A Mobile Access Gateway for Managing Intermittent Connectivity

Jörg Ott[1)] and Dirk Kutscher[2)]
[1)] Helsinki University of Technology, Networking Laboratory <jo@netlab.hut.fi>
[2)] Technologiezentrum Informatik (TZI), Universität Bremen <dku@tzi.uni-bremen.de>

***Abstract*— The Drive-thru Internet architecture allows exploiting intermittent connectivity by temporarily connecting to IEEE 802.11 WLAN access points at the roadside from moving vehicles. This poses numerous challenges to a mobile user's equipment: extreme networking characteristics such as short periods of connectivity, unpredictable disconnection times, and vastly varying transmission characteristics. Heterogeneous WLAN hot-spot installations may also require different authentication mechanisms and credentials. We have designed a mobile access gateway to deal with these issues on behalf of a user (group) in a moving vehicle and provide usable connectivity for applications without requiring manual operation. The gateway maximizes the use of short connectivity periods by detecting network access providing signaling functions for local application processes. It also allows using dedicated radio equipment to prolong connectivity periods. Finally, in selected multi-user scenarios, further performance improvements are conceivable by sharing (non-confidential) information across users and applications.**

I. Introduction

Mobile users and nomadic computing are today supported by two classes of networks: Cellular networks aim at providing ubiquitous connectivity, even across different service providers. However, their price-performance ratio is rather poor and temporary disconnections may still occur for various reasons. IEEE 802.11 WLAN hot-spots do not aim at seamless connectivity; their limited reach implies disconnection periods while the user is moving between locations. Hybrid approaches are pursued to keep users *always best connected* [1] [2] by combining access to different service providers or integrating wireless WAN and LAN to maximize connectivity, improve the achievable data rate, and minimize cost [3] [4].

In the Drive-thru Internet project, we rely on WLAN connectivity to provide affordable high-performance communications to mobile users and use dedicated as well as public hot-spots for Internet access. The cost for establishing and operating WLAN hot-spots can be quite low, and, since unlicensed operation is possible, deployment is not limited by regulations. As a result, WLAN has become an inexpensive commodity and the number of public hot-spot installations is ever-increasing: besides hotels, cafés, etc., particularly airports, train stations, gas stations, and service areas are covered, i.e., places serving commuters and travelers on the road.[1]

Working with (public) WLAN hot-spots usually requires manual user interaction, e.g., to (re)configure the WLAN interface, to authenticate with the wireless ISP [5] [6] [7], or to suspend, resume, and possibly reconfigure applications [8]. Working with hot-spots from (potentially fast) moving vehicles means that only a short connectivity window is available for establishing network access and carrying out the actual communication tasks [7]. To allow such tasks spanning multiple hot-spots without connectivity in-between, we have developed the Drive-thru architecture that conceals short-lived intermittent connectivity from applications [9] [10].

Regardless of the approach taken to provide wireless connectivity: all cases require sophisticated functions for network access, roaming, handover, authentication, cost and/or QoS optimization, etc. Such functionality may be located in the end user's device (e.g., as offered by multi-access PC cards and associated software for laptops) or may be implemented in a dedicated access device, such as MAR [3], the mobile router in the eMotion project [11], or the FleetNet access router [12].[2] These projects focus on offering ubiquitous connectivity (seamless handover and roaming) using mostly well-defined access control procedures and employing (variants of) mobile IP, i.e. they largely operate at the IP layer and below.

Performing access functions in separate devices offers numerous advantages: Dedicated radio equipment (including, e.g., external antennae mounted on top of a vehicle) provides better signal reception and prolonged connectivity periods [9]. Furthermore, a single router rather than multiple end systems accessing the same access point leads to more efficient utilization of the wireless medium and thus better performance [13]. Finally, an access router may be augmented to perform higher layer functions such as TCP performance improvement or caching. The major disadvantage is that, with multi-user scenarios, individual access charges across a common access router are difficult to account and bill for. Trust is considered less an issue since end users are expected to use secure communication protocols at least for sensitive data anyway.

This paper presents the design and implementation of a Drive-thru mobile access gateway (DT-MAG), a stand-alone device that serves mobile devices (within a vehicle) and connects them to hot-spots along the road. In contrast to the aforementioned routers, the DT-MAG also performs transport and application layer functions that raise numerous issues regarding security and persistence of information. A flexible and

[1]Examples include Agip gas stations and MAXI service areas in Germany, Neste A24 gas stations in Estonia, Statoil in Norway, and Texaco service stations in the UK as well as truck stops in the US.

[2]Or the multi access router developed in the 6WINIT project in support of IPv6-based mobile networks.

modular design allows various scenarios to be accommodated simultaneously. In section II, we briefly summarize the Drive-thru Internet architecture, in section III we review related work. We present usage scenarios in section IV and derive requirements for the DT-MAG in section V. The design and implementation of the DT-MAG are presented in section VI. Section VII summarizes our results and outlines future work.

II. Drive-thru Internet

As mentioned above, the Drive-thru Internet project [9] aims at providing Internet services to mobile users moving at high speeds. The objective of Drive-thru Internet is to enable access to Internet services by exploiting connectivity from conveniently located WLAN hot-spots that is temporarily established while a user traverses the hot-spot's coverage area. The Drive-thru architecture allows existing and future applications to take advantage of such potentially short and unpredictable periods [10]. It relies on a connection splitting approach where a proxy in the fixed network maintains long-lived connections on behalf of mobile clients that would otherwise be affected by intermittent connectivity [14]. Figure 1 depicts an overview of the Drive-thru Internet architecture.

The *Persistent Connection Management Protocol* (PCMP) is used for the communication between the mobile Drive-thru client and the Drive-thru proxy, allowing for creating and maintaining multiple persistent transport layer sessions despite frequent link layer disconnections. Moreover, Drive-thru Internet clients must be able to operate in today's *existing* WLAN infrastructure, which mostly consists of public hot-spots. In [7] we discuss the requirements of automatic WLAN hot-spot association in detail and describe our approach; in [15] we provide details of the automated authentication mechanism.

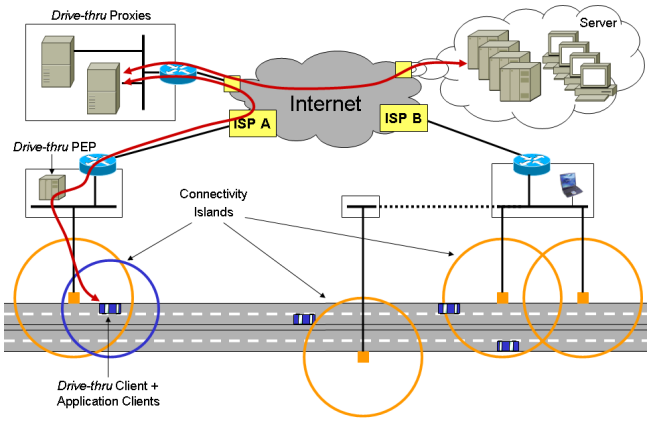

Fig. 1. Overview of the Drive-thru Internet Architecture

Aggregating wireless communications from multiple end-points, automatic hot-spot association, and persistent connectivity management are examples of services that can be provided by a dedicated gateway for Drive-thru Internet environments on behalf of one or more end user devices. The Drive-thru gateway concept extends the ideas of mobile routers such as the Mobile Access Router (MAR) described in [3] or the mobile router in [11] by providing specific support for intermittent connectivity that can be used for various scenarios such as nomadic computing, WLAN mobility and mobile networks. It is particularly the Drive-thru (session and) application layer functionality where a DT-MAG provides significant value-add beyond plain IP routing and mobility.

III. Related Work

Our work from the Drive-thru Internet project described in this paper addresses vehicular network access in general and focuses on providing dedicated gateway devices, their functionality, and the implications for the mobile users' devices. IP communications on the road has independently been studied in FleetNet [12] and Networks on Wheels, with a different focus and slightly different goals though: both projects primarily target inter-vehicle communications in wireless ad-hoc networks for traffic-related control information and data sharing across vehicles, the latter of which is also addressed in Hocman [16]. Hybrid network access for vehicles has been addressed, e.g., in OverDRIVE [17], IPonAir [4], and with MAR [3]. Dealing with temporary connectivity loss is studied in the eMotion project [11]. The latter two implement dedicated mobile routers to provide wireless network access, addressing multi-provider support at the IP layer and temporary connectivity interruptions at the transport layer, respectively. Finally, delay/disruption-tolerant networking [18] [19] deals with intermittent connectivity for asynchronous applications and Drive-thru clients and proxies conceptually resemble DTN routers to a certain degree. Many of the aforementioned projects also address authentication but all of them assume a well-known authentication mechanism. Gaining knowledge about heterogeneous hot-spots and the corresponding WISPs may be achieved by means of—standardized—service discovery mechanisms as has been discussed, e.g., for Wi-Fi alliance's smart client authentication [5] and FleetNet [20].

IV. Mobile Usage Scenarios

Mobile access routers in general and the DT-MAG in particular can be used in different settings. We can differentiate at least according to the following aspects: single-user vs. multi-user; dedicated gateway system vs. complementary software component on a user's laptop; and according to the accounting/trust relationships between users and the DT-MAG in the multi-user case. This results in the following scenarios:

1) A mobile user without a vehicle (or without any supportive infrastructure within a vehicle) may use arbitrary hot-spots for her communication needs. Obviously, such a user needs to carry her client-side Drive-thru infrastructure with her at all times (e.g., on her laptop). Using only her laptop for all functions, she is responsible for herself and there is no need for shared accounting/trust. Note that this case also includes multiple independent users in the same vehicle.

2) For a user alone in his car, a similar 1:1 trust relationship exists. However, wireless access, persistent connections, and

application support may be provided by physical a DT-MAG device that is part of the car's communication infrastructure.

3) Multiple users in a vehicle may use the same DT-MAG components with a shared trust relationship, e.g., for a family traveling together in a car.

4) Multiple users in a vehicle may use the same DT-MAG components without a shared trust relationship, e.g., passengers in a bus or on a train.

The degree of support provided by (or requested from) the vehicular infrastructure may differ (figure 2): as a simple access router, a DT-MAG may just provide wireless connectivity (the access function, AF, usually including authentication) or may also implement a shared Drive-thru client (DTC) offering persistent connections and application support. In the latter case, further application-specific functions (e.g. a shared web cache) may also be realized on the DT-MAG.

Except for case 1—where the user is in full control of her entire Drive-thru infrastructure at all times (fig. 2a)—we can further differentiate whether *i)* application sessions may persist across a user entering and leaving a vehicle or *ii)* they only last while the vehicular infrastructure components are available. Some users traveling with their laptops will presumably prefer type *i)* as this allows them to maintain persistent application sessions at all times (particularly if their time aboard the same vehicle is limited; e.g., short-distance commuters). This implies that the DT-MAG support is limited to wireless access functions (fig. 2b–2d). In contrast, users with their own laptops who remain aboard a vehicle for an extended period of time (such as long-distance travelers) and users accessing the Internet via a vehicle's built-in devices will find type *ii)* sufficient. In this case, the DT-MAG may provide persistent connections for the applications (fig. 2e and 2f).

Finally, for hot-spot access and Drive-thru proxy communications, mobile users need to authenticate with the respective service provider: If a DT-MAG provides wireless access (2b–2f), the users are required to share the access provider (since accessing multiple WISPs from the same wireless station adapter is usually not supported in practice). If the DT-MAG also acts as a Drive-thru client (2c–2f), the Drive-thru proxy (and hence the Drive-thru provider) must also be shared by the users (2e), unless the Drive-thru client can interact with multiple Drive-thru proxies and offers users a choice (2f).

V. Mobile Access Router Requirements

In a Drive-thru environment, a mobile node must find and gain access to hot-spots quickly to make most use of the potentially short connectivity period. While portable computers may well perform this function on their own, a dedicated DT-MAG device for Drive-thru clients may benefit users in numerous ways: it may offer dedicated high performance radio equipment, may be specifically designed to deal with rapidly changing connectivity[3], and, if shared among multiple users, may improve network utilization. Measurements have shown dramatic performance differences when comparing Drive-thru WLAN usage with and without external antenna [9].

[3]This may be of crucial importance depending on the operating system. For example, Microsoft Windows XP may take 30–60 s to detect and auto-configure wireless network interface upon first contact with a new access point, a period after which a connectivity island may have already passed.

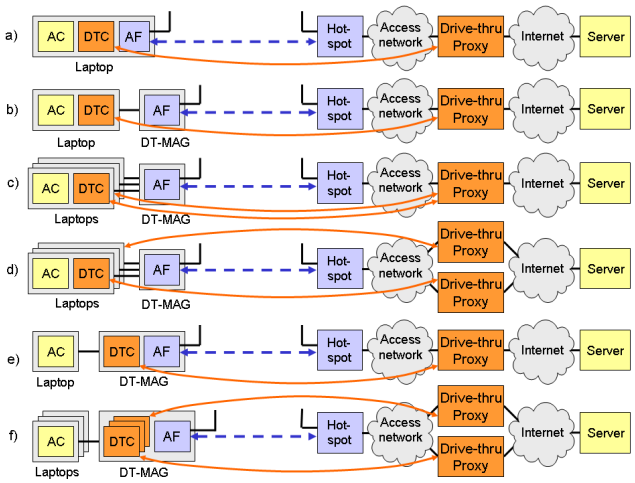

Fig. 2. Usage scenarios for a Drive-thru Mobile Access Gateway

The following list outlines the requirements for a DT-MAG, motivated by the goal to move as much Drive-thru-specific functionality as possible into the DT-MAG device to minimize dependencies on user equipment. The above scenarios are used to infer requirements for the distribution of these functions between a DT-MAG built into the vehicle and the user devices.

A. Detecting network access. The detection of network access involves both sensing link layer connectivity and testing whether a handover has been performed, i.e., in order to determine that a new IP stack configuration process has to be initiated. Detecting (and establishing) link layer connectivity is a perfect fit for a DT-MAG device since this function does not involve user-specific action and hence is easily sharable—and all users may benefit from router support for additional link layer technologies. E.g., in hybrid networking environments [1], the task for simultaneously probing different network interfaces and establishing network access on the optimal interface can best be provided by a dedicated device.

B. IP auto-configuration. When link layer connectivity has been established the IP auto-configuration process must be initiated, typically DHCP for IPv4 in today's hotspots, but other available configuration mechanisms (if any) must also be detected automatically. The DT-MAG is a good match for this function if only a single IP address for the entire vehicle is needed per wireless network that can be shared by all users.

Similarly, a DT-MAG needs to provide plain IP access router functionality to the user devices (e.g., DHCP and IP routing) to allow them to also connect transparently to the Internet when connectivity is available.

C. Network selection, authentication, and accounting. Typical hot-spot installations rely on a web-based access method, where users have to authenticate themselves before obtaining Internet access. Larger WLAN hot-spots may support multiple operators sharing the radio infrastructure and

thus require a network selection step before the actual authentication. While today most web based access authentication methods are generally intended for human users, it is an obvious requirement for the Drive-thru environment that the authentication process be performed automatically [7]. With all users on the vehicle sharing the same network access, this fairly complex task may also be taken up by the DT-MAG.

D. Service detection. Mobile nodes may benefit from service announcements indicating available WISPs, authentication methods, and tariffs to avoid sophisticated heuristics and trial and error methods for authentication. Furthermore, hot-spots could announce additional Drive-thru or other services [7]. Service announcements need to be interpreted by the DT-MAG and be used in conjunction with e.g., authentication. As they may also be useful for client applications running on the user devices, the DT-MAG must also be capable of distributing these announcements to clients on the local network.

E. PCMP client functions. The PCMP client is responsible for initiating a PCMP connection to the corresponding Drive-thru proxy (including user authentication) and for resuming application sessions when a connectivity island becomes available—as well as to suspend these sessions and tear down the PCMP connection when connectivity is lost. This particularly incurs maintaining the state necessary for persistent application sessions. Hence, using PCMP client functions on the DT-MAG is only feasible if the application sessions need not persist longer than the user is aboard the respective vehicle. Otherwise, the PCMP client needs to reside on the user device.

As the PCMP client also authenticates with the Drive-thru proxy, this requires either a shared account (and hence trust) or an accounting relationship between all users. Alternatively, the PCMP client may establish per-user PCMP connections—which, however, would require means to delegate user authentication to the DT-MAG. For simplicity, we will restrict our further considerations to the former, shared account case.

F. Application-specific functions. Access routers in aircrafts, trains, etc. often provide functions to improve application performance, e.g., web caches, SMTP proxies, etc. Such functions are also applicable to the Drive-thru environment. However, to realize them on the shared DT-MAG, it needs to have access to the application connections and hence must run the—shared—PCMP client to terminate the PCMP sessions.

G. Triggering applications. All functions that are provided on the DT-MAG must be able to notify the user's applications about state changes that may be of interest to them (e.g., when connectivity becomes available or is lost, etc.). This allows applications to react quickly to such changes and particularly make efficient use of short connectivity windows.

VI. Design and Implementation of a DT-MAG

In order to support the different potential usage scenarios and their specific requirements we have designed a modular architecture for the DT-MAG that allows to assign the individual components to different devices (DT-MAG or user device) as depicted in figure 3. We have largely mapped the functional requirements identified in the previous section to individual software modules. The *ConnectivityDetector* is responsible for monitoring one or more (wireless) links and providing information about available networks. It is always running on the DT-MAG as is the *AutoConf* module which performs IP layer autoconfiguration. The *AutoAuthenticator (AA)* authenticates the DT-MAG with the WISP—and also listens to service announcements from the hot-spot provider on a well-defined multicast transport address. The AA may run on the DT-MAG and on the mobile nodes—in the latter case, however, the AA will be disabled when it notices that a DT-MAG provides this functionality. Finally, the PCMP client provides persistent transport connections across connectivity islands. If running on the DT-MAG, additional application functions such as caching may be integrated; otherwise, only the application-specific adaptation modules may be included.

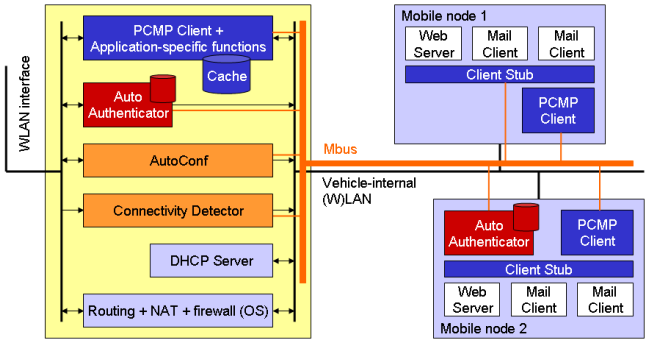

Fig. 3. Structure of DT-MAG and associated mobile nodes

These entities interface to each other using a message-oriented group communication mechanism for coordination in component-based systems—the *Message Bus (Mbus)* [21]. We have defined Mbus messages for the following basic trigger messages all of which convey soft-state updates:

1) Indication of availability (and loss) of network connectivity including link layer type, network name (e.g., SSID), signal strength (SNR), and L2 transmit rate.
2) Completion of IP layer autoconfiguration including external stack configuration parameters (IP address, netmask, DNS server, etc.).
3) Information about the necessary authentication procedures (at the link or IP layer) and whether this authentication needs to be performed by the individual mobile nodes or whether this is taken care of by the DT-MAG.
4) An indication that authentication has completed and that the access network is now ready to use.
5) If available, transport addresses of the PCMP client on the DT router and the supported application-layer functions.

This set of messages is used both for coordination between the access router components and for informing mobile devices about the progress and the functions they may need to perform. Connectivity information is provided by the *ConnectivityDetector* that will also send authentication-related messages if WEP or WPA are enabled. If not, an (enhanced) DHCP client

performs IP autoconfiguration and indicates its completion. It is up to the *AutoAuthenticator* (prior to or after IP autoconfiguration) to authenticate with the WISP and indicate when network access becomes available. This trigger is recognized by the PCMP client (on the DT router or the mobile nodes) and causes the PCMP sessions to be resumed.

On the mobile node, we provide a simple configurable stub to deal with each application to be enhanced by Drive-thru services. It allows standard applications (such as mail client and web browser) to be configured with a static peer/proxy address—i.e., an address on the local machine—and redirects incoming connections: to a local PCMP client on the mobile node or to the PCMP client in the vehicle as determined by means of the local announcements.[4]

Our initial DT router prototype implementation runs on a Linux-based laptop with a WLAN interface featuring an external antenna and an Ethernet interface for local in-vehicle communications. We have implemented the *ConnectivityDetector* and the *AutoAuthenticator* as separate modules. The *ConnectivityDetector* currently signals "up" and "down" as well as additional information for 802.11 WLANs. The *AutoAuthenticator* supports web-based authentication for hot-spots following the conventions of the Universal Access Method (UAM) [5] and also operates with open and WEP-protected WLANs (assuming preconfigured keys for the latter). [7] provides a more detailed description of the *AutoAuthenticator* and measurement results of real-world tests. All of these functions currently run on the DT-MAG. Finally, the PCMP client may be run either on the DT-MAG or on a user's mobile node. The present version of the integrated PCMP client provides just persistent transport connections but a stand-alone implementation already supports POP3 and SMTP as application protocols. This allows us to operate standard email applications (e.g. Netscape, Outlook) with our department's mail server in the presence of highly intermittent connectivity—as lab experiments with remotely controlled access points have shown.

VII. Conclusion

This paper has presented the motivation for a DT-MAG and its modular design following the requirements and the grouping of functions we have derived from various operational scenarios. We have implemented a prototype of the DT-MAG and have started testing with different applications. The DT-MAG enables several users to efficiently share a common network access link and Drive-thru communication context. Its modular design and the link-local communication bus allow flexibly moving functionality between the DT-MAG and user devices. The design particularly supports users with devices capable of stand-alone Drive-thru operation to dynamically locate and take advantage of a DT-MAG.

While the motivation is clearly to push as much functionality as possible to the DT-MAG to maximize its effectiveness, this requires common accounting and, to some degree, trust in the DT-MAG. Independent of accounting and trust, however, Drive-thru functions running on a car router also imply that the persistent connection state resides on this router, thereby disallowing a user to resume communications initiated before entering and to continue after leaving the vehicle. While this is not an issue for devices built into e.g., a bus, individual communications is clearly restricted. We are currently investigating whether simple PCMP state transfer mechanisms can be employed to mitigate this shortcoming. We are also looking into integrating application-specific functions with the car router in a way that works with PCMP in the router as well as on the clients. Finally, business aspects and their technical implications to make hot-spots broadly available to Drive-thru users deserve further consideration so that Drive-thru Internet access becomes equally attractive for a single user in a car and anonymous individuals sharing resources on a bus or train.

[4] A future optimization will be to transparently capture the application's TCP packets and terminate the respective connection without any manual reconfiguration required for the application.

References

[1] Eva Gustafsson and Annika Jonsson, "Always Best Connected," *IEEE Wireless Communications*, vol. 10, no. 1, pp. 49–55, February 2003.

[2] G. Leijonhufvud, "Multi access networks and Always Best Connected, ABC," MMC Workshop, November 2001.

[3] P. Rodriguez, R. Chakravorty, J. Chesterfield, I. Pratty, and S. Banerjee, "MAR: A Commuter Router Infrastructure for the Mobile Internet," in *Proc. of ACM Mobisys*, June 2004.

[4] M. Zitterbart et al., "IPonAir – Drahtloses Internet des nächsten Generation," PIK, Vol 26, No 4, October 2003.

[5] B. Anton, B. Bullock, and J. Short, "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming, Version 1.0," Wi-Fi Alliance, February 2003.

[6] A. Balachandran, G. M. Voelker, and P. Bahl, "Wireless Hotspots: Current Challenges and Future Directions," in *Proceeding of WMASH 2003*, September 2003.

[7] J. Ott and D. Kutscher, "Exploiting Regular Hot-Spots for Drive-thru Internet," in *Proceedings of KiVS 2005, Kaiserslautern*, March 2005.

[8] J. Ott and D. Kutscher, "Why Seamless? Towards Exploiting WLAN-based Intermittent Connectivity on the Road," in *Proceedings of the TERENA Networking Conference, TNC 2004, Rhodes*, June 2004.

[9] J. Ott and D. Kutscher, "Drive-thru Internet: IEEE 802.11b for „Automobile" Users," in *Proc. of IEEE Infocom, Hong Kong*, 2004.

[10] J. Ott and D. Kutscher, "The "Drive-thru" Architecture: WLAN-based Internet Access on the Road," in *Proc. of VTC Spring 2004*, May 2004.

[11] A. Baig, M. Hassan, and L. Libman, "Prediction-based Recovery from Link Outages in On-Board Mobile Communication Networks," in *Proceeding of IEEE Globecom 2004*, December 2004.

[12] "Homepage of FleetNet," http://www.fleetnet.de/, 2003.

[13] L. Bononi, M. Conti, and E. Gregori, "Design and Performance Evaluation of an Asymptotically Optimal Backoff Algorithm for IEEE 802.11 Wireless LANs," in *33rd Hawaii International Conference on System Sciences*, January 2000.

[14] J. Ott and D. Kutscher, "A Disconnection-Tolerant Transport for Drive-thru Internet Environments," in *Proc. of IEEE Infocom, Miami*, 2005.

[15] J. Ott, D. Kutscher, and M. Koch, "Towards Automated Authentication for Mobile Users in WLAN Hot-Spots," Accepted for Publication at VTC Fall 2005.

[16] M. Esbjörnsson, O. Juhlin, and M. Östergren, "The Hocman Prototype - Fast Motor Bikers and Ad-hoc Networking," Proc. of MUM, 2002.

[17] Website of the OverDRIVE project, "http://www.ist-overdrive.org/," .

[18] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proceedings of ACM SIGCOMM 2003, Computer Communications Review, Vol 33, No 4, August 2003.

[19] DTN Website, "http://www.dtnrg.org/," .

[20] M. Bechler, L. Wolf, O. Storz, and W. Franz, "Efficient Discovery of Internet Gateways in Future Vehicular Communication Systems," in *Proc. of VTC Spring 2003, Jeju, Korea*, April 2003.

[21] J. Ott, C. Perkins, and D. Kutscher, "A Message Bus for Local Coordination," RFC 3259, April 2002.