2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems

High-performance, Energy-efficient Mobile Wireless Networking in 802.11 Infrastructure Mode

Hanno Wirtz, Georg Kunz, Johannes Laudenberg, Robert Backhaus, Klaus Wehrle
Chair of Communication and Distributed Systems, RWTH Aachen
{wirtz, kunz, laudenberg, backhaus, wehrle}@comsys.rwth-aachen.de

***Abstract*—A plethora of mobile wireless networking approaches, from multi-hop infrastructure-less networking to mobile offloading and crowd sourcing, relies on establishing communication directly between devices. However, the 802.11 ad-hoc mode, as the designated technological means to realize device-to-device communication, suffers from missing support by vendors and operating system and lacks 802.11 functionality support. If at all, mobile wireless networking approaches reach a very low number of compatible devices and have to tolerate low network performance, deprecated WEP network security, and a lack of energy saving mechanisms. Eventually, this lack of a technological basis prevents the timely and beneficial real-world adoption of mobile networking.**

We thus propose such a basis in MA-Fi, multi-hop mobile networking using the 802.11 infrastructure mode. Building on comprehensive vendor and device support, MA-Fi realizes 802.11n performance, WPA2 security, and efficient energy saving mechanisms in ubiquitously compatible, mobile 802.11 infrastructure mode networks. Specifically, MA-Fi uses network virtualization to establish a two-tiered network topology that seamlessly incorporates legacy Wi-Fi devices. In comparison to the ad-hoc mode, MA-Fi achieves throughput of up to 340 % while reducing the network-wide energy consumption by up to 75 %.

I. Introduction

Mobile 802.11 wireless networking, driven by the readily available critical mass of smartphones and laptops [1], serves as the envisioned communication technology in a diversity of approaches that complement access to globally reachable Internet services with mobile, local communication structures. Approaches thereby range from performance-oriented, infrastructure-less mobile networks [2] to opportunistic networking [3], crowd sourcing [4], mobile sensing [5], and mobile social networking [6]. In this, mobile offloading [7], [8], i.e., exploiting mobile network structures to relieve overloaded carrier networks, especially highlights the utility and timeliness of communication in mobile 802.11 networks. The continually increasing number of mobile wireless devices and associated mobile Internet traffic suggest that the importance of offloading traffic in local wireless networks will further rise in the further, both from an economical and performance point of view.

Enabling local mobile wireless communication then requires a means of establishing networks between heterogeneous mobile devices. Traditionally, the IEEE 802.11 ad-hoc mode constitutes the assumed technological basis to spontaneously establish such mobile networks. Yet, it suffers from irregular or even non-existing support by manufacturers and vendors of Wi-Fi cards [9], [10] and operating systems [11]–[13]. For example, the short list of supported devices in the Commotion Wireless project [14] as well as several academic approaches [3], [15] highlight the difficulty in establishing real-world mobile wireless networking in the 802.11 ad-hoc mode. As a result, mobile networking approaches remain confined to academia and rarely manifest themselves in real-life applications.

TABLE I. Missing vendor support for important 802.11 functionality in ad-hoc mode networks.

	Throughput	WPA2 Security	802.11 PSM
Linux	17.4 MBit/s	irregular	no support
OS X	19.6 MBit/s	no support	no support
Windows 7	13.5 MBit/s	supported	irregular
Android [11]	no support	no support	no support
iOS [12]	no support	no support	no support
WP 7 [13]	no support	no support	no support

To quantify these shortcomings[1], Table I lists the measured one-hop throughput performance as well as the security and energy saving capabilities of the 802.11 ad-hoc mode in major operating systems[2]. Analyzing the throughput measurements reveals that the transmitted 802.11 frames exclusively announce data rates of 54 MBit/s or less, indicating mere 802.11g-like performance. Furthermore, although standardized in 802.11 [16], WPA2 network security for ad-hoc networks is unsupported in OS X [17] and is only irregularly supported under Linux [18]. Last, operating system vendors do not provide information whether 802.11 power saving mechanisms (PSM) are supported in the ad-hoc mode. During our tests, neither Linux- nor OS X-driven devices supported PSM. In practice, this inconsistent support of ad-hoc networking functionality translates into incompatible setups, low performance, and high energy consumption.

In order to provide a compatible and deployable basis for mobile networking approaches, we thus propose MA-Fi (Mobile Ad-Hoc Wi-Fi), practical mobile multi-hop wireless networking utilizing exclusively the 802.11 infrastructure mode. MA-Fi is motivated by two observations: 1) Every Wi-Fi device supports the 802.11 infrastructure mode and its main networking features, namely 802.11n performance, WPA2 security, and PSM energy saving. 2) Mobile networking approaches assume a (multi-hop) wireless network for packet transmissions but abstract from the underlying mode of operation.

Existing efforts [3], [15], [19] that aim at realizing the benefits of mobile infrastructure-mode 802.11 networking only

[1]Please note that this evaluation bases on the devices available to us, representing a typical everyday scenario. Select combinations of wireless card and 802.11 drivers may show other performance.

[2]Linux 12.10: Lenovo IdeaPad S10-3, Atheros AR9285. OS X 10.6.8: MacBook Pro, Broadcom BCM4321. Windows 7: Lenovo ThinkPad T400s/420, Intel 5300/6300.

978-1-4799-6036-1/14 $31.00 © 2014 IEEE
DOI 10.1109/MASS.2014.21

provide one-hop networks. In contrast, MA-Fi establishes a mobile *multi-hop* network infrastructure using 802.11n infrastructure-mode links. It thus realizes the performance and compatibility of 802.11 infrastructure mode networks within the flexibility and dynamics of ad hoc mode-like multi-hop networks, as envisioned in the rich history of ad-hoc networking research (e.g., [2], [20], [21]). MA-Fi leverages wireless network virtualization to establish a two-tier network hierarchy comprising i) an optimized sparse backbone network of *routing nodes* (RONs) that provide ii) Wi-Fi infrastructure mode networks to (legacy) 802.11 station devices (STANs). To achieve IBSS-like multi-hop communication, RONs act as legacy gateways and employ a modified variant of the DYMO (Dynamic MANET On-demand Routing) [22] routing protocol in the backbone network. MA-Fi then makes the following contributions to enable and improve mobile networking without relying on the 802.11 ad-hoc mode:

i) A novel, mobile multi-hop network design utilizing the infrastructure mode that offers up to 340 % of ad-hoc mode throughput between commodity real-world devices.
ii) A low-overhead topology coordination mechanism that reduces the number of forwarding nodes by up to 75 % while providing 93 % of the ad-hoc mode connectivity.
iii) An unassisted duty cycling approach for RON backbone devices that supports 802.11 PSM by legacy devices to reduce network-wide energy consumption by up to 75 %.
iv) A proof-of-concept distributed 802.1X authentication to provide state-of-the-art WPA2 network security instead of deprecated WEP support in the 802.11 ad-hoc mode.

The proposed network structure resembles a mobile variant of wireless mesh networks [23]–[25]. Our contribution is the analysis of state-of-the-art device capabilities with regard to mobile wireless networking and the subsequent realization of a high-performance, compatible, energy-efficient mobile network structure built on commodity, single-radio mobile devices. In our emphasis of real-world applicability, we strive to contribute to manifesting mobile networking approaches in real life.

Section II distinguishes our contributions from related approaches that target compatible, energy-efficient, or secure mobile wireless networking. We furthermore analyze the applicability of the infrastructure mode for mobile ad-hoc networking in Section III by comparing it with the 802.11 ad-hoc mode. Based on this analysis, we present our design of an infrastructure mode-based multi-hop mobile wireless network in Section IV. Section V shows the feasibility, performance, and energy efficiency of our design. We conclude in Section VI.

II. Related Work

MA-Fi relates to approaches in infrastructure mode, energy-efficient, and secure mobile wireless networking.

A. 802.11 Infrastructure Mode Ad-Hoc Networking

WiFi-Opp [3], *Cool-Tether* [15], and *Wi-Fi Direct* [19] enable direct communication between mobile devices *in single-hop scenarios.* Building on tethering (or softAP) functionality, they exploit the asymmetry of the 802.11 infrastructure mode to provide compatible wireless networking. In contrast, MA-Fi is the first approach to expose the performance of the infrastructure mode to mobile multi-hop networking. MA-Fi accounts for multi-hop routing and communication as well as mobility support in a distributed network topology.

In multi-hop approaches, the 802.11s standard [25] as well as the *iMesh* [23] and *MeshCluster* [24] approaches establish two-tier wireless mesh networks that provide connectivity to legacy stations. These approaches create *stationary* mesh networks and build on dedicated multi-radio, high-performance network elements. A real-world example of this notion is the *Commotion Wireless* [14] project that aims at combining an ad-hoc mode mesh backbone with infrastructure mode client networks. MA-Fi shares its two-tiered topology design with these approaches, but provides mobile multi-hop networking using commodity devices that dynamically operate the network, increasing the real-life feasibility of ad-hoc networking.

B. Energy Efficiency in Multi-Hop Mobile Networks

MA-Fi achieves energy efficiency through opportunistic duty cycling of RONs in the routing backbone and leveraging the support for 802.11 PSM in the legacy networks. We share the motivation of optimizing a connected network with traditional ad-hoc mode approaches, e.g., [26], [27]. However, the applicability and benefit of these mechanisms is strongly diminished by the missing support for 802.11 PSM in the ad-hoc mode. Hence, MA-Fi leverages the ubiquitous PSM support in the infrastructure mode to actually realize the conceptual benefits in mobile networks.

Cool-Tether [15] and *DozyAP* [28], among others, optimize the energy efficiency of (mobile) single-hop 802.11 infrastructure mode networks but require significant adaptations of the communication infrastructure. Specifically, *Cool-Tether* requires an energy-aware cloud proxy server that governs the workload of mobile devices while *DozyAP* relies on modifications of the client 802.11 functionality to enable negotiation of AP duty cycling in a "sleep protocol". In contrast, energy efficiency optimizations in MA-Fi are autonomous within the network scope. Driven by empirical observations, RONs duty cycle sleep phases without client support to ensure compatibility.

C. Security in Multi-Hop Mobile Networks

MA-Fi exposes WPA2 network security mechanisms to mobile multi-hop mobile networks and supports distributed RADIUS-based 802.1X authentication. It leverages the comprehensive support of WPA2 and 802.11i in the infrastructure mode to realize a security architecture resembling [29]. MA-Fi's network-level security features are complementary to secure routing and neighbor detection.

III. Comparing the 802.11 Infrastructure and Ad-hoc Mode for Mobile Wireless Networking

In this section, we analyze the suitability of the 802.11 infrastructure mode for establishing mobile networks in place of the vanishing ad-hoc mode. To this end, we compare both modes in terms of *network operation* and *mobility support*. While both modes share the same physical (PHY) and medium access (MAC) layer specifications in terms of modulation schemes and carrier sense functionality, the absence of a central entity in mobile scenarios requires distribution of 802.11 and networking functionality among all devices.

A. Network Operation

In an infrastructure mode network, denoted Basic Service Set (BSS), one device in access point mode (AP) provides the network to a number of devices in station mode (STAs). The AP announces the BSS through beacon messages containing its layer 2 address (BSSID) and the network identifier (SSID). On layer 3, the AP typically incorporates additional functionality such as routing and centralized services, e.g., device configuration by DHCP and name resolution via DNS. Station devices associate with the AP and leave all (coordination of) network functionality to the AP.

In an ad-hoc mode network, called Independent BSS (IBSS), *all participating devices* in ad-hoc mode jointly establish and announce the network through beacon messages. Lack of support for fundamental ad-hoc mode functionality [3], [11]–[13], [15] greatly reduces the number of devices that *can* participate in ad-hoc mode networks in the first place. Also, distributed network operation entails several drawbacks that are absent in BSS networks. First, medium access without a central entity results in frequent collisions on the medium, subsequent back off times and thus reduced network performance. Second, ad-hoc mode networks exhibit a random, dynamic topology, making layer 3 functionality such as routing and addressing a challenging task. Third, device configuration and address resolution, if established in a distributed fashion, require costly multi-hop updates and look-up events.

We argue that, given mobile AP devices, mobile infrastructure mode networks are simpler, more convenient, and compatible to more devices. This practicality and the inherent AP functionality in current mobile devices motivates the use of interconnected infrastructure mode networks in MA-Fi.

B. Mobility Support

Both the infrastructure and ad-hoc mode support station mobility [16]. However, the respective mechanisms differ due to the different network characteristics.

In infrastructure mode, mobile devices assume that APs broadcasting an identical SSID belong to the same Extended Service Set (ESS) [16] in the same overall network. When leaving the range of an AP, stations simply associate to another AP with the same SSID. In an ESS, such a handover is handled by adjusting the layer 2 routing to reflect the new location of the client. Hence, mobility support is entirely managed by the network infrastructure, leaving clients merely with the task of changing their AP association.

In ad-hoc IBSS topologies, devices connect to networks jointly provided by *multiple stations* announcing the same SSID, instead of single APs. Since devices establish routing cooperatively, mobility induces topological changes, thus requiring active maintenance of the routing topology. Ad-hoc routing protocols accomplish this task at the expense of maintenance overhead at each node.

MA-Fi combines both approaches in a two tier hierarchy using exclusively the 802.11 infrastructure mode: MA-Fi-enabled devices (RONs) offer ESS-like mobility support by providing 802.11 infrastructure mode networks to which unmodified station devices (STANs) connect. Moreover, RONs interconnect by means of infrastructure-mode links to form a backbone network while maintaining the flexibility, topology, and routing of an IBSS.

IV. MA-Fi DESIGN

Our design of mobile wireless networking in the 802.11 infrastructure mode reflects the functional role distinction of access points (AP) and stations (STA) in a two-tiered hierarchy of routing nodes (RONs) and station nodes (STANs). We introduce the resulting network topology and describe how MA-Fi facilitates multi-hop routing and addressing. Leveraging the resulting functional hierarchy, we propose an efficient topology control mechanism that allows MA-Fi networks to substantially reduce the number of devices that make up the multi-hop network, minimizing traffic and energy overhead. MA-Fi supports legacy 802.11 energy saving mechanisms in STANs and opportunistically duty cycles RONs to optimize energy consumption. Last, our design incorporates proven WPA2 and 802.1X mechanisms to address the security shortcomings of WEP-based ad-hoc mode networks.

A. Network Design

MA-Fi strives to provide the characteristics of mobile IBSS-based networking building on 802.11 infrastructure mode BSSs. Following the role distinction in infrastructure mode networks, we thus distinguish between two types of devices. *Routing nodes* (RONs) are capable of advanced networking functionality by providing AP functionality and services such as DHCP and DNS. In addition, unmodified 802.11 *station nodes* (STANs) participate in the network by associating to a BSS but can not contribute to its operation.

MA-Fi's network design thus entails four challenges:

i) Interconnection of isolated BSSs to establish an IBSS-like mobile network topology.
ii) Provision of legacy BSSs to STANs offering DHCP, DNS, and routing gateway functionality.
iii) Multi-hop IP routing between disjoint 1-hop BSSs.
iv) Support for RON and STAN mobility.

In this section, we first introduce the detailed design of MA-Fi networks addressing the first two challenges (Section IV-A1). We then present our adaption of an ad-hoc routing protocol (Section IV-A2) before illustrating the support for device mobility in MA-Fi (Section IV-A3).

1) Network Construction and Operation: Figure 1 illustrates the schematic network topology of MA-Fi in comparison to an ad-hoc mode network. In contrast to a collection of devices with homogeneous functionality, MA-Fi creates a two-tier functional hierarchy. In this hierarchy, RONs i) provide *legacy BSSs* for STANs and serve as DHCP server, DNS server, and routing gateway and ii) interconnect by providing a designated *backbone BSS* at each node and associating to other RON's backbone BSSs as stations.

This requires RONs to simultaneously operate as an AP and as a station in a number of foreign BSSs. In contrast to multi-radio devices designated for wireless mesh networks, MA-Fi assumes prevalent commodity Wi-Fi devices with a single radio and builds on *network virtualization* (cf. [30] for example) to establish multiple virtual network interfaces. Wireless network virtualization is inherently supported in Linux

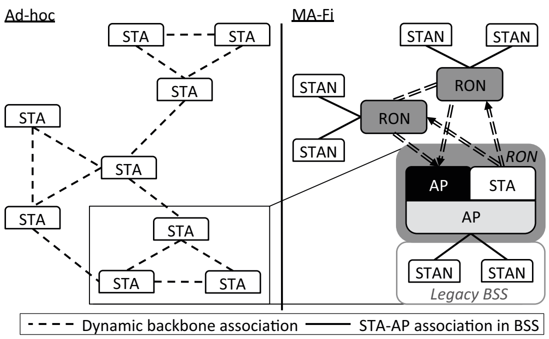


Fig. 1. Topological illustration of an ad-hoc mode network (left) and an equivalent MA-Fi network (right). RONs establish a meshed backbone network that connects the legacy networks provided at each RONs .

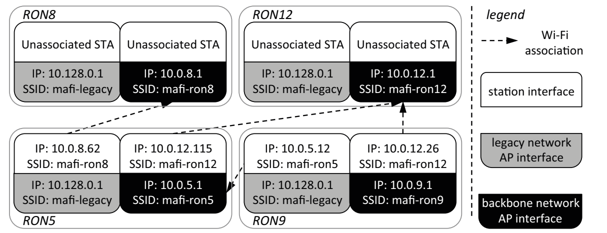


Fig. 2. RONs operate multiple virtual interfaces in station (STA) or access point (AP) mode. Identical AP interfaces at RONs span a continuous legacy network, while RONs connect to backbone networks of other RONs as stations.

and current Windows OSs, is feasible in Mac OS X through TUN/TAP support, and is becoming available in Android through mac80211-compliant SoftMAC drivers, making MA-Fi widely applicable in practice.

RONs *interconnect* to form a backbone network by periodically scanning for the beacons of other backbone BSSs and associating using virtual station interfaces that are created as required. Furthermore, *providing a legacy BSS* to STANs is straightforward, as 802.11 AP, DHCP, DNS, and gateway functionality is ubiquitously supported by current OSs and 802.11 Wi-Fi cards. Finally, RONs bootstrap their backbone AP interface by randomly choosing a $/24$ subnet from a large private address space, e.g., $10.0.0.0/9$, to avoid collisions and selecting the first IP from the respective subnets.

While MA-Fi thereby constructs an IBSS-like multi-hop network on layer 3, it does not provide a continuous layer 2 network and broadcast domain that is equivalent to an IBSS. RONs therefore encapsulate layer 2 broadcasts, e.g., for ARP requests, and forward them to other legacy BSSs.

2) Multi-hop Routing: To establish multi-hop routing that accounts for mobility of RONs and STANs, we adapt the DYMO (Dynamic MANET On-demand Routing) [22] routing protocol to operate within the multi-interface, multi-network design of RONs. MA-Fi is independent of the specific routing protocol and its proactive or reactive type. We chose DYMO for its (more) recent standardization documentation, hybrid character, and modular Linux kernel module implementation.

The multi-interface design of RONs affects the reliance of DYMO on broadcasts to sense new neighbors and distribute routing information. RONs mimic broadcasts to all associated RONs by sending and receiving routing messages on *all* active interfaces simultaneously. While this creates overhead due to multiple transmissions per broadcast, it allows for a highly controllable and adaptable routing topology. Our evaluation shows in Section V-A that this overhead does not influence routing performance.

As STANs are unmodified station devices, they route all traffic over the routing gateway, i.e., the RON, of their current legacy BSS. RONs thus serve as routing proxies that hide the routing complexity and dynamics of the routing backbone from STANs by discovering and recovering routes for their associated STANs.

3) Mobility Support: To support STAN mobility, RONs provide a *continuous legacy BSS* in the overall network. All RONs therefore provide an identical legacy BSS in terms of the SSID, the MAC and IP of the gateway interface, and the IP subnet distributed via DHCP (see Figure 2). MA-Fi thus leverages the inherent 802.11 handover mechanisms typically used to switch between APs in an ESS to roam between RONs. Reusing the same global IP address space and the MAC and IP of the gateway interface avoids extra DHCP and ARP requests in the case of STAN handovers.

RON mobility is accounted for by RONs monitoring their associations and scanning for additional backbone BSSs. Analogous to a neighbor change in ad-hoc mode routing, a RON recovers all routes that traversed a recently terminated association. Furthermore, RON mobility influences the routing backbone topology. To compensate for missing legacy BSS coverage after a RON leaves the network or to balance the number of legacy BSSs in a densely populated area, we propose an efficient topology control mechanism in the next section.

B. Energy Efficiency

MA-Fi improves on the energy efficiency of ad-hoc mode networks in two aspects. By minimizing the number of active RONs, inactive RONs and legacy devices may leverage the PSM support in 802.11 station mode (Section IV-B1). Duty cycling of active RONs affords further energy saving in the routing backbone and legacy BSS (Section IV-B2). In this paper, we do not address energy efficiency in routing. Similarly, as we focus on commodity devices, we regard layer 1 or layer 2 optimizations as outside of the scope of this paper.

1) Topology Control: RON functionality exhausts battery life quicker than STAN functionality, due to virtualizing multiple interfaces and performing additional routing functionality. In contrast to homogeneous ad-hoc mode networks, the infrastructure mode allows capable devices to adjust their role between active RON or inactive RON/STAN to save energy. Hence, RONs in MA-Fi strive to minimize the routing backbone while providing sufficient coverage. To this end, RONs communicate status indicators, for example the battery status, number of associations, as well as number, activity, and routes of stations, in 802.11 beacon frames via beacon stuffing [31]. This way, nearby RONs learn the status and number of RONs and legacy BSS in their transmission range. Based on this information, active RONs that observe a number of networks equal or greater than a threshold N may switch to STAN functionality, i.e., become inactive. Inactive RONs that observe fewer than N

networks or a resource limited neighboring RON will switch to RON functionality to supplement the overall network.

Topology adaptations require a handover of STANs, as supported by the native 802.11 handover mechanisms, as well as a recovery of the respective routing information. In the latter aspect, MA-Fi's design is equivalent in to ad-hoc mode networks that require route recoveries as well. However, due to this overhead, RONs switch roles only if necessary, depending on the mobility and current state of devices.

In this design, MA-Fi realizes the goals of topology control mechanisms in ad-hoc or sensor networks, e.g., Span [27]. In contrast to ad-hoc mode networks, MA-Fi is able to adjust both the communication functionality, e.g., routing duties, and the networking functionality, i.e., operating as RON or STAN. Furthermore, operating as STAN allows devices to go to power save modes, a functionality current ad-hoc mode implementations do not support. In this, MA-Fi provides a viable basis for real-world implementations and optimizations of energy-conserving approaches. We evaluate the energy consumption in the respective functional roles in Section V-B2 and the savings achieved by our mechanism in Section V-B1.

2) RON Duty Cycling: Topology control and support of PSM in STANs already offer an improvement over real-life ad-hoc mode networks. However, active RONs, in equivalence to existing approaches [27], expend a relatively large amount of energy if they are continuously awake.

MA-Fi improves upon an always-on backbone network by *opportunistic duty cycling* of active RONs. RONs hence aim for maximal sleep intervals while adhering to their functionality in the network, such as provision of the legacy BSS, routing, and traffic forwarding. RONs therefore sleep for a multiple of their advertised beacon interval and wake up periodically to receive messages. Notably, we refrain from client–server negotiation of sleep intervals, such as in *DozyAP* [28], as we can not realistically assume STANs to support the advanced functionality. Instead, we build on two observations: i) STANs decide autonomously whether to switch to sleep mode and ii) 802.11 stations allow for a small number of missed beacon frames before disassociating.

In each interval, RONs turn on their radio and broadcast beacon frames and listen for 802.11 frames sent by STANs, e.g., probe request or Null frames to test the availability of the current AP. If no frame is received, RONs opportunistically turn their radio off and sleep for a pre-defined interval. However, to ensure on-demand availability, for example for route discoveries initiated by STANs or forwarded by other RONs, RONs stay awake for the next beacon interval if they received a frame in the current one. As such, RONs stay available for routing or forwarding duties while conserving energy opportunistically.

This design entails a trade-off between the availability and response time of RONs, with regard to the layer 2 retransmission of missed frames, and the achievable sleep intervals. We empirically evaluate this trade-off in Section V-B2.

C. 802.1X Security

Network provision in the 802.11 infrastructure mode inherently supports WPA2 network security. To allow for 802.1X user authentication, we propose a distributed RADIUS implementation that allows for insertion and removal of user credentials. As RADIUS databases are of negligible size even for large number of users[3], RONs continuously replicate and update the respective RADIUS database among themselves using Lamport timestamps. This ensures response times comparable to single-hop or wired 802.1X authentication and provides redundancy. In contrast to available ad-hoc mode implementations, MA-Fi thus supports state-of-the-art network security to encrypt and protect traffic.

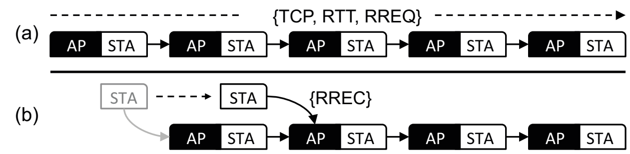


Fig. 3. Topologies to evaluate (a) throughput, round trip time and route request delay and (b) route recovery delay in case of STAN mobility.

V. Evaluation

We compare the performance of our MA-Fi implementation with ad-hoc mode networks (Section V-A). To assess the improvements in energy efficiency, we evaluate our topology control mechanism using real-world mobility traces (Section V-B1). We furthermore evaluate our duty cycling approach through real-world measurements and mobility trace-driven simulations (Section V-B2). Last, we briefly show that MA-Fi networks support 802.1X authentication with comparable performance as wired networks (Section V-C).

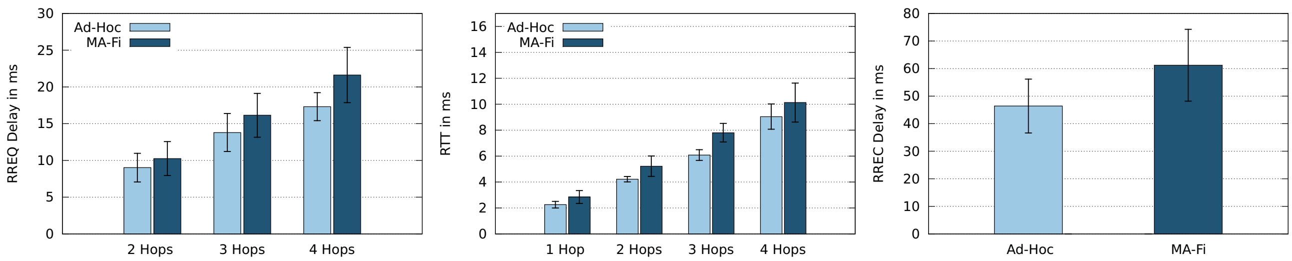
A. MA-Fi Network Performance

Our evaluation uses netbook devices as RONs. The netbooks have a dual-core 1.5 GHz CPU and an Atheros AR9285 802.11n wireless card, run Ubuntu 12.10 and execute our adapted DYMO protocol. We regard the netbooks as a good estimate of the real-life feasibility of MA-Fi, as the netbooks possess neither top-tier processing power nor specialized wireless hardware and are likely to be found in real-life scenarios. For comparison of the ad-hoc mode between different vendors and 802.11n drivers, we use Apple MacBook Pro devices with 2.4-2.8 GHz Intel Core 2 Duo CPUs and Broadcom BCM43xx 802.11n wireless cards running OS X 10.6. We do not optimize the devices in terms of 802.11n parameters or Wi-Fi driver modifications and all AP interfaces use the same channel.

In all experiments, five netbooks were placed in a straight line without obstacles, separated by about 20 meters, and are thus in a single interference domain. We manually set the routes to obtain a strict multi-hop topology, as shown in Figure 3(a). RONs are interconnected through their backbone networks and no STANs were associated to the respective legacy networks.

1) Throughput: We first evaluate the throughput of the ad-hoc mode and MA-Fi using *iperf*. Figure 4 shows the average results and their standard deviation for 30 runs of 30 sec in comparison to ad-hoc mode transmissions on Linux- and OS X-driven devices. In both configurations, the ad-hoc mode throughput between modern, identical devices did not exceed

[3]Length of passphrase multiplied by the number of users, i.e., 300 kB for 10000 users with keys of, on average, 30 Byte.



(a) RREQ delay (b) RTT (c) RREC delay

Fig. 5. Route establishment, round trip time, and route recovery performance of MA-Fi over increasing hop counts, in comparison to the 802.11 ad-hoc mode.

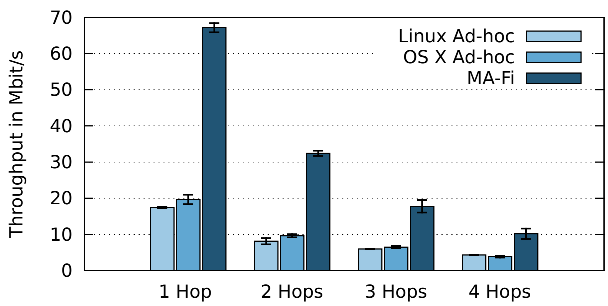


Fig. 4. Multi-hop TCP throughput of MA-Fi in comparison to ad-hoc mode.

20 MBit/s. In fact, the 802.11 frames captured by *wireshark* consistently showed data rates of or below 54 MBit/s, indicating that the network operates merely in 802.11g mode. These results highlight both the lack of support for the ad-hoc mode and the contrasting high performance of infrastructure mode networks. Throughput in MA-Fi shows 802.11n performance, with up to 67 MBit/s on the first hop and 32 MBit/s and 17 MBit/s on the second and third hop, respectively.

These results support our design in three aspects. First, available devices and operating systems show significantly better support for the infrastructure mode than for the ad-hoc mode. Second, multi-hop throughput in MA-Fi constantly exceeds ad-hoc mode throughput over all measured path lengths. Specifically, MA-Fi achieves at least 230 % of the ad-hoc mode throughput over all measured hop counts. Furthermore, the 802.11n capability of RONs supports our two-tier design as the backbone network accommodates a considerable larger bandwidth than the ad-hoc mode. Third, first-hop throughput in MA-Fi, as observed in each legacy BSS, exceeds ad-hoc mode throughput by up to 340 %. Each RON is thus able to provide a high-performance network to a large number of unmodified, associated STANs in his legacy network.

2) Virtualization Delay: We further analyze the impact of operating multiple interfaces. Due to the delayed processing of packets in the protocol stack caused by cycling through the established interfaces, we expect an increase in the response time of RONs. We refer to [30] for an in-depth discussion of switching time and algorithms.

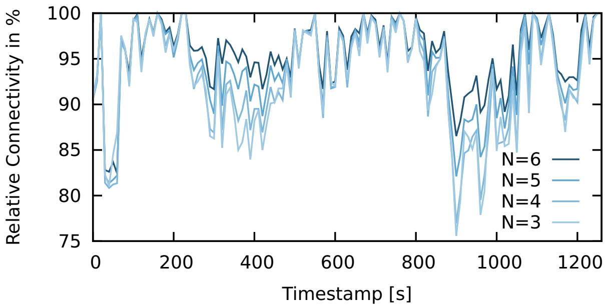
Figure 5(a) shows the average delay and standard deviation of 30 route requests (RREQ) in MA-Fi and in ad-hoc mode networks. In MA-Fi, DYMO requires an additional 1.5 ms per hop to establish routes. This is due to route requests traversing multiple independent networks per hop, rather than a single broadcast per hop as in ad-hoc mode. We obtain similar results when measuring the round trip time (Figure 5(b)). Finally, Figure 5(c) shows the average time and standard deviation of recovering a four-hop route (RREC) for a STAN if the next hop RON fails or in case of STAN mobility (see Figure 3(b)). We observe a slight increase in the order of 15 ms over the ad-hoc mode; this is again due to the recovering RON iterating through multiple networks to re-establish the route. We conclude that MA-Fi introduces only a small virtualization delay, which in turn is outweighed by greatly improved throughput.

B. Energy Efficiency

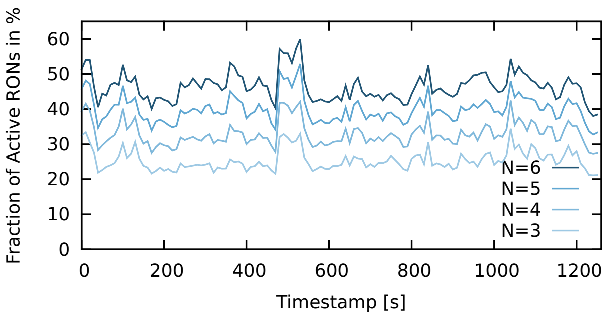
To assess the energy efficiency of MA-Fi, we first evaluate the effectiveness of our topology control scheme. We further investigate the energy consumption of RONs and the energy savings achieved by duty cycling.

1) Topology Control: The number and distribution of devices capable of establishing the routing backbone, i.e., active devices in ad-hoc mode networks and RONs in MA-Fi, determines the topology, connectivity, and energy consumption of the mobile network. We thus evaluate how our topology control mechanism balances the number of active RONs and the network connectivity. To this end, we use the real-world MANIAC mobility trace [32] which lists the connectivity patterns of 21 devices in 802.11 ad-hoc mode. Despite its small sample size, we use this trace instead of larger Bluetooth- or GPS-based mobility traces for its real-world ad-hoc Wi-Fi connectivity measurements. This is because, for our evaluation, Bluetooth-based traces overestimate connectivity because of Bluetooth's short range while GPS-based traces require (unrealistic) connectivity assumptions based on signal propagation and transmission range. To compare the network connectivity of the ad-hoc network with MA-Fi, we regard all devices in the trace as capable of serving as RONs. However, in contrast to ad-hoc mode networks, each RON may *additionally* serve a large number of STANs as AP, allowing a significantly larger overall network with the *same* connectivity.

Each RON observes the status messages of all neighboring RONs at each timestamp of the trace: If it overhears fewer than N active backbone BSSs, it will act as RON at the next timestamp, or as STAN otherwise (cf. Section IV-B1). The goal of this study is to investigate the impact of N and to derive a real-world base line for N. Hence, we vary N and measure the resulting *network connectivity*, i.e., the largest connected component, over the *number of active RONs*. All nodes only use purely *local* knowledge and initially act as STANs.



(a) Network connectivity relative to ad-hoc mode.



(b) Fraction of active RONs relative to ad-hoc mode.

Fig. 6. Network connectivity under topology control in real-life mobility [32].

Figure 6(a) shows the network connectivity for $N \in \{3, 4, 5, 6\}$ over the timestamps of the trace. Figure 6(b) illustrates the corresponding fraction of active RONs comprising the largest connected component. The results of both figures are normalized to the results of operating every device in 802.11 ad-hoc mode.

We observe in Figure 6(a) that MA-Fi achieves a network connectivity between 75 % and 100 % of the ad-hoc mode for all values of N. The generally lower connectivity is due to the fact that MA-Fi by design utilizes only a subset of all capable devices. Moreover, for periods with a connectivity exceeding 90 % of the ad-hoc mode, N has no significant influence, as indicated by the overlapping curves. This is due to a densely clustered network topology that provides multiple routes between all devices. Conversely, we also identify periods of diverging connectivity with respect to N. In these periods of the trace, all devices are sparsely connected, resulting in merely few paths through the backbone network. Hence, lower values of N tend to disconnect border regions of the network, causing a slightly lower connectivity. Still, even for $N = 3$ the overall connectivity averages at 92.83 % of the ad-hoc mode and never drops below 75 %, highlighting the effectiveness of MA-Fi's topology control mechanism.

In contrast to the connectivity, the fraction of active RONs in the network is highly sensitive to changes of N (see Figure 6(b)). Despite showing equivalent behavior over time for all values of N, increasing or decreasing N by 1 causes the fraction of active RONs to consistently increase or decrease by 5 % to 10 %. As a result, the fraction of active RONs ranges from 45 % ($N = 6$) down to 25 % ($N = 3$). N thus affords an intuitive trade-off between a more stable network topology

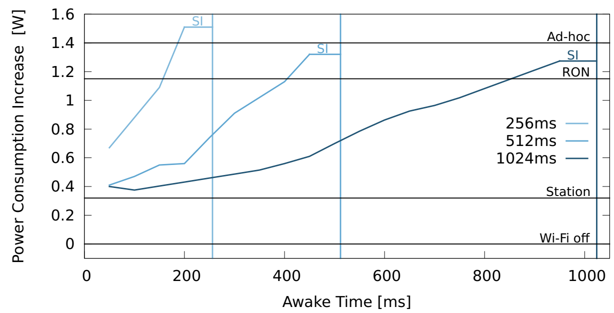


Fig. 7. Energy savings, compared to 802.11, follow a trade-off between the switching interval (SI) of the Wi-Fi card and 802.11 driver, the response time of the network and the awake time in each duty cycle interval (256/512/1024 ms).

at the cost of more active RONs and sparser, more volatile backbone networks that require less RONs.

Recalling the results of Figure 6(a), we conclude that MA-Fi and its local topology control scheme successfully establish mobile networks with a connectivity comparable to the ad-hoc mode, yet with a significantly smaller fraction of backbone devices. Moreover, since each RON potentially serves multiple client devices, MA-Fi's topology provides an efficient basis for reducing the energy consumption of the entire network.

2) RON Duty Cycling: We realize RON duty cycling in a proof-of-concept implementation for Linux that allows to periodically (de)activate the Wi-Fi card and (un)load the driver. To measure the energy consumption of RONs, we follow the setup detailed in [33], [34], i.e., we trace the voltage at a shunt resistor in series with the mobile device using an oscilloscope and determine the power draw. Note that, as the Wi-Fi cards are built into the netbooks, we are only able to measure the energy consumption of the whole device. All energy consumption results thus are the difference between the measured consumption and the devices' base energy consumption (Wi-Fi off)[4] of 6.3 W. We further refrain from artificial traffic patterns and varying numbers of associated STANs or RONs and instead only evaluate the energy consumption of an established yet idle network. This is because RONs stay awake to process traffic and in that time consume energy as required by the 802.11 hardware regardless of our mechanism (cf. Section IV-B2). Furthermore, different combinations of Wi-Fi cards and 802.11 drivers show vastly different interactions with the AP in terms of probe requests and Null frames sent as well as subsequent (dis)association decisions. To ensure real-world applicability, we thus associate a set of 5 STANs running Android, Linux, OS X, and Windows 7 with the RON's legacy BSS to empirically derive bounds for awake times and duty cycle intervals. The devices utilize Broadcom, Intel, Ralink, and Atheros Wi-Fi cards and the respective drivers.

Figure 7 shows the energy consumption of a netbook serving as AP for duty cycling intervals of 256 ms, 512 ms, and 1024 ms over the awake time per duty cycling interval in steps of 50 ms. The figure furthermore provides the energy consumption of the device with Wi-Fi off, in station, AP, and ad-hoc mode

[4]Wi-Fi off: Idle system after boot, no active wireless network interface, 802.11 driver unloaded.

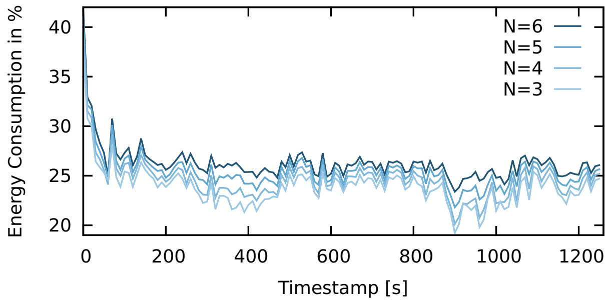


Fig. 8. Cumulative network-wide energy consumption of duty cycled RONs and associated STANs relative to ad-hoc mode consumption.

as static references. The vertical lines indicate the end of the respective duty cycling interval. The results confirm the intuitive assumption that longer awake times per duty cycling interval increase the energy consumption. Also, they highlight the trade-off between the response time of the network, influenced by the duty cycle interval, the awake time necessary to maintain station associations, and the switching interval (SI) of the Wi-Fi card and 802.11 driver. We empirically measured the minimum awake time to be 20 % of each interval for switching intervals of 40 ms. For smaller awake time ratios, too many beacon frames are omitted and Null frames unacknowledged, causing unmodified STANs devices to disassociate. Intervals in which the start-up time takes up a large fraction increase the energy consumption further and suffer from the overhead of managing the duty cycling. As such, intervals of 256 ms are limited to savings of at most 42 % (0.48 W) compared to the baseline result of always-on AP operation. Decreasing this fraction, intervals of 512 ms and 1024 ms afford comparable savings of up to 59 % (0.68 W) and 62 % (0.72 W), when adhering to the minimum awake time of 100 ms and 200 ms, respectively, thereby providing an adjustable parameter with regard to the network response time.

Figure 8 shows the network-wide energy consumption of the simulated network using the previous measurement results and our duty cycling scheme, again normalized to the ad-hoc mode. Each RON duty cycles using 512 ms intervals with 100 ms awake times, but remains active for 2 s after establishing a new connection with a neighboring RON or STAN. The figure illustrates that the network-wide energy consumption, including RONs and inactive RONs, quickly converges from initially 40 % to an average of 25 % of the ad-hoc mode. We ascribe the initial convergence phase to the fact that building the backbone network involves establishing a high number of new connections among RONs, preventing RONs from sleeping. Yet, once the network has stabilized after about 90 s (1 s = 1 timestamp), RONs can take full advantage of duty cycling. Again, the choice of N impacts the number of RONs and number of connections, higher values of N thus lead to higher energy consumption because of a densely connected backbone.

Last, we analyze the impact of duty cycling on the response time of the network by repeating the round trip time measurement from Section V-A (cf. Figure 5(b)). We again employ a 512 ms interval with an awake time of 100 ms and measure the round trip time of 100 packets for each hop count. To artificially model uncoordinated traffic patterns originating from STANs, the sending device sends each packet with a randomly selected time offset within the duty cycle interval of 512 ms. Table II lists the average measured round trip times for each hop count in comparison to the results without duty cycling from Section V-A. On average, duty cycling prolongs the round trip time by roughly 50 % of the sleep interval as packets are only processed if received while the RON is awake. As RONs stay awake for another interval in case they process traffic, returning packets experience no further delay.

TABLE II. Impact of an example duty cycling schedule (100 ms awake time in 512 ms intervals) on the round trip time in MA-Fi.

	1 hop	2 hops	3 hops	4 hops
RON	2.85 ms	5.22 ms	7.80 ms	10.13 ms
512/100	187.91 ms	194.24 ms	218.32 ms	225.59 ms

In this, the results affirm our goal of adjustable network response time with regard to the implemented duty cycling schedule and thus energy savings. Note that RONs may balance these performance factors against each other based on the recently observed network behavior, i.e., traffic demands as well as leaving and joining devices. From this, RONs can derive more appropriate parameter settings for the duty cycling interval and communicate these to other RONs in order to achieve network-wide synchronization.

C. Security

To evaluate our proof-of-concept implementation of a distributed, replicated RADIUS database, we measure the association time of RONs implementing 802.1X authentication. For RONs that do not employ duty cycling, we observe an association time of 1 s on average, comparable to the observed association time of our university's stationary 802.1X-secured Wi-Fi network. Only with a duty cycling interval of 512 ms does the association time rises to 13.25 s, on average, due to retransmitted association requests. In this, we observe a back-off interval of 6 s, i.e., subsequent retries at 7 s, 13 s, and 19 s, etc. Integrating this interval with a duty cycling schedule would allow reducing the association time.

VI. Conclusion

In this paper, we proposed MA-Fi, a real-world applicable and high-performance approach to mobile wireless networking in 802.11 infrastructure mode. In comparison to the 802.11 ad-hoc mode, MA-Fi achieves i) a throughput of up to 340 % and comparable performance in routing, ii) a reduction in energy consumption of up to 62 % by leveraging the 802.11 PSM support in infrastructure mode and by opportunistic duty cycling of backbone RONs, iii) a functionality-driven topology control that establishes an energy-efficient network structure while maintaining connectivity with as little as 25 % of the required ad-hoc mode devices, and iv) a ubiquitous, flexible basis for mobile wireless networking based on the compatibility and support for the infrastructure mode. Our design builds on the observation that every 802.11 capable device supports the infrastructure mode. We leverage this large set of available target devices to utilize network virtualization in a small subset to build the multi-hop network topology. The resulting two-tier architecture of unmodified 802.11 devices and backbone devices then hides the complexities of ad-hoc network provision, multi-hop routing, mobility management, and energy saving mechanisms from commodity devices of mobile participants.

We evaluate MA-Fi using a prototype Linux implementation and compare its performance against the 802.11 ad-hoc mode. Our results show that the impact of multiple virtual interfaces on response times and routing performance is negligible. By means of simulation on real-world mobility traces, we highlight that MA-Fi achieves comparable network connectivity in realistic mobility scenarios. MA-Fi thus offers a i) practical, ii) high-performance, iii) energy-efficient, and iv) readily deployable basis for applications and research in mobile wireless networking, uncoupling the applicability of mobile networking from the vanishing 802.11 ad-hoc mode. We will moreover publish the MA-Fi source code for use by others.

Acknowledgements

We are grateful for funding by the DFG Cluster of Excellence on Ultra High-Speed Mobile Information and Communication (UMIC).

References

[1] Shu Liu and Aaron D. Striegel. Exploring the potential in practice for opportunistic networks amongst smart mobile devices. In *Proc of the ACM Intl. Conf. on Mobile Computing and Networking (MobiCom)*, 2013.

[2] Roy Friedman and Noam Mori. 3dls: density-driven data location service for mobile ad-hoc networks. In *Proc. of the ACM Intl. Symp. on Mobile ad hoc networking and computing (MobiHoc)*, 2009.

[3] Sacha Trifunovic, Bernhard Distl, Dominik Schatzmann, and Franck Legendre. Wifi-opp: ad-hoc-less opportunistic networking. In *Proc. of the ACM Workshop on Challenged Networks (CHANTS)*, 2011.

[4] Cong Shi, Vasileios Lakafosis, Mostafa H. Ammar, and Ellen W. Zegura. Serendipity: enabling remote computing among intermittently connected mobile devices. In *Proc. of the ACM Intl. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2012.

[5] Moo-Ryong Ra, Bin Liu, Tom F. La Porta, and Ramesh Govindan. Medusa: a programming framework for crowd-sensing applications. In *Proc. of the ACM Intl. Conf. on Mobile Systems, Applications, and Services (MobiSys)*, 2012.

[6] Kanchana Thilakarathna, Aline Carneiro Viana, Aruna Seneviratne, and Henrik Petander. Mobile social networking through friend-to-friend opportunistic content dissemination. In *Proc. of the ACM Intl. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2013.

[7] Bo Han, Pan Hui, V.S. Anil Kumar, Madhav V. Marathe, Guanhong Pei, and Aravind Srinivasan. Cellular traffic offloading through opportunistic communications: a case study. In *Proc. of the ACM Intl. Workshop on Challenged Networks (CHANTS)*, 2010.

[8] Yong Li, Guolong Su, Pan Hui, Depeng Jin, Li Su, and Lieguang Zeng. Multiple mobile data offloading through delay tolerant networks. In *Proc. of the ACM Intl. Workshop on Challenged Networks (CHANTS)*, 2011.

[9] NETGEAR Ad-Hoc Support. [Online] http://kb.netgear.com/app/answers/detail/a_id/1069/kw/ad-hoc_mode/r_id/100109.

[10] D-Link Ad-Hoc Support. [Online] http://www.dlink.com/uk/en/support/faq/access-points-and-range-extenders/access-points/dwl-series/why-cant-i-get-the-advertised-speed-and-performance-when-in-ad-hoc-mode.

[11] Google. Ad-Hoc Support in Android. [Online] http://code.google.com/p/android/issues/detail?id=82.

[12] iOS Developer Library. Document Transfer Strategies. [Online] http://developer.apple.com/library/ios/technotes/\\tn2152/_index.html.

[13] MSDN Developer Forums. Wireless issues. [Online] http://social.msdn.microsoft.com/forums/wpapps/en-US/01ecb5da-457c-4ca9-9a63-24f6e224c2e3/wireless-issues.

[14] Commotion Wireless. Supported Hardware and Devices. [Online] https://code.commotionwireless.net/projects/commotion/wiki/Supported_\\Hardware,https://commotionwireless.net/docs/supported-devices.

[15] Ashish Sharma, Vishnu Navda, Ramachandran Ramjee, Venkata N. Padmanabhan, and Elizabeth M. Belding. Cool-tether: energy efficient on-the-fly wifi hot-spots using mobile phones. In *Proc. of the ACM Intl. Conf. on Emerging Networking Experiments and Technologies (CoNext)*, 2009.

[16] IEEE. 802.11 standard. [Online] http://standards.ieee.org/findstds/standard/802.11-2012.html.

[17] OS X Mavericks: Create a computer-to-computer network. [Online] http://support.apple.com/kb/PH13796.

[18] Create WPA2 adhoc is Open, not encrypted. [Online] https://bugs.launchpad.net/ubuntu/+source/network-manager/+bug/905748.

[19] Wi-Fi Alliance. Wi-Fi Direct White Paper. [Online] http://www.wi-fi.org/knowledge_center_overview.php?docid=4685.

[20] Mi Kyung Han, Apurv Bhartia, Lili Qiu, and Eric Rozner. O3: optimized overlay-based opportunistic routing. In *Proc. of the ACM Intl. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2011.

[21] Han Cai and Do Young Eun. Aging rules: what does the past tell about the future in mobile ad-hoc networks? In *Proc. of the ACM Intl. Symp. on Mobile ad hoc networking and computing (MobiHoc)*, 2009.

[22] I. Chakeres and C. Perkins. Dynamic MANET on-demand (DYMO) routing. Internet Draft, March 2009.

[23] V. Navda, A. Kashyap, and S.R. Das. Design and evaluation of imesh: an infrastructure-mode wireless mesh network. In *Proc. of the IEEE Intl. Symp. on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*, 2005.

[24] K. N. Ramachandran, M. M. Buddhikot, G. Chandranmenon, S. Miller, Belding E. M. Royer, and K. C. Almeroth. On the Design and Implementation of Infrastructure Mesh Networks. *Proc. of the IEEE Workshop on Wireless Mesh Networks (WiMesh)*, 2005.

[25] IEEE. 802.11s standard. [Online] http://standards.ieee.org/findstds/standard/802.11s-2011.html.

[26] Yu-Chee Tseng, Chih-Shun Hsu, and Ten-Yueng Hsieh. Power-saving protocols for ieee 802.11-based multi-hop ad hoc networks. In *Proc. of the IEEE Intl. Conf. on Computer Communications (INFOCOM)*, 2002.

[27] Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. In *Proc. of the ACM Intl. Conf. on Mobile computing and networking (MobiCom)*, 2001.

[28] Hao Han, Yunxin Liu, Guobin Shen, Yongguang Zhang, and Qun Li. Dozyap: power-efficient wi-fi tethering. In *Proc. of the ACM Intl. Conf. on Mobile systems, applications, and services (MobiSys)*, 2012.

[29] Andreas Hafslund and Jon Anderson. 2-level authentication mechanism in an internet connected manet. In *Proc. of the Scandinavian Workshop on Wireless Ad-hoc Networks*, 2006.

[30] R. Chandra and P. Bahl. Multinet: connecting to multiple ieee 802.11 networks using a single wireless card. In *Proc. of the IEEE Intl. Conf. on Computer Communications (INFOCOM)*, 2004.

[31] Ranveer Chandra, Jitendra Padhye, Lenin Ravindranath, and Alec Wolman. Beacon-stuffing: Wi-fi without associations. In *Proc. of the IEEE Workshop on Mobile Computing Systems and Applications (HotMobile)*, 2007.

[32] L.A. DaSilva, A.B. MacKenzie, M.S. Thompson, and E.Q. Baumann. The maniac challenge: Educational experiences in ad hoc networking. *Pervasive Computing, IEEE*, 8(1), 2009.

[33] L.M. Feeney and M. Nilsson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In *Proc. of the IEEE Intl. Conf. on Computer Communications (INFOCOM)*, 2001.

[34] Atheros. Power Consumption and Energy Efficiency Comparisons of WLAN Products. [Online] http://www.qca.qualcomm.com/wp-content/uploads/2013/09/Power_Consumption_whitepaper.pdf.