Establishing Mobile Ad-Hoc Networks in 802.11 Infrastructure Mode

Hanno Wirtz, Tobias Heer, Robert Backhaus, Klaus Wehrle*
RWTH Aachen University
Chair of Communication and Distributed Systems
{wirtz, heer, backhaus, wehrle}@comsys.rwth-aachen.de

ABSTRACT

The 802.11 ad-hoc mode is supported by every IEEE 802.11-compliant wireless device. Due to this widespread availability, the ad-hoc mode appears especially suited to set up mobile ad-hoc networks (MANETs) between a wide range of heterogenous devices. Yet, in practice, creating a MANET is challenging because typical mobile devices do not implement the configuration, routing, and name resolution functions required to operate in an ad-hoc scenario. Software restrictions on modern mobile operation systems, such as Android and iOS, even prevent mobile devices from actively participating in ad-hoc networks without circumventing vendor barriers (e.g., acquiring root access). In contrast, full support for 802.11 infrastructure mode networks is a commodity even on closed platforms and embedded Wi-Fi systems. However, it is not suited for ad-hoc establishment of multi-hop networks. This discrepancy between lack of support for ad-hoc networks and lack of functionality in infrastructure mode networks led us to the question whether efficient ad-hoc networks can be formed by solely using 802.11 infrastructure mode. In this paper, we present an approach for 802.11 infrastructure mode ad-hoc networks in which mobile devices simultaneously function as an access point and as a station to mesh with other access point devices, thereby establishing multi-hop communication across multiple infrastructure mode networks. Our evaluation shows that 802.11 infrastructure ad-hoc networks even outperform 802.11 ad-hoc mode networks in terms of multi-hop throughput.

1. INTRODUCTION

The independence of any pre-defined network infrastructure makes mobile ad-hoc networks (MANETs) suitable for environments and situations where such infrastructure does not exist. One example scenario are disaster areas in which communication between rescue workers, search teams, and medical personnel needs to be established despite the destruction of network infrastructure. In another scenario, participants of a conference or an event create an ad-hoc network to communicate securely or transfer files between devices. To operate in a MANET, a device needs to switch its network card to ad-hoc mode and join the existing network. It then assigns an identifier to itself and takes part in the routing protocol that is used in the network to establish communication over multiple hops. MANETs should excel in terms of ease of use as well as flexibility because no wireless infrastructure must be set up and administered. However, MANETs are rarely seen in daily life. In our opinion, the proliferation of MANETs is currently hindered by three obstacles: *i)* Special-purpose devices, such as medical equipment, but also smartphones [6] do not necessarily support the 802.11 ad-hoc mode or do not provide user interfaces to enable it. *ii)* Supporting ad-hoc mode is insufficient for partaking in a MANET since every device must also support additional specialized MANET protocols for routing and address resolution. *iii)* Mobile device vendors and operating system developers focus on the widely-used 802.11 infrastructure mode and have little commercial incentive to provide full MANET functionality because of low customer interest.

In our opinion, the lack of MANET support in devices has lead to a lack of demand from customers, which in turn manifested the lack of device support. This circle creates a *chicken and egg* problem that is hard to overcome. At the same time, support and use of the 802.11 infrastructure mode is ubiquitous and some devices even allow to run several instances of wireless stations and wireless access points on a single wireless network card. With this capability, building mesh-like network structures consisting of access points and stations becomes possible. By using 802.11 infrastructure mode, all 802.11 devices, even devices that do not support any ad-hoc functionality, can become part of the MANET – a property that might solve the *chicken and egg* problem.

We thus analyze the creation of mobile ad-hoc networks in 802.11 infrastructure mode, which is supported by every 802.11-compliant device and relies on plain IP-routing. We propose MA-Fi (Mobile Ad-Hoc Wi-Fi), in which capable client devices such as notebooks or netbooks serve as access points for other station devices in the vicinity. At the same time, these client devices establish one or more associations to infrastructure networks provided by other clients to achieve interconnection between networks. While providing a traditional infrastructure mode network that is supported by all types of devices, MA-Fi allows for multi-hop communication through these interconnections.

The rest of this paper is structured as follows: In Section 2 we introduce the main technique that we employ to create an ad-hoc network in 802.11 infrastructure mode. We highlight the challenges of establishing an ad-hoc network using MA-Fi in Section 3. Section 4 shows the feasibility of MA-Fi through a performance evaluation and Section 5 discusses related work. We discuss current limitations of our approach in Section 6 and conclude with Section 7.

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

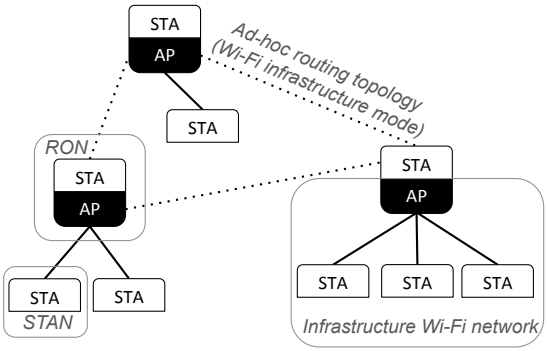

Figure 1: Nodes provide autonomous 802.11 infrastructure mode networks to stations. Additionally, nodes maintain associations to networks provided by other nodes to achieve interconnectivity and multihop communication.

2. MA-Fi NETWORKING

To address the aforementioned problems of insufficient device support for ad-hoc networking and complex setup, we propose to use the 802.11 **infrastructure-mode** for building ad-hoc networks. Based on commodity mobile devices, we create an ad-hoc topology of wirelessly interconnected access points. Clients without special software or ad-hoc functionality can associate to mobile devices that serve as access points and participate in the ad-hoc network. Hence, we create a two-tier hierarchy of router nodes (RONs) that perform ad-hoc functions and station nodes (STANs) that are connected to the ad-hoc network via a RON. From the perspective of a STAN, the RON behaves like an ordinary Wi-Fi infrastructure mode access point that connects the STAN to the entirety of the ad-hoc network.

An exemplary network is shown in Figure 1. Three RONs form the backbone of an ad-hoc network while six STANs use the network without being aware that they participate in an ad-hoc network. The only requirement for STANs is to be able to associate to a RON by using a single 802.11 association in infrastructure mode. Examples for STANs are smartphones without ad-hoc support; Google disables ad-hoc networking in Android by default [1] while the iPhone 4 only connects to ad-hoc networks in Wi-Fi fashion, i.e. spanning a single hop. A second example is special-purpose equipment such as medical devices that transmit results back to a base station over the wireless infrastructure link. A RON serves two purposes: First it serves as a wireless infrastructure network access point (AP) to the STANs. Second it meshes with other RONs in the ad-hoc backbone and performs routing functions. Examples for RONs are notebooks and netbooks, see Section 4.1.

To form the ad-hoc Wi-Fi backbone, each RON associates to APs of multiple other RONs. Typically, mobile devices associate only to a single network or exclusively provide AP functionality (e.g., for tethering). A straightforward approach to associating to multiple networks is to use multiple network cards per device. Although the use of multiple cards offers better mobility handling and throughput maximization [1], typical mobile devices only feature one physical network card. In principle, mobile devices can use a single physical network card to simultaneously act as AP and station by defining virtual network interfaces. Drivers such as the *ath9k* driver for Atheros wireless network cards support this mode of operation natively. Each virtual network interface is then separately configurable and appears as a normal interface to applications, with the restriction of using the same channel on all interfaces. However, such parallel operation requires the network card driver to iterate between the different networks, i.e. switch the card in time to serve or listen to each network.

In MA-Fi, STANs only maintain one association to an infrastructure network and thus only operate one interface in station mode (STA). As shown in Figure 1, RONs operate multiple interfaces in station or access point (AP) mode. The AP interface provides an 802.11 infrastructure mode network to STANs, the STA interfaces connect a RON to the networks provided on the AP interfaces of other RONs. While each network is autonomous, routing towards other networks is enabled over the links between RONs.

The approach of providing interconnected autonomous networks in 802.11 infrastructure mode is the main aspect of MA-Fi. STANs that do not support 802.11 ad-hoc mode communication and thus cannot participate in ad-hoc mode MANETs, can associate to one network and communicate with distant networks using the connections between networks. Furthermore, there is no need for a custom routing protocol for STANs, as they perceive the whole network as a regular, one-hop 802.11 infrastructure mode network.

Using this approach, we establish a network of arbitrary size consisting of STANs and RONs. However, several challenges exist in providing a dynamic mobile ad-hoc network. First, STANs require services like host configuration and name resolution in the network. We discuss the challenges in providing these services and supporting STANs as in typical 802.11 infrastructure mode networks in Section 3.1. Second, to achieve network coverage while maintaining good performance when routing between nodes, the MA-Fi network should balance the number of RONs and thus the number of autonomous networks. In Section 3.2, we discuss challenges in achieving a good balance. Third, we assume STANs and RONs to be mobile devices, hence STAN and RON mobility needs to be supported in the network. Section 3.3 and Section 3.4 discuss the respective challenges. Finally, the association of multiple networks and the operation of multiple interfaces on a RON includes a performance penalty compared to operating exclusively as a station or an AP. We evaluate this performance penalty and the performance of MA-Fi compared to ad-hoc mode MANETs in Section 4.

3. CHALLENGES

While the basic MA-Fi approach allows for a basic, static network structure, multiple challenges with regard to the maintenance of the network and the support for mobile clients remain. We now discuss the main aspects of providing a dynamic ad-hoc network based on 802.11 infrastructure mode.

3.1 STAN Support

To a STAN that supports only 802.11 infrastructure mode networks, the MA-Fi network has to look like and provide the same set of services as an AP-based Wi-Fi network. This is achieved by offering the same set of software and services at RONs instead of wired APs.

When first joining a network, a STAN expects a DHCP server to provide a host configuration. Next to an IP-address,

[1]It is possible to enable ad-hoc networking, but this requires root access to the phone.

this includes information about essential services like the designated gateway or name servers in the network. Just as in one-hop Wi-Fi networks, these services are provided by the local RON, serving as the AP in this network. These services can be provided in a distributed or centralized fashion. A RON may either serve as an independent DHCP server or may serve as a DHCP relay that forwards requests to a designated server in the MA-Fi network. Such a network-wide DHCP server can centrally coordinate the address assignment for all STANs in the network. While this is feasible and provides the advantage of keeping only one host database, we argue that a local DHCP server better serves the autonomous character of local networks. Having separated IP-assignments for local networks enables the application of NAT functionality and facilitates IP-based routing between networks. Analogous to one-hop Wi-Fi networks, name resolution should be provided transparently by the RON as well. As no designated name server exists in MA-Fi, name resolution may be distributed over the existing RONs. To achieve good coverage, a cluster-based resolution scheme may be employed [9]. Finally, the RON also serves as a gateway to the rest of the ad-hoc network and hides the routing complexity of the ad-hoc network from STANs.

3.2 Network Establishment

Mobile STANs that leave the coverage of a RON must be able to instantly associate to another RON to maintain their existing network connections. Thus, to achieve good coverage as in a MANET a sufficient number of devices must operate as RONs. However, too many RONs in a network can limit the forwarding efficiency of the network. Therefore, selecting a suitable number of RONs includes a tradeoff between coverage and performance. In the following, we discuss this tradeoff.

In a straightforward approach, every device capable of using virtual networks and providing AP functionality serves as a RON. This approach works well in sparse ad-hoc network scenarios. However, this is different in densely populated networks. As shown in [7], the capacity of wireless channels experienced at each device depends on the number of devices in the vicinity. While we have no influence on the number of STANs, we can adjust the number of RONs and thus the number of networks. A high number of RONs promises good coverage and fine-grained IP-routing in terms of target networks that are available. However, in this case, RONs need to manage a high number of STA interfaces and not much benefit is gained from providing additional networks in already covered areas. This is because additional routing steps between RONs that could be served in one network require more medium access steps and thus place a higher load on the wireless medium. Thus, a low number of networks in the vicinity that provide connectivity to the network is preferable to oversaturation of a given area.

The problem of a good RON assignment to provide these networks is very similar to the dynamic selection of cluster heads in hierarchic cluster-based routing protocols [5]. Another comparable scenario is the assignment of landmark functionality in hop-count based routing schemes [13]. Although there is only one hierarchy level and the selection of RONs is not only dependent on hop-counts, the techniques presented in these approaches may give rise to comparable solutions in our approach.

While the connections between RONs provide a routing topology, we need an efficient routing scheme in the MA-Fi network. In principle, any MANET routing protocol is suited to provide routing between RONs. However, in this work we focus on the feasibility of building ad-hoc networks based on 802.11 infrastructure mode. Hence, the selection of a suited MANET routing protocol is out of scope and presents future work.

3.3 STAN Mobility

Station devices in a MANET are assumed to be mobile. In traditional MANETs, each device provides a point of association to the network. In contrast to this, we establish autonomous infrastructure networks that also need to appear as one large network to a mobile STAN. Thus, once a STAN moves away from its current RON and associates to a new one, handover events on Layers 2 and 3 occur. If performed quickly enough to avoid timeout events on the upper layers, a handover on Layer 2 does not influence TCP/IP connections. A handover on Layer 3 usually breaks existing connections at the STAN as a new host IP address is assigned.

Our goal is thus to prevent STANs to notice network changes and to further be able to automatically switch to the current best RON in case of failure or mobility of the current one. To achieve this, we let each RON provide the same network in terms of the network SSID and the IP and MAC address of the gateway interface a STAN communicates with. We keep the MAC address of the wireless interface of the RON unique to enable STANs to distinguish RONs and to prevent packet duplication at nearby RONs. Thus, once a STAN moves, it perceives the new network as identical to the previous network save for the destination MAC address in Wi-Fi frames. As all networks carry the same SSID, a STAN can thus change networks automatically and transparently to the operating system. Using the same MAC address for the gateway interfaces of all RONs avoids ARP timeouts and enables the STAN to instantly send packets to the rest of the MA-Fi network.

Preserving connections on higher layers still presents a challenge as traffic that is addressed *to* the mobile STAN needs to be routed to the new RON. However, as only RONs handle connections to STANs in their network, a mobility solution that enables such re-routing would only need to be realized on this small set of devices instead of the whole network as in MANETs. Candidate solutions are proxy-based mobile IP variants or end-to-end mobility signaling as employed in HIP [12].

3.4 RON Mobility

In contrast to STAN mobility, RON mobility has an impact on the overall network topology and performance. As outlined in Section 3.2, the number of RONs and their locations make up the multi-hop routing topology in the network. If a RON moves, it alters the routing topology and may eventually require other client devices to create networks to preserve the coverage and connectivity. In addition, the RON may leave the vicinity of the STANs that are associated to it. Hence, when selecting candidate hosts for RONs, their mobility as well as their mobility in respect to their surrounding STANs should be taken into account. Stationary devices and devices that move together with other devices (i.e., similar to a personal area network) should be preferred as RONs.

In order to build a meshed network topology, RONs must decide to which other RONs they associate to. Links between two RONs are modeled by a RON in station mode that connects to a RON in AP mode. The links are defined by the AP's SSID, BSSID, and the MAC address of the RON that acts as station. Unlike STANs, RONs require explicit control of the inter-RON links they establish. Hence, using the same SSID for all inter-RON links may cause problems for the RON that acts as station because many operating systems automatically switch between APs with identical SSID, assuming that the APs belong to the same bridged network. Such automatic switching mutilates the routing topology and may lead to undesired effects at the routing layer. To avoid such automatic switching, we use SSIDs consisting of a global prefix and a RON-specific suffix. This way, RONs can associate to specific APs and disassociate from selected APs based on their own preference and without interference from the operating system.

4. PERFORMANCE EVALUATION

In this section, we introduce the actual devices we use as RONs and analyze the performance of these devices when serving as RONs in our scenario. To compare our approach against ad-hoc scenarios, we measure the throughput regression over multiple hops in infrastructure networks and in ad-hoc mode.

4.1 Feasibility

To show the feasibility of our approach on commodity client devices, we employ unmodified netbook devices that run Ubuntu 11.04 as the operating system. We create and manage virtual interfaces using the *iw* configuration utility that makes use of the *nl80211/cgf80211* interface, which is included in the standard Ubuntu distribution. To provide AP functionality like host configuration and name resolution at the AP device we employ *hostapd* to operate an interface as an AP and common tools like *dhcp3* or *dnsmasq* for service functionality. We thus only rely on standard software and commodity hardware to establish and maintain ad-hoc infrastructure networks on client devices, which shows the practicality of our approach.

Specifically, we employ two netbook devices as RONs in the following measurements. The first is an Asus Eee PC T91 with a 1.4GHz CPU and an Atheros AR9285 802.11n wireless network card. The second device is a Dell Inspiron Duo 3223 with a dual-core 1.5GHz CPU and an Atheros AR9285 802.11n wireless network card as well. We use these devices as representatives for mobile client devices that are likely to be found in ad-hoc network scenarios. Both devices neither possess top-tier computing power nor specialized networking hardware, which makes measurements using these devices a good estimate for results on wide-spread consumer-scale devices.

For reference measurements, we use Linksys WRT160NL WLAN routers that are equipped with Atheros AR9102 wireless network cards. Routers run OpenWrt as the operating system. While the router device possesses significantly lower processing power, it is a special-purpose networking device which allows us to compare its networking performance to the performance of client devices.

4.2 Client Capabilities

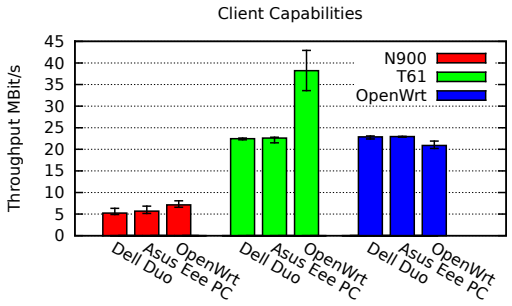

Figure 2: TCP throughput of two netbook devices (Asus Eee PC, Dell Duo) serving as RONs for different STAN types. As a reference, results of a WLAN router (OpenWrt) are shown.

We first need to analyze whether commodity client devices perform well as APs (RONs) in an 802.11 infrastructure network. To this end, we switch two netbook devices to AP mode and measure the possible TCP throughput between the netbooks and a smartphone, a notebook and, for reference, an OpenWrt router. Figure 2 shows the results of our measurements.

As a smartphone class STAN, we use a Nokia N900. In general, throughput performance of the N900 is low even towards the OpenWrt router, with the maximum throughput at 7 MBit/s. However, throughput towards any of the two RONs differs only slightly from the reference measurement towards the router, indicating capability of operating as an AP. In this scenario, the STAN is the bottleneck, as the following measurements with more powerful STANs show.

When using a Lenovo T61 notebook, we achieve a maximum data rate of 38 MBit/s towards the router device, more than five times the throughput of the N900. In comparison to this, throughput towards any of the two netbook devices is about 24 MBit/s or 63%. While this is a wide margin, the difference is due to special-purpose networking hardware in the router device, such as a designated 400MHz controller of the wireless network cards. However, both netbooks offer a similar performance as 802.11g WLAN routers, which exceeds typical ad-hoc mode performance. [2] These results are supported by throughput measurements originating from a router device. As almost identical data rates are achieved, the defining factor in the MA-Fi scenario appears to be the netbook devices. A throughput of over 20MBit/s at these devices makes them (and comparable devices) well suited for performing RON functionality in our scenario.

4.3 Performance Penalty

We compare the 802.11 infrastructure mode (Wi-Fi) and MA-Fi in the same network topology, in this case two STANs associated to one AP device (for Wi-Fi) and to one RON (for MA-Fi) respectively. In Wi-Fi mode, the AP is not associated to another network and hence only operates its AP interface. For MA-Fi the RON is associated to another network thus operating a STA interface in addition to its AP interface. Operating multiple interfaces and switching between associated networks claims a performance penalty [4]. To gain results that solely reflect this penalty we send no traffic over the STA interface in MA-Fi mode. In both cases

[2]Note that 802.11 ad-hoc mode implementations per standard only support data rates of 11MBit/s.

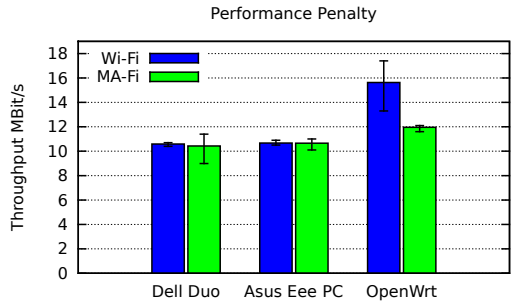

Figure 3: Throughput between two STANs connected to the same node in Wi-Fi and in MA-Fi. Operating an additional STA interface in MA-Fi reduces throughput, but still allows for good throughput between STANs.

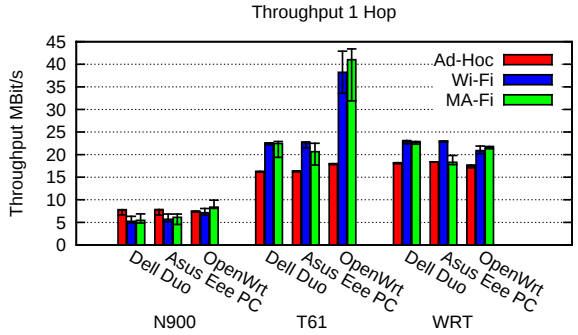

Figure 4: TCP throughput of STANs to different RONs. MA-Fi consistently offers throughput comparable to Wi-Fi and mostly better than ad-hoc mode, except for a few outliers in which MA-Fi performs worse than ad-hoc mode or even better than Wi-Fi.

we measure the unidirectional net TCP throughput between the two STANs.

Figure 3 depicts the results for our netbook devices and a WLAN router for reference. On the router, a significant performance penalty of about 20% exists when operating an additional interface. With Wi-Fi as reference value, we observe a MA-Fi throughput for the Dell Duo of 98.5% and for the Asus Eee PC of 99.9%. We can conclude that running a netbook with MA-Fi settings does imply a, rather small, performance penalty.

In comparison to direct one-hop throughput, as shown in Figure 2, about half the throughput is achieved between two STANs. This supports the intuitive thought that receiving from one STAN and sending to another STAN each consumes the same amount of airtime, while only a small amount of time is spent maintaining the passive network. Thus, with regard to the performance penalty, a good utilization of the wireless capabilities is achieved.

4.4 Throughput Comparison

First, we evaluate the possible throughput of MA-Fi over one hop in comparison to 802.11 infrastructure mode (Wi-Fi) and ad-hoc mode as shown in Figure 4. In MA-Fi, RONs maintain a second network association. As STANs, we use an N900 as a smartphone device, a Lenovo T61 as a notebook and an OpenWrt-based router as a reference. While

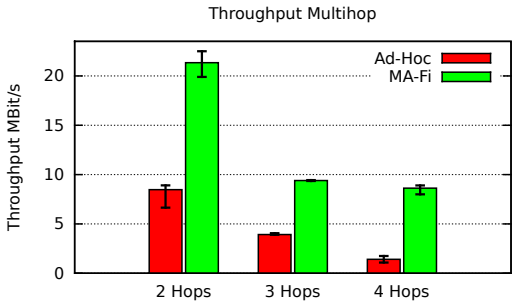

Figure 5: TCP throughput comparison over multiple hops between MA-Fi and ad-hoc mode. In both cases, throughput decreases over multiple hops, however, MA-Fi outperforms ad-hoc mode transmissions over every hop-count.

the N900 surprisingly achieves the best results in ad-hoc mode, results in MA-Fi and Wi-Fi are comparable. Using the T61 and router device, MA-Fi consistently outperforms ad-hoc mode transmissions and compares well against Wi-Fi. We regard results in which MA-Fi outperforms Wi-Fi as outliers, as supported by the high variance in these measurements.

Second, we measure the possible throughput in MA-Fi compared to ad-hoc mode transmissions. Through the successive transmission over infrastructure mode links operating at about 802.11g performance, we aim to achieve better throughput and less regression. Figure 5 shows the results of our measurements over 2, 3 and 4 hops. In both cases, throughput decreases over the number of hops. However, MA-Fi consistently achieves higher throughput than transmissions in ad-hoc mode, thus validating our approach of connecting autonomous networks over infrastructure mode links. This is due to the use of directed links in 802.11 infrastructure mode in contrast to the broadcast-centered transmissions at a low data rate in ad-hoc mode. While the infrastructure mode allows for rate adaptation and thus higher data rates towards stations, it lacks the broadcast functionality of the ad-hoc mode that is essential to flooding in MANET routing protocols. We thus will look into a suitable routing protocol for the ad-hoc routing topology and a corresponding use of broadcasts.

5. RELATED WORK

Chandra et al. first introduced the concept of virtualizing wireless network interfaces on a single network card to connect to multiple networks simultaneously and transparently to the operating system. In [4] they focus on algorithms that allow the virtualization layer to effectively switch between the present interfaces and the effect on TCP transmissions. Their work is realized in the VirtualWiFi [11] project and is included in the Windows 7 operating system as *Native 802.11 Virtual Wireless Fidelity*. In the *SoftRepeater* approach [2], they address the rate anomaly problem in Wi-Fi networks by providing a virtualized network interface to clients with poor link quality. FatVAP [10] employs network virtualization to make use of the combined backhaul capacity of multiple APs in the vicinity. By estimating the available bandwidth at each AP and switching between APs accordingly, FatVAP makes use of the higher bandwidth of wireless links to improve download speed and re-

sponse times. While also using network virtualization, none of these approaches targets autonomous ad-hoc network creation but they instead focus on the extension of AP-based networks that already operate in infrastructure mode. As such, no focus is placed on characteristics of MANETs such as a routing topology, mobility or the inclusion of stations without ad-hoc mode support.

The upcoming 802.11s standard [3] defines *Mesh Access Points* that provide an infrastructure mode network to clients in addition to the mesh backbone network between *Mesh Points*. From a network structural point of view, this approach is similar to ours. However, the 802.11s standard targets stationary infrastructure based mesh networks instead of mobile ad-hoc networks and assumes a maximum of 32 mesh nodes plus clients. Furthermore, mesh access points are assumed to be multi-radio devices so that traffic on one network card does not influence the performance of the other networks. In our approach, we assume single-radio, consumer-scale mobile devices that create networks for ad-hoc communication between an arbitrary number of nodes. Similarly, the Wireless Distribution System (WDS) enhances the coverage of a single base AP over a number of relay stations. While relay stations provide network access to clients, this approach, too, targets the extension of a stationary network. AP functionality at a central entity in the network furthermore hinders scalability and flexibility in network creation and routing.

The ad-hoc routing topology between selected nodes in MA-Fi resembles cluster routing approaches for MANETs [5, 8]. In these approaches, however, all devices need to support ad-hoc mode communication in a continuous network. In contrast to this, we establish smaller local networks in infrastructure mode to support all types of devices.

6. LIMITATIONS

Currently, network virtualization only works reliably with Atheros wireless chipsets, such as installed in the two netbook devices. We assume the reason for this to be the inherent support for multiple associations and virtualized interfaces by the device drivers for Atheros cards, namely *MadWifi*, *ath5k* and *ath9k*. Other chipsets either may not support the new *nl80211/cfg80211* interfaces or are not capable of operating in AP mode. An example for the former case are Broadcom chipsets, as found in the Apple MacBookPro series, while the Intel chipsets installed in Lenovo T500 and T61 notebooks do not support AP functionality. However, newer chipsets are likely to support virtualized interfaces as well as the *nl80211/cfg80211* interfaces in Linux as these replace the previous tools.

7. CONCLUSION

In this paper, we proposed and analyzed the use of 802.11 infrastructure networks to establish ad-hoc networks. Using the infrastructure mode, we achieve support for stations that do not support the 802.11 ad-hoc mode, remove the need for a custom MANET routing protocol supported by all nodes and enable support for Wi-Fi services such as host configuration in the local network. We discussed the challenges in establishing the ad-hoc routing topology and in supporting mobility and evaluated the feasibility of MA-Fi by performance measurements on commodity hardware. MA-Fi outperforms ad-hoc mode communication and offers throughput comparable to Wi-Fi, even over multiple hops. Using MA-Fi, the *chicken and egg* problem of establishing a network for applications can be solved as only very few devices are required to span the ad-hoc topology. Other devices perceive the network as a typical one-hop Wi-Fi network. Our approach is applicable in MANET scenarios such as disaster recovery but also provides a mechanism for ad-hoc network provision in daily life. As future work, we will look into suitable, scalable routing mechanisms for the ad-hoc topology as well as a decentralized RON selection scheme. Furthermore, we will evaluate the applicability of legacy services in our MA-Fi scenario.

8. REFERENCES

[1] Bahl, P., Adya, A., Padhye, J., and Walman, A. Reconsidering wireless systems with multiple radios. *SIGCOMM Comput. Commun. Rev. 34* (October 2004), 39–46.

[2] Bahl, P., Chandra, R., Lee, P. P. C., Misra, V., Padhye, J., Rubenstein, D., and Yu, Y. Opportunistic use of client repeaters to improve performance of wlans. In *Proceedings of the 2008 ACM CoNEXT Conference*, CoNEXT '08.

[3] Camp, J., and Knightly, E. The IEEE 802.11s extended service set mesh networking standard. *IEEE Communications Magazine 46*, 8 (Aug. 2008).

[4] Chandra, R., Bahl, P., and Bahl, P. Multinet: Connecting to multiple ieee 802.11 networks using a single wireless card. In *IEEE INFOCOM* (2004).

[5] Chiang, C.-C., Wu, H.-K., Liu, W., and Gerla, M. Routing in clustered multihop, mobile wireless networks with fading channel. In *IEEE Singapore International Conference on Networks, SICON'97*.

[6] Google. Ad-Hoc Support in Android. [Online] Available http://code.google.com/p/android/issues/detail?id=82, May 18, 2011.

[7] Gupta, P., and Kumar, P. The capacity of wireless networks. *Information Theory, IEEE Transactions on* (mar 2000), 388 –404.

[8] Haas, Z. J., Pearlman, M. R., and Samar, P. The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft, July 2002.

[9] Hong, X., Liu, J., Smith, R., and Lee, Y.-Z. Distributed naming system for mobile ad hoc network. In *ICWN* (2005).

[10] Kandula, S., Lin, K. C.-J., Badirkhanli, T., and Katabi, D. Fatvap: aggregating ap backhaul capacity to maximize throughput. In *Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation* (2008), pp. 89–104.

[11] Microsoft. VirtualWiFi Project. [Online] Available http://research.microsoft.com/en-us/um/redmond/projects/virtualwifi/, May 18, 2011.

[12] Moskowitz, R., Nikander, P., Jokela, P., and Henderson, T. Host Identity Protocol. RFC 5201 (Experimental), 2008.

[13] Pei, G., Gerla, M., and Hong, X. Lanmar: landmark routing for large scale wireless ad hoc networks with group mobility. In *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing* (2000), MobiHoc '00.