.com/, Jan. 18, 2010.

[7] Paris Wi-Fi, "Paris Wi-Fi," [Online] Available http:/wifi.paris.fr, Jan. 18, 2010.

[8] Panoulu, "public access network OULU," [Online] Available http://www.panoulu.net/index.shtml.en, Jan. 18, 2010.

[9] C. Szabó, K. Farkas, and Z. Horváth, "Motivations, design and business models of wireless community networks," *Mob. Netw. Appl.*, vol. 13, no. 1-2, pp. 147–159, 2008.

[10] FON WIRELESS, Ltd, "FON City Website," [Online] Available http://www.fon-city.de/, Jan. 18, 2010.

[11] T. Heer, S. Götz, E. Weingärtner, and K. Wehrle, "Secure Wi-Fi Sharing on Global Scales," in *Proc. of 15th International Conference on Telecommunication (ICT '08)*, 2008.

[12] N. Sastry, J. Crowcroft, and K. Sollins, "Architecting Citywide Ubiquitous Wi-Fi Access," in *Proceedings of ACM SIGCOMM HotNets (HOt Topics in Networks)*, Nov. 2007.

[13] Sonera, "Sonera Homerun Website," [Online] Available http://www.sonera.fi/en/, Jan. 18, 2010.

[14] DS Group, "Aachen Warwalking," [Online] Available http://ds.cs.rwth-aachen.de/research/projects/Muni-Fi/, Jan. 18, 2010.

[15] K. Wierenga and L. Florio, "Eduroam: past, present and future," *Computational Methods in Science and Technology*, vol. 11, no. 2, pp. 169–173, 2005.