ITS World Congress and Exhibition, London, UK, October 2006

INTERNET ACCESS FOR VEHICULAR COMMUNICATION – A TWO-STAGE APPROACH WITH PUBLIC HOT-SPOTS AND DEDICATED ROAD-SIDE UNITS

Andreas Festag[1] and Roberto Baldessari[2]

[1] NEC Deutschland GmbH
Reichenbachstr. 1
D - 85737 Ismaning
Phone: +49/(0) 6221/4342-0, Fax: +49/(0) 6221/4342-155
festag@netlab.nec.de

[2] NEC Europe Ltd., Network Laboratories
Kurfürsten-Anlage 36
D - 69115 Heidelberg
Phone: +49/(0) 6221/4342-0, Fax: +49/(0) 6221/4342-55
baldessari@netlab.nec.de

Abstract. Communication capabilities in future vehicles and a road-side infrastructure, deploying wireless LAN IEEE 802.11 technology, are expected to provide Internet access for drivers and passengers. This paper analyzes two approaches for Internet access with respect to its technical deployability in vehicular scenarios: With increasing proliferation of WIFI hots spots, access points at public places can be reused in scenarios with low mobility. Alternatively, road-side units mainly dedicated to road safety, can be enhanced to provide Internet connectivity as an additional service. Judging the merits of *public hot spots* and *dedicated road-side units* we propose an integrated solution and discuss technical issues for their deployment. Experiments in a real-world environment demonstrate the feasibility of vehicular Internet access.

1 INTRODUCTION

The use of communication capabilities in vehicles is one of the main trends in development of future automobiles. When used for extending the driver's range of recognition, communication offers a wide range of applications to improve safety and comfort of driving, such as road obstacle warning, intersection collision warning, traffic information, and user communication & information.Various efforts, such as VII [1], C2C-CC [2], Internet ITS [3], and DSRC [4] projects and standardization bodies target at development of vehicular communication systems based on IEEE 802.11-like short-range wireless technology.[3] Vehicular ad hoc networks (VANETs) provide the technical means for direct exchange of data among vehicles, where intermediate vehicles can relay data via multiple wireless hops [6]. In these networks data is transmitted on the shortest path from the source to the destination vehicle(s) without crossing any infrastructure. While vehicle-to-vehicle (V2V) is important for many applications that improve road safety [7], this paper focuses on infrastructure access via vehicle-to-roadside (V2R) communication.

The network architecture addressed in this paper integrates both V2V and V2R communication modes using wireless multi-hop communication. For safety applications, we assume dedicated road-side units (RSU): A RSU can either warn vehicles of imminent danger related to infrastructure or simply extend the range of a vehicular network in a scenario with a sparse distribution of vehicles. For Internet access from a vehicle, we assume that these RSUs can also be used as wireless Internet point-of-attachment along the road.

A serious challenge for a vehicular communication system is the market introduction which faces a typical *chicken-and-egg* problem: Since in the introduction phase the share of vehicles equipped with

[3] Also referred to *Dedicated Short Range Communication (DSRC)*

a communication system is small, investments in infrastructure will reluctantly be made and only if a future large scale deployment is very likely. Furthermore, drivers would equip their vehicles only if they will have an immediate benefit of it.

In order to alleviate the *chicken-and-egg* problem we propose a two-stage approach of Internet access for vehicular communication: *Public hot spot* and *dedicated road-side unit*. In both approaches a forwarding chain of vehicles to reach the infrastructure considerably extends the virtual range of communication – in a late deployment phase of such a system. Then, the main difference between the two approaches is where the end point of the ad hoc network is located, either in the last vehicle of the forwarding chain *(public hot spot)* or as part of the infrastructure *(dedicated road-side unit)*. Clearly, the main benefit of the *public hot spot* approach is the fact that a potentially existing infrastructure offering high wireless bandwidth can be reused. This is particularly important in the introduction phase of such a system, where RSUs are almost not available. Our work concludes that, in a later deployment phase where cities and highways are potentially equipped with RSUs for safety, the approach with *dedicated road-side units* have benefits compared with the *public hot spot* approach. These include i) less complexity for implementation and deployment, ii) better connectivity in scenarios with wireless multi-hop access to the infrastructure and driving vehicles, and iii) support of additional features, such as vehicle-to-vehicle communication over larger distances where a part of the data path is via the infrastructure.

We propose an integrated system for vehicular communication that provides both techniques, *public hot spots* and *dedicated road-side units*, for Internet access. For a quick market introduction of a VANET system, the solution allows Internet access via *public hot spots* and wireless single-hop communication in a static scenarios right from the beginning for nomadic Internet access. With gradual deployment of RSUs along streets and highways, *dedicated road-side units* provide Internet access on the road.

The main contribution of the paper is as follows: It i) describes the state-of-the-art of the two approaches for Internet access, ii) analyzes technical strengths and weaknesses, and iii) proposes an integrated solution of Internet access via *public hot spots* and *dedicated road-side units*. Finally, the paper presents measurement results that show firstly the feasibility of Internet access via dedicated RSUs and secondly the benefit of adopting wireless multi-hop communication.

The remaining sections are structured as follows: After presenting the network architecture in Sec. 2, Sec. 3 describes technical details of Internet access using *public hot spots* and *dedicated road-side units*, and analyzes both approaches. Sec. 4 discusses technical issues of an integrated solution. Sec. 5 presents measurement results, and Sec. 6 concludes.

2 ASSUMED NETWORK ARCHITECTURE

The assumed network architecture defines three distinct domains: *in-vehicle*, *ad hoc*, and *infrastructure domain* (Fig. 1). The *in-vehicle domain* is a network composed of an *on-board unit* (OBU) and (potentially multiple) *application units* (AUs). AUs are typically portable devices such as laptops, PDAs or game pads attached to an OBU and normally connected via a wired connection. The *ad hoc domain* comprises vehicles equipped with OBUs and stationary nodes along the road, termed *road-side units* (RSUs). The units (OBUs and RSUs) can directly communicate if direct wireless connectivity exists. In the case that no direct connectivity exists, intermediate nodes relay data (multi-hop communication). The ad hoc routing is provided by a *position-based routing* protocol, termed PBRV [7]. PBRV offers efficient data delivery in highly dynamic environments as with vehicles, and naturally enables the addressing of nodes located in a geographical area and the geographically-scoped distribution of packets, referred to as *geographic broadcast (Geocast)*.

For access to the Internet we assume two options: i) *Public hot spots* are operated by wireless Internet service providers at locations that are frequently passed by travelers, such as gas stations and restaurants at highways, but also 'info stations' in cities. Public hot spots facilitate auto-configuration, secure data transfer and charging. Today's public hot spots support IPv4, future hot spots might incrementally apply IPv6. ii) *Road-side units* are primarily designated to improve road safety and are installed at locations of the traffic infra-structure, such as intersections, dangerous curves, and bridges. The RSUs

can offer Internet access as an additional value, but have to ensure that the data transfer for safety applications is not impaired. While we expect that data traffic for safety applications for car-to-car and car-to-roadside communication is free of charge, Internet access via RSU is offered – similar to public hot spots – at low costs. Since we assume that cars will use IPv6 addresses right from the start[4], Internet access via RSUs in this network architecture is based on IPv6.

We assume that vehicles are equipped with different variants of wireless LAN technology: For safety applications OBUs and RSUs are expected to use IEEE 802.11p [8] operating at dedicated frequencies. Public hot spots use the popular IEEE 802.11a/b/g (or future variants) technologies. A vehicle might be equipped with two separate network interface cards, or with a single, multi-mode card that is able to switch between the different technologies.

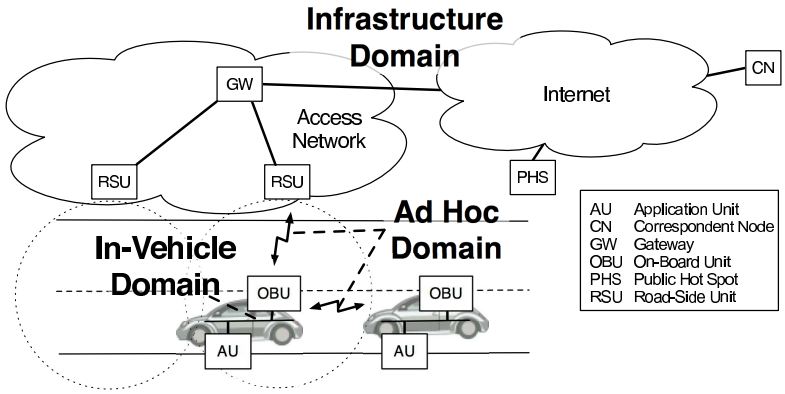


Fig. 1. System architecture view

3 TWO APPROACHES FOR INTERNET ACCESS

This section describes the use of *public hot spot* and *dedicated road-side unit* as two approaches for Internet access. Both approaches are then analyzed with respect to their use in vehicular environments.

3.1 Public Hot Spot

This approach uses regular commercial WIFI hot spots that are operated by wireless Internet service provides. When a vehicle wishes to send a data packet to a node in the Internet, the packet is forwarded hop-by-hop from the source to the vehicle with access to the hot spot, potentially via multiple forwarders. The last vehicle in the forwarding chain acts as a router. It 'translates' the packet header from the ad hoc routing protocol to an IP header and forwards it to the hot spot.

This solution is essentially based on currently existing technologies for hot spots: A vehicle enters the transmission range of a wireless access point (AP) and negotiates access according to the provided user credentials and service options. Nowadays, this is mostly achieved by adopting IP filtering and HTTP redirection to an operator login page. For the near future, authentication and authorization protocols will likely be based on IEEE 802.1x with EAP for automated and quick configuration.[5] For vehicles, this advanced solution is more suitable and guarantees shorter overall negotiation phase.

After the negotiation phase, the vehicle gains IP(v4) connectivity and, from the perspective of the VANET, becomes a *gateway vehicle (GWV)*: It now offers Internet access to other vehicles and acts as an IP router. Since IPv6 has been chosen for future ITS and today's commercial hot spots operate with IPv4, the GWV routes packets between the IPv6-based VANET and the IPv4-based infrastructure.

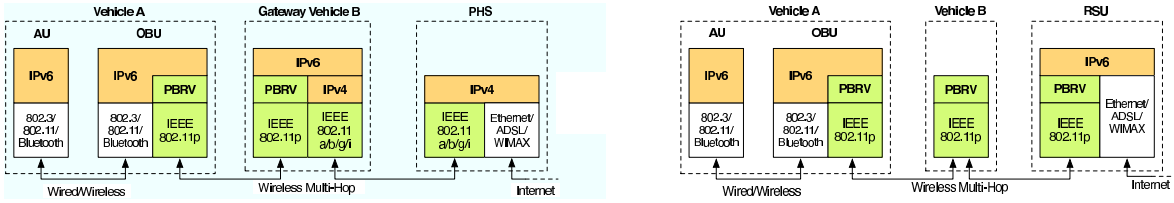
[4] Mainly due to the lack of IPv4 addresses for the potentially high number of OBUs and RSUs.
[5] Commercial products from major vendors are already available.

The translation can mainly be achieved by means of two methods: Address translation (NAT-PT [9]) or IPv6-in-IPv4 encapsulation (also called *configured tunneling* [10]). In the presented solution, tunneling was chosen because of simplicity and the fact that NAT-PT mechanism implies several restrictions for IPv6 mobility support and IPv6 applications [11].

In order to announce GWV availability, the GWV distributes IPv6 *router advertisement* in the ad hoc domain by means of multi-hop forwarding with PBRV. Other vehicles consider the GWV as the IPv6 *access router* of the visited link and are (logically) connected to the IPv6 subnet at the end-point of the tunnel in the infrastructure domain. A vehicle configures a globally routable IPv6 address and the in-vehicle application units, if available, are globally reachable through IPv6 mobility support.

In scenarios with driving vehicles, the network topology can change. In case the vehicle leaves the transmission range of the GWV, the vehicle might acquire direct access to the PHS or select another GWV if available. A similar procedure is applied if the GWV moves and breaks the forwarding chain: Another GWV is chosen, if available. Every time that multiple GWVs are available, vehicles need to select one according to distance and hop number criteria. This is achieved by using PBRV filter functionality: the PBRV layer passes to the upper IPv6 layer the *router advertisements* that comes only from the closest GWV.

Furthermore, in case of a highly mobile scenario, such as passing cars on a highway, it is worth noting that a vehicle becoming a GWV executes all steps (negotiation, configuration, service announcements) before being able to forward data packets to the hot spot.



(a) Public hot spot

(b) Dedicated road-side unit

Fig. 2. Resulting protocol architecture

3.2 Dedicated Road-Side Unit

Though the main task of road-side units utilized in this approach is road safety, they might be equipped with additional network capabilities to provide Internet connectivity. A vehicle communicating with the Internet forwards data packets potentially via multiple wireless hops to the road-side unit via the ad-hoc routing protocol. The road-side unit in turn forwards the data packet as a regular IP packet toward the Internet node.

The protocol architecture of this solution (Fig. 2) is similar to the one of the hot spot approach, but simplified: A RSU interconnects two IPv6-based networks and acts as IPv6 *access router* for the vehicular ad hoc network. Due to the fact that RSUs are principally used for safety purposes, the exchange of PBRV packets between vehicles and RSUs is always guaranteed without the need to negotiate any service. On the contrary, access to the Internet provided by RSU needs to be authorized and charged. For this purpose, an IP-based authentication protocol (such as EAP over PANA [12]) could be used, with the advantage that the negotiation does not interfere with the exchange of safety messages.

As a result of the above considerations, a RSU provides Internet access by periodically announcing IPv6 *router advertisements (RAs)* in the ad-hoc domain. On recpetion of an RA, a vehicles automatically configure an IPv6 address and choose the RSU as default gateway for IP traffic. When a vehicle moves out of a range of the current RSU and receives another RA, the vehicle can configure a new IPv6 address and the next RSU. However, this method does provide neither global reachability nor session continuity, as explained later.

3.3 Analysis of both approaches

Based on the functional comparison we analyze both solutions with respect to the following criteria:

Availability and investments. *Public hot spots* based on WLAN are well established and widespread.[6] Market introduction of products based on IEEE 802.11p (which is not finalized yet) are expected after 2010. In some regions (such as North America [13]) governmental programs finance RSUs to a large extend. In other regions, however, RSUs will only be incrementally installed.

Mobility support. Both proposed solutions provide basic Internet access. They ensure that a vehicle is able to communicate with nodes in the Internet. In order to support global reachability and session continuity when a vehicle changes its Internet point of attachment, an addition solution (such as Mobile IP [14, 15]) is needed. One possible solution that adapts Mobile IPv6 for vehicular networks is proposed in [16]. For the *public hot spot* solution, mobility support in the sense of handover between different hot spots is very limited due to frequent changes in the network topology and necessary re-configuration of gateway vehicles.

Configurability. The specific characteristics of vehicular Internet access with short Internet connectivity demands an automated configuration and authentication, and applicable tariff models (e.g. flat rate). While efforts for a unified approach for hot spots exists (e.g. IEEE 802.1x and [17]), it is likely that future hot spots will still utilize heterogeneous mechanisms for configuration.

Complexity. The coexistence of IPv4 (mainly used by hot spots) and IPv6 (used in the vehicular network) considerably increases the complexity due to the need for tunneling or NAT. Also, the functionality needed in the gateway vehicle (negotiation, configuration, announcement, see Sec. 3.1) is more complex compared with the dedicated RSU solution.

Charging. Though many free-of-charge *public hot spots* exist today, we assume that the majority public hot spots will charge the user. Similarly, Internet access via RSUs is regarded as an opportunity to re-finance the deployment of RSUs for safety. Since in our approach, one vehicle offers its Internet access to others, advanced charging mechanisms are necessary for both solutions. Incentive-based charging schemes [18] offer rewards to those users that forward data on behalf of others.

Additional functions. The approach with dedicated road-side units offer the opportunity to specifically enhance RSUs by features, such as communication between vehicles whereas a path segment is via the infrastructure (opposed to direct vehicle-to-vehicle communication).

From these statements we can conclude that both schemes can be principally deployed, but require additional functionality. These include automatic configuration (hot spots) and suitable tariff models, mobility support, and enhanced charging support. Comparing both, *public hot spots* are rather for scenarios for static or slow moving cars, but offer potentially higher bandwidth. We regard the approach with *dedicated road-side units* rather suitable for mobile scenarios with smaller bandwidth requirements, but offering enhanced functionality. Table 1 compares both approaches with respect to technical functions.

Criteria	Public Hot Spot	Dedicated Road-Side Unit
Typical locations of stationary units	Private locations	Public infrastructure
Address domain	IPv4/v6	IPv6
Address assignment	DHCP	IPv6 stateless auto-configuration
Multi-homing	Yes	No
Address translation	NAT/Tunneling	No
Gateway between ad hoc & infrastructure	Vehicle (mobile)	Access point (stationary)
Service detection	Router advertisements / Geocast	
Procedure for reconnection	Full	n.a. (Transparent)
Authentication & charging	IEEE 802.1x (e.g. EAP)	IP-based (e.g. PANA)

Table 1. Functional comparison

[6] *JiWire.com*, the leading WLAN hot spot locator, lists 120,000 public hot spots worldwide (August 2006).

4 INTEGRATED SOLUTION

In this section we describe an approach for the integration of both – *public hot spot* and *dedicated road-side unit* – approaches into a single, integrated solution.

In the long term, we expect that RSUs are installed along roads, intersections and places with high vehicle density, mainly by public authorities. Relying on the solution described in Sec. 3.1, the availability of hot spots in parking sites, gas stations and commercial areas, installed either by public or private bodies, we regard PHS as rather complementary to the RSUs' function than competing. The resulting network architecture of the integrated solution is depicted in Fig. 3. Public hot spots, belonging to the *Wireless Internet Service Provider (WISP)* networks, coexist with road-side units connected to public network infrastructures. For Internet access, the direct connectivity to the hot spot is managed through the authentication protocol adopted by the WISP. In contrast, the Internet access from a vehicle through wireless multi-hop is regulated by IP-based authentication protocols. Hence, an IP-based authentication scheme can be applied for both PHS- and RSU-based Internet access. This is typically achieved by means of 'tunnels' for data packets, where data are encapsulated and decapsulated to be sent through the tunnel. As a result, in both cases the vehicles are logically connected to an IPv6 network.

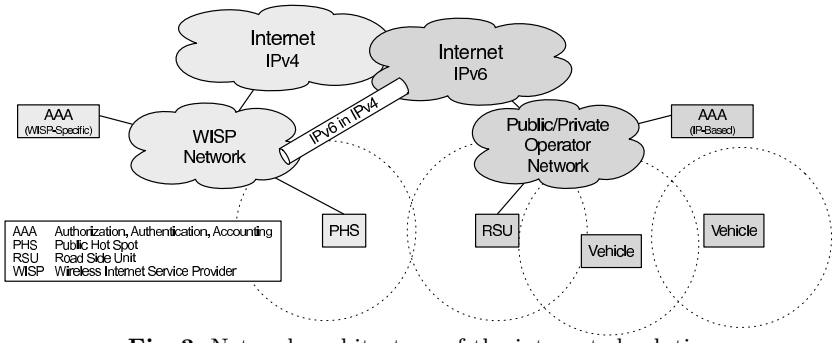


Fig. 3. Network architecture of the integrated solution

The main benefits of integrating PHSs and RSUs in this architecture are extension of wireless coverage and increment of available bandwidth. Two main technical issues arise from integration:

Selection of an access mode. In case that PHSs and RSUs are simultaneously available, a vehicle can choose one of the modes. The following criteria can be used for selection of an access mode:
- *Level of dynamics.* Since PHSs are not suitable for high dynamic scenarios, RSUs should be preferred in case of car movement. This guarantees a better communication continuity.
- *Required bandwidth:* For high-bandwidth applications (e.g. multimedia applications, VoIP, etc.), the PHS should be chosen.
- *Hop count and distance:* In order to reduce the load of the data traffic forwarded through multiple hops, a vehicle should possibly use the closest (in terms of wireless hops) point of attachment. Optionally, the geographical distance provided by the PBRV protocol could be taken into account.

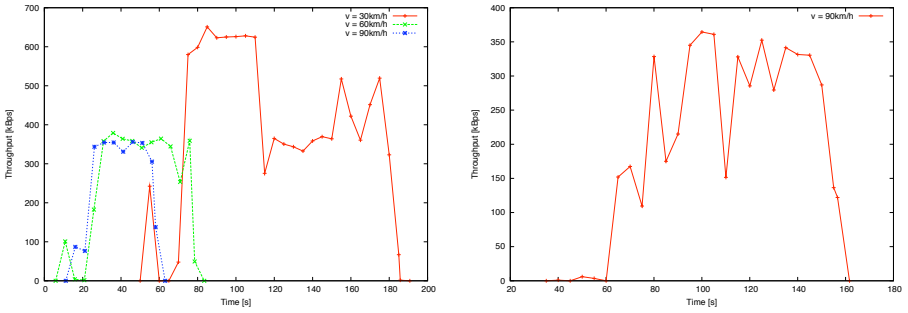
Switching between access modes. When a vehicle has Internet connectivity via a PHS and enters the coverage area of a RSU (or vice versa), it potentially could switch the communication mode. Since we assume that GWV and RSU are different Internet points of attachment to the infrastructure and belong to different networks in IP terminology, a switching is regarded to as an handover at network protocol layer[7]. Therefore, a policy to switch between the two possible access modes can be offered by one of the existing schemes for access network selection in IP mobility support. For example, solutions have been studied ([19, 20]) for mobile terminals or mobile routers equipped with multiple interfaces, in order to enable them to select a different access network according to the characteristics of the interface technology and data traffic.

[7] A scenario in which all RSUs and GVWs' tunnel endpoints are assigned to the same IPv6 prefix would be simpler but less scalable.

5 MEASUREMENT RESULTS

As proof of concept for the feasibility of Internet access from vehicles, we have conducted an initial set of experiments that examine the duration of time a vehicle can communicate with a road-side unit while driving for both, wireless single-hop and multi-hop communication. The experimental setup consists of standard 'x86-based' notebooks connected to an IEEE 802.11a-like radio module adapted to vehicular environments[8], and an antenna with a gain of 5 dBi. All nodes run a prototype software implementation of PBRV, the operating system is Linux, kernel version 2.6. A node can either be configured as an on-board unit in a car with a roof-top antenna, or as a stationary RSU with a mobile power supply and an antenna on a tripod.

We conducted the tests on a straight road of almost 2 km length in a rural outdoor environment with every-day road traffic. Transmission power was set to 20 dBm, bandwidth 20 MHz at 5.9 GHz. We defined two scenarios with *i)* single-hop and *ii)* two-hop communication. In *i)* a car passed a RSU with a defined speed controlled by the car's cruise control. In *ii)* a car passed first another, stationary car and then the RSU, whereas the stationary car had permanent wireless connectivity to the RSU via a distance of about 400 meters. When the first car passed the second car, data were forwarded via two wireless hops to the RSU. As soon as the first car was in wireless range of the RSU it switched to direct wireless communication. In both scenarios, the RSU periodically broadcasted Mobile IPv6 router advertisements, which were distributed via multiple wireless hops in the second scenario. On reception of an advertisement, the first car configured an IPv6 address and started a bulk packet transfer at a constant rate of 10 packets per second and a packet size of 500 bytes.



(a) Single hop scenario (b) Two hop scenario

Fig. 4. Measurement results

We define *RSU connectivity time* the duration of time in which the vehicle is able to communicate with the RSU. In the single-hop scenario we measured a *RSU connectivity time* of 135 s, 75 s, and 50 s for speeds of 30 km/h, 60 km/h, and 90 km/h, respectively (Figure 4(a)). The throughput is about 400 kBps on average, strong variations occur due to obstacles along the road, such as passing cars. Figure 4(b) shows that wireless multi-hop communication can considerably extend the *RSU connectivity time*, i.e. 120 s in the scenario with two wireless hops, measured for a speed of about 90 km/h.

The measurement results show that a vehicle's sojourn time in the wireless range of an RSU is sufficiently long to establish a communication session and exchange data. For public hot spots a considerable duration of time will be consumed for authentication and authorization with the WISP [21], and hence is limited to rather low mobility scenarios. In addition, the measurements complements the experiments in [22] with IEEE 802.11b technology, but with an experimental radio technology close to a future IEEE 802.11p standard.

[8] Wireless Radio Module (WRM), version 1.3 from DENSO Inc.

6 SUMMARY AND CONCLUSIONS

This paper investigates two approaches for Internet access in vehicular networks using short-range wireless technology as part of the envisaged Intelligent Transportation Systems (ITS). In both approaches, the wireless range of the access point is extended by wireless multi-hop communication. Immediate deployment can be achieved by reusing *public hot spots*. Future road-side units that are primarily used to improve road safety can also offer Internet access. We propose a hybrid strategy: *public hot spots* should be applied in an early introduction phase of a system in scenarios with static or slowly moving vehicles. Due to the limitation in mobility (and others including complexity and configurability) of *public hot spots*, *dedicated road-side units* are the preferred approach of Internet access for vehicles if they are available. We have described a solution that integrates both approaches. Initial measurement results show the feasibility of vehicular-based Internet access and the benefits of using wireless multi-hop technology to reach road-side infrastructure.

7 ACKNOWLEDGMENTS

A. Festag acknowledges the support of the German Ministry of Education and Research (BMB+F) for the project *'NoW – Network on Wheels'* under contract number 01AK064F. We thank R. Schmitz and H. Wang for support in the measurement campaign.

References

1. Vehicle Infrastructure Integration (VII). `http://www.its.dot.gov/vii/`.
2. Car 2 Car Communication (C2CC) Consortium. `http://www.car2car.org`.
3. Internet ITS Consortium. `http://www.internetits.org`.
4. DSRC Working Group. `http://grouper.ieee.org/groups/scc32/dsrc/index.html`.
5. DSRC Project. `http://www.leearmstrong.com/DSRC/DSRCHomeset.htm`.
6. B.N. Karp and H.T. Kung. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. In *Proceedings MobiCom*, pages 243–254, Boston, MA, USA, Aug. 2000.
7. A. Festag, H. Füßler, H. Hartenstein, A. Sarma, and R. Schmitz. FleetNet: Bringing Car-to-Car Communication into the Real World. In *Proceedings ITS World Congress on ITS*, Nagoyoa, Japan, Nov. 2004.
8. IEEE. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 3: Wireless Access in Vehicular Environments (WAVE), Jan. 2006.
9. G. Tsirtsis and P. Srisuresh. Network Address Translation - Protocol Translation (NAT-PT). RFC 2766, Feb. 2000.
10. E. Nordmark and R. Gilligan. Basic Transition Mechanisms for IPv6 Hosts and Routers. RFC 4213, Oct. 2005.
11. C. Aoun and E. Davies. Reasons to Move NAT-PT to Experimental. Internet Draft, Work in Progress, Oct. 2005.
12. A. Yegin, Y. Ohba, R. Penno, G. Tsirtsis, and C. Wang. Protocol for Carrying Authentication for Network Access (PANA) Requirements. RFC 4058, May 2005.
13. Intelligent Transportation Society of America. National ITS Program Plan: A Ten Years Vision. `http://www.itsa.org/subject.nsf/vLookupReport/10+Year+Plan!OpenDocument`, July 2004.
14. C. Perkins. IP Mobility Support for IPv4. RFC 3344, Aug. 2002.
15. D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775, June 2004.
16. R. Baldessari, A. Festag, A. Matos, J. Santos, and R. Aguiar. Flexible Connectivity Management in Vehicular Communication Networks. In *Proceedings WIT*, pages 211–216, Hamburg, Germany, March 2006.
17. A. Anton, B. Bullock, and J. Short. Best Current Practices for Wireless Internet Service Provider (WISP) Roaming. Wi-Fi Alliance, Feb. 2003.
18. B. Lamparter, K. Paul, and D. Westhoff. Charging Support for Ad Hoc Stub Networks. *Elsevier Journal of Computer Communications*, 26(13):1504–1514, 2003.
19. L. Suciu, J.-M. Bonnin, K. Guillouard, and T. Ernst. Multiple Network Interfaces Management for Mobile Routers. In *Proceedings of ITST*, Brest, France, June 2005.
20. R. Wakikawa, K. Uehara, and J. Murai. Multiple Network Interfaces Support by Policy-Based Routing on Mobile IPv6. In *Proceedings ICWN*, Las Vegas, NV, USA, June 2002.
21. J. Ott, D. Kutscher, and M. Koch. Towards Automated Authentication for Mobile Users in WLAN Hot-Spots. In *Proceedings VTC Fall*, Dallas, TX, USA, Sep. 2005.
22. J. Ott and D. Kutscher. Drive-thru Internet: IEEE 802.11b for "Automobile" Users. In *Proceedings INFOCOM*, Hong Kong, China, March 2004.