# Enhancing User Mobility with Network Service Maps

Dirk Kutscher
Technologiezentrum Informatik (TZI)
Mobile Research Center Bremen
dku@tzi.org

Jörg Ott
Helsinki University of Technology
Networking Laboratory
jo@netlab.hut.fi

March 21, 2006

**Keywords:** Mobility, Roaming, 4G, WLAN, Service Discovery

**Abstract**

Many mobile networking scenarios, such as campus WLAN roaming and public WLAN hotspot usage, require support for network selection and automatic network association on the mobile client side. In this paper, we analyze these and other scenarios with respect to use cases of network information services and infer a set of requirements that have led to the design of a network information service for supporting nomadic and mobile WLAN usage. Our approach called *Network Service Maps* can be characterized as provider- and network-independent, representing an extensible information service that is built on the notion that receivers obtain service descriptions from arbitrary sources over different networks and compose *individual service maps* based on filtering with respect to current location, sought-after service, personal preferences, etc.

It differs from existing network information systems in its generality and network- and topology-independence, and it differs from existing service-location approaches in its applicability to wide-area, location-based service description distribution. The information service is based on a general service description information framework that provides different transport mechanisms for supporting heterogeneous network environments and on a data model for service description that enables receivers and transceivers to flexibly (re-) composing received service information with respect to different criteria.

## 1 Introduction

Wireless LAN hotspots have become widespread and service providers increasingly engage in (bilateral) roaming agreements or use clearinghouse services (such as Boingo Wireless [Wir03]) to expand the coverage for their customers. Additional upcoming mobile access technologies such as 3G, WiMAX (IEEE 802.16), and 4G hybrid networking environments embracing multiple technologies will further enhance service availability for mobile and nomadic users. Focusing on commodity WLAN services, most activities are driven by commercial services, by municipalities [Wei05], and by private sharing activities [ST03]. But also organized (non-profit) networks operating based upon reciprocity of cost and benefit such as the *FON movement*[1] can be found. Most notably is the Eduroam activity enabling sharing of wireless LANs across university campuses with members throughout Europe [FW05] in addition to the multitude of local campus networks that partly need expand across a city and offer service to local researches and students.

With such a multitude of choice, it becomes increasingly difficult for the user to keep her orientation: with respect to 1) which service provider offerings may be available at a particular location, 2) how to authenticate with the service provider (which credentials for which realm using which authentication methods), 3) what tariff models (and, ultimately: charges) may apply for

[1] http://en.fon.com/

which service provider, and 4) where network access can be obtained in the first place *given her specific subscription profile*. While, for cellular communication, sufficiently widespread coverage is available,[2] WLAN hotspots—which usually offer superior performance—are restricted in their geographic coverage so that locating access networks as per (4) above remains an issue for the foreseeable future. This also applies to hybrid network access scenarios allowing for seamless handover across arbitrary link layer technologies in order to optimize performance and/or minimize cost for the communication tasks at hand. Today's practice in order to address the above four issues is still rather basic as discussed in the following:


Figure 1: WLAN Hotspot information display

Locating hotspots and service providers (1 and 4) is typically addressed by web-based locators[3] that are offered by the service providers or clearinghouses and must be interactively operated by humans). Commonly available "alternatives" include hints on the web page for "signing on" within a hotspot (see next paragraph) and signposts (see figure 1). To allow its users to locate WLANs of the *eduroam* roaming infrastructure [FW05], the TERENA mobility task force is proposing an "access point phone book". The idea is to use a database containing location information about eduroam access points. Some initial proposals for a data model have been made[4] that are currently concentrating on WLAN-related information for eduroam access point installations. In a recent development, IEEE 802.21 Media-independent Handover Services [IEE05] defines how to obtain a local overview of (immediately) surrounding networks—the Media-independent Information Service (MIIS) that is intended for L2 information about network elements in the neighborhood but also supports higher layers (Internet access parameters, descriptions about VPN and VoIP services etc.).[5]

The solution to 2), at least for public hotspots, usually defaults to *web-based authentication* which is recommended by the Wi-Fi Alliance [ABS03] and named *Universal Access Method, UAM,* (see section 2 for details). While the web pages provide at least some information about available service providers, this is targeted at human consumption and often requires interactive navigation. Based upon the service provider information and her personal service contracts, the user can then decide if she wants to initiate a network association process. However, it would be preferable to have the hotspot operator disseminate information about available service and providers, tariff models, and access methods using a standardized protocol and description language.

[2] and it is implicitly assumed that service cost and quality are acceptable

[3] Typically, these are just front-ends to some database.

[4] http://www.eduroam.org/wiki/AccessPointDB?v=d8o

[5] Independent of specific wireless network access, a variety of service discovery protocols have been developed, most of which focus on "local" services within a connected network (e.g., [GPVD99] [Cor00] [Mic01]) but reviewing this entire landscape is beyond the scope of this paper.

Automating hotspot association is also desirable because of the proliferation of installations where multiple different authentication methods are available. For example, public installations such as university campus WLAN services typically provide different authentication methods depending on the country and local policies, and some installations offer different alternative methods. As a consequence, roaming users, e.g., eduroam users who want to connect to their home institutions, currently have to determine manually which method to use at a specific site.

While manual authentication is cumbersome, the necessary human interaction also "enables" retrieving some information for 3)—but, in many cases, this information is restricted to charges for one-time payments for a fixed amount of access time. If the user has a subscription and may need to determine roaming charges, she will usually not succeed (similar to a traveling cellphone user who also learns about the true roaming charges from his next invoice). The resulting drawback is that virtually no cost and/or performance optimizations are possible as the necessary input data is missing.

This short analysis illustrates that nomadic WLAN access is still dominated by manual operation. While some basic hints for handover are being defined, automating network selection and association requires additional information services [OKK]. This is especially true when we consider mobile scenarios, e.g., as in the Drive-thru Internet project [OK04a] [Dri] where WLAN hotspots are accessed from fast moving vehicles so that the selection and association must be performed quickly and hence automatically. In such environments, it is especially useful to have advance knowledge of hotspots and their locations, providers, tariffs, and access parameters. But even nomadic users, who pause at a hotspot to obtain network access, would clearly benefit from machine-processable service information that can guide them to an access network, help them choosing the best service provider (according to their policy), and allow them to efficiently authenticate with minimal overhead.

In order to accommodate the needs of mobile and nomadic users, we have proposed the general concept of *Service Maps* [KO]. In this paper, we enhance this approach towards *Network Service Maps* for the specific use case of wireless LAN access. While we focus on IEEE 802.11 WLAN because its widespread availability makes it an attractive substrate for wireless access, our approach is designed to be network-independent and particularly suitable for distributing access information across network boundaries in hybrid networking environments. We start by reviewing the landscape of existing approaches and relevant base technologies in section 2. In section 3, we introduce four different classes of (public) access networks which are, in the authors' experience, representative for the majority of WLAN installations available today. Considering a mobile usage scenario with extreme requirements, we uses these access network classes to derive the requirements for our network service maps. We present our approach, in which we combine service, location, and other relevant information from a holistic perspective, in section 4. In particular, we synthesize a data model suitable for describing network access but also other value added services that allows for receiver-side composition of service maps from fragments received via different communication channels and enables creating different views on a service map according to the needs of the user. The resulting information service enables users on the move to automatically and efficiently choose and access (wireless) networks following their needs and preferences and gain access to additional services as desired. Section 5 concludes this paper with a short assessment and points to future work.

# 2 Related Work

Today, Information Services are developed with different objectives. As described in [Wil05], the main focus is on avoiding connectivity interruptions as may be caused by handover in heterogeneous networks. IEEE 802.21 Media-independent Handover Services [IEE05] defines Media-independent IS (MIIS) as part of a handover service including a command and event service for communication between mobiles nodes (MNs) and network elements. MNs shall be able to acquire a global view of heterogeneous networks to facilitate seamless handover and to allow network selection according to the MNs' requirements. MIIS is intended for L2 information about network elements in the neighborhood but also about higher layers such as Internet access parameters, descriptions about VPN and VoIP services, etc. MIIS defines a data schema that allows representing this information in protocol transactions. It also has the concept of looking for network services in a geographic region, e.g., for available 802.11 networks using the current 3G link. Three classes of IS elements are defined: 1) *General Network information* such as overviews of networks (network ID, location of points of attachment, IP version, available operators etc.), 2) *Link Layer information* such as link parameters (channel, frequency, neighbor info, security), and 3) *Higher Layer information* such as descriptions of available Multimedia Messaging Services, Mobile IP, VPN, VoIP, pricing, use of NAT, etc. IEEE 802.21 does not define the IS transport mechanism but suggests carrying L2 information directly in the link layer protocol (which would require extensions to many link layers). IEEE 802.21 specifies a data scheme for information elements in RDF, defining a fixed base scheme plus an extended scheme to be updated by future extensions. The data scheme features different classes, e.g., different kinds of addresses (geographic, civic) for location information. The intended interaction scheme for IS is *request/response*.

In the IETF, ISs have played a role in different protocol developments. The Candidate Access Router Discovery (CARD) protocol (RFC 4066 [CFL$^+$05]) can optimize next access router selection by *reverse address translation*, enabling an MN to map an observed access router (AR) layer 2 ID to its IP address by querying its current access router. In a typical CARD scenario, an MN that is attached to a link and associated with an access router senses alternative access point IDs in the wireless network neighborhood and can retrieve information about these from the current access router. The MN can also query the current access router for candidate access routers (CARs) in the network neighborhood. CARD is a query/response protocol that allows the MN to specify filters (preferences) for queries and that supports the access router to provide additional information such as CAR capabilities. CARD defines the MN-to-AR protocol and also the AR-CAR protocol (based on SCTP), by which the current AR can query requested parameters from the CAR. RFC 4068 (Fast Handovers for Mobile IP [(Ed05]) defines *off-link inverse neighbor discovery* by which an MN can query its current AR for subnet information of neighbor access points in order to prepare handover.

The discussion of IS in the context of IEEE 802.21 has led to an effort for developing an IS transport mechanism in the IETF for which some initial proposals have been submitted. [DFHX05] analyzes requirements for a media independent handover IS in order to identify suitable IETF technologies for an IS as proposed by IEEE 802.21. [KK05] specifies a transport independent network information representation format for allowing a node to discover information about surrounding networks and is targeted at ISs for Fast Mobile IP and CARD scenarios. The proposal is intended to satisfy requirements for transport-independent network discovery with a focus on efficiency with respect to transmission and processing complexity.

For commercial hotspots, such identification services are not (widely) available. The most common method is *web-based login*, recommended by the Wi-Fi Alliance [ABS03] as *Universal Access Method* (UAM) and based on the notion of *captive portals*: a user is granted L2 access but, to obtain full Internet connectivity, a web-based authentication process must be performed first. We have discussed UAM in detail in [OKK]. Its operation can be summarized as follows: The user's mobile device connects to the hotspot WLAN that has SSID broadcast enabled and does not use WEP. A DHCP server supplies the necessary IP and DNS parameters but access to the Internet is still disabled at this point. The hotspot access control function intercepts the first HTTP request from the user's device and redirects the user's web browser to the operator's login page. The login page prompts the user to enter her credentials. If the user is authorized network access is granted, typically by means of MAC or IP address filtering. Terminating the use of a hotspot (and thus stopping accounting) may also be done via the web browser and is usually complemented by inactivity detection. This approach has the advantage that it imposes very little requirements on user equipment, the authentication approach is clearly targeted at human users and difficult to automate, e.g., for an intelligent and automatic network association for mobile computing. Nevertheless, it would be preferable to have a hotspot operator disseminate information about available services and providers, tariffs, and access methods using a standardized protocol and description language. The Wi-Fi Alliance suggests the service announcement-based *smart client* authentication protocol [ABS03]. Other announcement-based approaches are discussed, e.g., in [BWSF03] and [KO03].[6]

The existing approaches do not consider network ISs and service location together in a holistic fashion. While some current activities for IS such as IEEE 802.21 (under development at the time of writing) *are* considering distributing network information to an MN for currently not-connected networks, these approaches are limited to the handover optimization use case. On the other hand, service location approaches so far have mainly focused on locating and describing services directly available in the currently associated network, without really considering the requirements for infrastructures that can provide MNs with service information independent of the currently connected network.

# 3 Scenarios and Requirements

Network Service Maps are intended to improve the experience of mobile users when accessing wireless networks on the move. In this paper, we focus on access via wireless LANs which leads us to four different scenarios that represent the typical setups mobile users may face: 1) roaming among different organization (campuses), 2) nomadic and mobile usage of public WLAN hotspots, 3) shared usage of private (but open) WLAN installations, and 4) authorized access via closed (private or corporate) WLANs. We analyze each of these scenarios with respect to *how* network service information can be made available and with respect to *what* type of information is useful. At this point, we consider all the information listed as equally important and leave it up to operators and, ultimately, applications to determine which information is needed and how far in advance it should be distributed. Subsequently, we briefly present mobile WLAN usage in the Drive-thru Internet project as one particularly demanding use case for mobile Internet access. In a conclusion, we summarize those aspects relevant for our design and hint at a potential distinction between fundamental information sets and optional refinements.

## Campus Roaming

Roaming among different research organizations refers to nomadic users who have an identity and a network access authorization in their home institution and try to connect to visited networks, performing the local configuration and authentication steps in the visited network. Today, human users have to know in advance where campus roaming is available and what authentication mechanisms would be supported. If a suitable campus network exists, users and/or devices still have to scan for appropriate ESSIDs and finally perform the network association, the user authentication, and further configuration steps.

Eduroam[7] is a European initiative that has been initiated by the TERENA Mobility Task Force[8] in order to facilitate nomadic WLAN usage for academic users visiting foreign campus networks, such as university networks. Inter-campus roaming at a European level is not trivial because of the huge diversity in WLAN installations throughout campuses in the different member states. Historically, WLAN installations at research institution campuses differ with respect to authentication mechanisms, addressing architectures, and visitor access due to different local requirements and a large variety of technical alternatives and implementation capabilities, especially considering user authentication. For example, the lack of strong security and reliable user authentication in the initial IEEE 802.11 standard has led to a development of architectures such as *docking networks* providing initial local connectivity that can be used to perform a layer three authentication step, which

[6] Independent of specific wireless network access, a variety of service discovery protocols have been developed, most of which focus on "local" services within a connected network (e.g., [GPVD99] [Cor00] [Mic01]) but reviewing this entire landscape is beyond the scope of this paper.

[7] http://www.eduroam.org/

[8] http://www.terena.nl/tech/task-forces/tf-mobility

enables complete connectivity. The different variants for performing indirect user authentication include VPN-based and UAM-based access.

After WLAN standardization and corresponding product advancement had overcome the initial deficiencies, some institutions have introduced new mechanisms providing direct user authentication on layer two. As a result, there are now different local WLAN installations and authentication procedures in place. This means that the challenge for the Eduroam activity is to define a trans-european roaming architecture while allowing for individual national (and organization-specific) user authentication mechanisms. The chosen architecture is described in [Mob03]. One of its core features is that it does not prescribe a specific access method. Instead, the architecture assumes that different variants will continue to exist, potentially in parallel at some institutions. Users are expected to be able to determine which mechanisms are available at a given site and to select the most appropriate one. The proposed solution to determine available mechanisms and to differentiate them is to use multiple ESSIDs (WLAN identifiers), each of which representing a specific access method and each of which being potentially mapped to a VLAN in the distribution network.

Because this process involves probing, which can be time-consuming and error-prone, the TERENA Mobility Task Force has initiated work on an "access point phone book" approach that is intended to provide information about WLAN infrastructures and individual access points but also about higher layer services at campuses, such as VoIP services.

The roaming process could be supported by providing users (and devices) with explicit knowledge about WLAN installations at visited campuses.This can be useful in different scenarios: 1) users could **obtain "WLAN maps" for a given visited network in advance**, e.g., when they are still at their home institution and require knowledge whether network access will be available at all and whether their current device configuration support the required network access procedures. 2) When visiting a foreign campus, information about the available network and required configuration parameters could be distributed in order to facilitate network access. In addition, information about higher layer services such as VoIP services could be distributed to facilitate network and service selection. Furthermore, users could be interested in *alternative* access networks, such as surrounding WLAN hotspots in order to enable mobility (e.g., when moving off-campus).

The following information is relevant for an information service for campus roaming: there is fundamental information such as the **location** of the network service that may be specified as a **geo-location** and/or a **civic address** and allows to select network services based on the location. Further fundamental service attributes are the **network operator**, the **service provider** (that may be different from the operator), and the **type of network**, i.e., the specific link layer technology, e.g., IEEE 802.11g.

At some installations, the WLAN access network is used to offer a set of different services, e.g., Internet access offered by different providers or different authentication mechanisms as pursued by Eduroam. There are different possibilities for multiplexing the fundamental WLAN access service for these multi-service scenarios. For example, it is possible to have users select the desired service (e.g., the service provider) on a web page of a captive web portal or to advertise multiple ESSIDs representing different services. In Eduroam, ESSIDs are used to advertise different authentication mechanisms, e.g., UAM (web-based), IEEE 802.1X, and VPN. The **supported authentication mechanisms** and the corresponding **ESSIDs** are therefore important parameters for network selection and device configuration.

In addition, the **type of service** should be described explicitly. For example, the Eduroam infrastructure typically provides network access to users' *home networks*, not necessarily Internet access in general. In addition to Eduroam connectivity, a site may offer additional services such as local access to information systems for guest users without an Eduroam affiliation.

Furthermore, users may be interested in detailed **information about the geographic coverage** of a WLAN infrastructure. In addition to the coverage area of a whole service set (such as a campus), some users might be interested in precise positions of individual access points, e.g., for optimizing access or avoiding interference but also to allow more precise calculation of their own position as may be needed for emergency calls.[9] This information is not required for common use

[9] Access point positions may even be exploited for maintenance applications.

cases and service usage decisions and should therefore only be made available upon request.

## Nomadic Usage of Public WLAN hotspots

Public hotspots provide some similarities to campus WLANs: they consist of a service set of WLAN access points and there can be multiple services that can be provided over the same "radio network", e.g., there can be multiple service providers that are offering services at a hotspot operated by a specific operator. The **hotspot operator** and the available **service providers** are important information for network selection, as users may have existing business relationships with specific providers. The applicable **tariff schemes** for different providers at a given hotspot and the **WLAN roaming possibilities** (and the associated costs) are additional important criteria. For example, a user might prefer hotspots (or providers) that allow for cost-efficient short connectivity sessions when she knows that she will only be within the coverage zone for a short period of time or will only need to use the service for a few minutes (e.g., to quickly send or retrieve email).

Public hotspot-based Internet access is often marketed by larger providers offering services at many different, isolated hotspots, i.e., the service is not geographically concentrated as for the campus WLAN scenario. Nomadic users who are, at a time, connected to a hotspot might thus be interested in **other hotspots of the same provider** in some geographic scope, e.g., in the vicinity or on their movement path. In heterogeneous network environments, user might also be interested in **other network services of the same provider**, e.g., a UMTS service that can provide coverage when moving between two hotspots.

## Shared Usage of Private WLAN installations

In addition to commercially operated hotspots there is an emerging sector of private WLANs that are opened for public usage through access-link sharing technologies, e.g., as developed by sofanet[10] and FON[11]. Guest users can associate to the private hotspot and gain Internet access (either for free or for paying the provider who is managing the sharing infrastructure). In this scenario, the private access point owner assumes the role of a **hotspot operator** while organizations such as sofanet and FON represent **providers**. The local infrastructure provides typical hotspot functions such as user authentication, accounting and, in addition, allows to separate the traffic of external users from the internal (private) traffic.

Similar to commercial hotspots, providers maintain lists of hotspot locations and offer services such as "hotspot locators" allowing users to **locate suitable private WLAN installations**, however the private WLAN service base provides a higher dynamics with respect to the set of available hotspots and parameters such as tariffs at individual hotspots (as they may be defined by the operator and/or the provider). As a result, information systems for privately operated hotspots must be able to accommodate a **a large and dynamic information set** for network services.

Private hotspot operators (and providers) may choose to offer differently priced services beyond Internet access, e.g., providers may offer free access to a selected set of websites (as currently offered by sofanet's *freegarden* service), and private operators may choose to provide additional services. The availability of these services may be interesting criteria for network selection, i.e., information services should support the distribution of **rich service descriptions** and the concept of **augmenting provider service descriptions by local operator service descriptions**.

## Closed Networks

Although most users will rely on *public* network services as described above, there are also *closed* networks, e.g., corporate WLANs and private home networks protected by WEP, WPA and other mechanisms that typically used to restrict usage to a certain user group. Although the availability of these network services is typically not announced in the public, some users will have legitimate

[10] http://www.sofanet.de
[11] http://en.fon.com

access to closed networks—in most cases, at least their home network. Therefore, closed networks can represent a possible network access option at a given location and should thus be considered for interface selection. This means, the network information system on a user's device should support non-public network service descriptions which may either be provided by the user herself (e.g., about her home network) or be **received over a non-public, secure channel**. For example, a company might provide network service information to employees over a secure, web-based distribution channel. In such cases, user are likely to **receive service descriptions from multiple sources**, i.e., public sources and non-public ones, and the network service management system on a user device must be able to **aggregate information from different sources to a coherent service map** that can be used (possibly also considering user preferences) to select the most adequate service at a given location.

## Extreme Usage Scenario: Drive-thru Internet

The previous subsections have discussed typical WLAN installations. These are typically designed for nomadic users but may also support mobile users if they can be accessed efficiently. An extreme example for mobile WLAN usage is the Drive-thru Internet approach [OK04a]. In this project, we aim at providing Internet services to mobile users moving at high speeds. Rather than using typically slow and expensive cellular networks, we enable network access by exploiting connectivity from conveniently located WLAN hotspots next to the road while the user traverses a hotspot's coverage area. The Drive-thru architecture allows existing and future applications to take advantage of such potentially short and unpredictable periods [OK04b]. 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. The *Persistent Connection Management Protocol* (PCMP) is used for the communication between the mobile Drive-thru client and the Drive-thru proxy, allowing for maintaining persistent transport layer sessions. [OK05a]. Figure 2 depicts an overview of the Drive-thru Internet architecture.

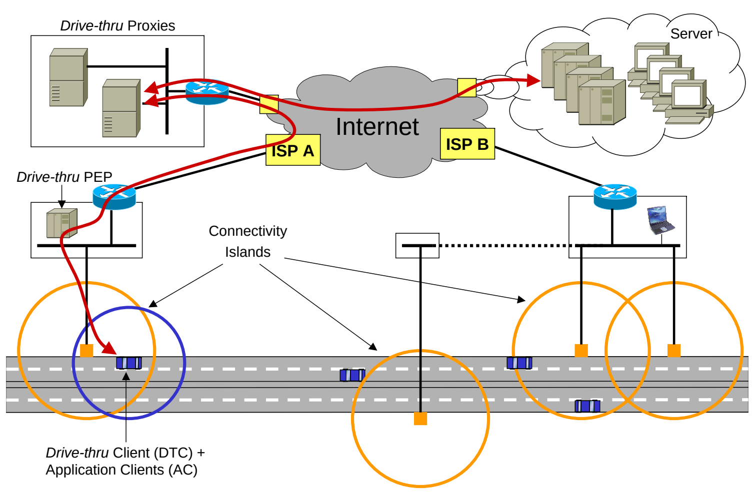


Figure 2: Drive-thru Internet Overview

Drive-thru Internet clients must be able to operate in today's *existing* WLAN infrastructure that mostly consists of public hotspots and private WLANs, i.e. in all of the four classes described above. In [OK05b], we have discussed requirements for automatic hotspot association in detail and, in [OKK], we describe a mechanism we have developed for automating the authentication process with different types of hotspots. The mechanism infers the type of the hotspot and its authentication mechanisms and associates on behalf of the user, relying on some heuristics and user preferences[OKK].

Without any IS, the only way to find out details about access points is to actually move into the coverage zone and initiate a probing process, which involves detecting the fundamental WLAN parameters (open/closed system, ESSID, usage of WEP/WPA), comparing this information to an internal database for hotspot selection, and then performing the actual authentication. In case of a public hotspot with UAM authentication, the system has to find out about the WISP (e.g., by analyzing the UAM web page) and then perform the authentication by providing the pre-configured user credentials. Because of the necessary probing steps—some of which have to be performed in a trial-and-error scheme—this process can take two seconds or longer. The plurality of authentication schemes and the diversity even within the perceivedly straightforward web-based authentication procedures that resemble the UAM approach but, nevertheless, exhibit serious differences may prevent automated authentication altogether unless hotspot-specific authentication rules are implemented in the mobile node.

From these considerations, two application areas for a network IS become apparent: 1) Learning about available Internet access services (hotspots) in the neighborhood including their access schemes and 2) learning about services available at a specific hotspot. Advanced information about available hotspots per 1) is especially useful for vehicular networking because, in many cases, the present position of the vehicle is known and its path is predictable. Knowing about the positions of eligible Internet services allows the connectivity management subsystem and the applications (if they can be made aware) to schedule their behavior according to expected connectivity and thus achieve a better user experience. If several hotspot providers are available in the same area, the choice may depend on which of these offers Drive-thru-specific services as add-on as can be determined per 2).

## Summary

The discussion of the four different scenarios has shown that there are different ways for interacting with an information service: users can obtain service information in advance, without actually being connected to the respective network, they can retrieve detailed service information and configuration parameters for a local service after associating, and they can use a current link for obtaining information about surrounding networks—of the same or a different network type.

In all four scenarios, we can identify **fundamental service attributes** that are required for identifying and selecting the service such as location, provider, type of service, etc. This information is of *strategic* nature in the sense that it is suitable for (policy-based) decisions which services to use when—be these decisions taken consciously by the user or automatically by her mobile device. We can furthermore identify **additional service information** such as detailed configuration parameters, utilization, precise device locations, etc. that is not important to the average user but is rather of *tactical* nature and used to efficiently execute the decisions taken before.

The scenarios differ in the way how information can be obtained locally. Some authentication approaches such as web- or VPN-based authentication provide the concept of *docking networks*, i.e., preliminary WLAN connectivity that may be used to distribute information, whereas other approaches require a complete authentication before the network can be used at all. Enabling services and optimizing performance on one hand while minimizing bandwidth utilization in mobile scenarios on the other hand require **making the fundamental information available directly and as early as possible**. Additional, non-critical information should not be distributed without solicitation, but should be made available over separate channels, i.e., requiring an explicit request for **refining a fundamental service description**.

Location information is one of the most important parameters in a service description as it is the basis for service selection. In order to allow identifying alternative service descriptions and to relate service description from different providers geographically to each other, **location information should rely on standardized location specifications** where possible, i.e., civic addresses for public places, sights and other landmarks should be standardized and used across service description from different providers. Complementary GPS coordinates allow for calculating distances to service points or areas independent of regional road maps being available.

It is particularly the location information that allows, for example, a Drive-thru Internet user to determine the next connectivity opportunity on her path. Peered with available tariff information, this allows the user ahead of time to determine whether to use a certain connectivity island for information exchange or whether to wait for the next (possibly cheaper) one. The link layer configuration parameters allow the mobile users device to tune into the right channels and the authentication information enable immediate authentication without the need for time-consuming heuristic operation so that, in total, the Drive-thru user can be granted instant access and can maximize utilization of the WLAN hotspot.

# 4 Approach to Network Service Maps

Based on the previously described scenarios and the derived requirements we have designed *Network Service Maps* intended to support nomadic and mobile users in WLAN environments with respect to robust and efficient service selection. Our resulting network service information system comprises two aspects: 1) the general architecture and the transport mechanisms for conveying service descriptions to mobile users and 2) the data model for service descriptions which is the focus of this paper.

## 4.1 Architecture and Transport

The general distribution framework is described in [KO]. We have defined a model for describing network services in a way suitable for distribution in heterogeneous, multi-operator networks, focusing on the following requirements: 1) use of a generalized network service description language that is not limited or tied to specific link-layer technologies and architectures; 2) scalability at both infrastructure and receiver side at least in terms of number of mobile users as well as services; 3) support for a wide range of service descriptions not limited to plain Internet connectivity; and 4) extensibility (for describing new services and configuration parameters).

The distribution framework is based on the Internet Media Guides framework [OKGL05] [NWL$^+$04] and enables information dissemination using three different distribution mechanisms to accommodate different networks and device capabilities. The ANNOUNCE mechanism provides broadcasting/multicasting and is envisioned for (but not limited to) unidirectional networks such as DVB-H. Clients obtain on-demand interactive access to service information using a QUERY/ RESOLVE mechanism and, in a complementary fashion, a SUBSCRIBE/NOTIFY mechanism allows clients to subscribe to service descriptions of a specific type that will received asynchronously (as update notifications). Users can choose the distribution mechanism that is best suited for them given their current network connectivity and preferences. The general framework is designed to be *network- and provider-independent* and does not rely on centralized information service providers. Instead, users can access multiple information services (e.g., operated by different network service providers) and may receive information from all of them, simultaneously or alternatingly depending on their current network connectivity. They may complement such public information services by private sources. The ability to receive and *aggregate* any number of service descriptions is a key concept allowing receivers to *construct their own service map* by combining input from multiple sources while filtering out duplicate and (currently) irrelevant information.

Figure 3 depicts a sample service map distribution setting: a local provider, e.g., a campus network operator maintains a local service map distribution infrastructure that can be used by local clients to obtain detailed information about the local network. This information can be made available via the ANNOUNCE mechanism, e.g., by broadcasting the fundamental service description over the WLAN docking network. In addition to local services, the local distribution infrastructure can also provide information about other providers' network services. E.g., the local provider may maintain a database of service descriptions for *ISP A* and *ISP B* that is kept up-to-date by relying on the SUBSCRIBE/NOTIFY mechanism. Furthermore, one of the local clients is interested in detailed service information from *ISP C* and performs direct QUERY/RESOLVE transactions in

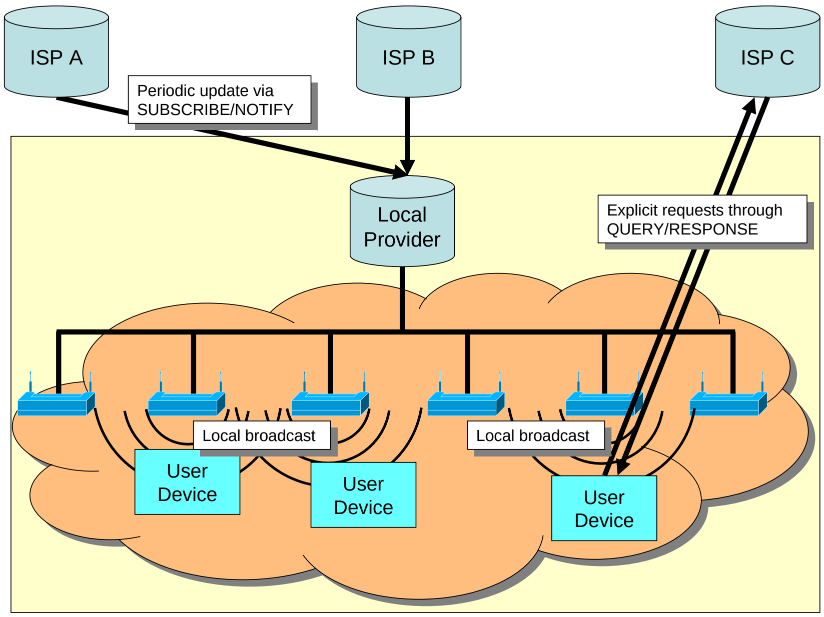


Figure 3: Service map distribution framework

order to obtain this information over the Internet connection provided by the local operator. The client thus retrieves service information from different sources via different channels and performs individual filtering and selection in order to generate a device- and user-specific network service map. The independent construction of service maps is enabled by a suitably defined *data model*, which is described in the following subsection.

## 4.2 Data Model for Network Service Maps

Our framework of Service Maps as introduced in [KO] provides a flexible means for describing arbitrary services. A key element towards building network service maps is the notion of *specializing* service descriptions in two dimensions: 1) refining a single service description from an overview version to a complete version; and 2) extending the data model for future services such as new network services and higher layer applications. The service description data scheme addresses the first aspect by *structuring* service descriptions into multiple segments that are suitable for individual transmission and processing: a service description can be divided into a general ("overview") part and the specific configuration details for a given service ("refinement"). This means that we do not rely on a flat key-value data structure as, e.g., proposed by the WiFi-Alliance smart-client approach [ABS03] and the Access Point Phone Book database structure of the TERENA TF-Mobility.

In order to address the extensibility aspect, we have defined a fixed set of base vocabulary and allow for application-specific extensions that can be uniquely distinguished from the base vocabulary and other extensions. The common base vocabulary includes fundamental service identification mechanisms (service identifiers, names, and providers) and application-independent vocabulary for specifying positions, service regions, pricing information, etc. These are subsequently correlated in *service instantiations*, which allows for effective description re-use.

Our service description format is based on XML, and we use XML Namespaces [BHLT04] for identifying vocabulary from different application domains.

A mobile node of a user interested in obtaining an overview of available WLAN Internet access services in a certain (geographic) region performs the following steps: 1) To obtain an overview of available services it may, e.g., passively listen to announcements distributed via a multicast transport. Information received in this way may be complemented by pre-configured or cached data from earlier operation.[12] 2) The mobile node selects interesting services—as determined by user preferences and the tasks to be accomplished—by geographic position/regional scope and service type. 3) For such specific services, say Internet access in some county, the mobile node requests details such as *type of network*, *tariff and roaming options*. 4) It finally matches this information against device capabilities, e.g., network interfaces, and configured user preferences such as roaming contracts, acceptable maximum cost and intended usage mode. For this procedure, the node extends the overview description by additional information by obtaining the *refinement information*. The overview variant of a service description specifies those parts that can be refined in future transactions and also provides information about the type of sub-descriptions, thus enabling user-devices to select those parts of the overall description that are relevant for their capabilities and user preferences.

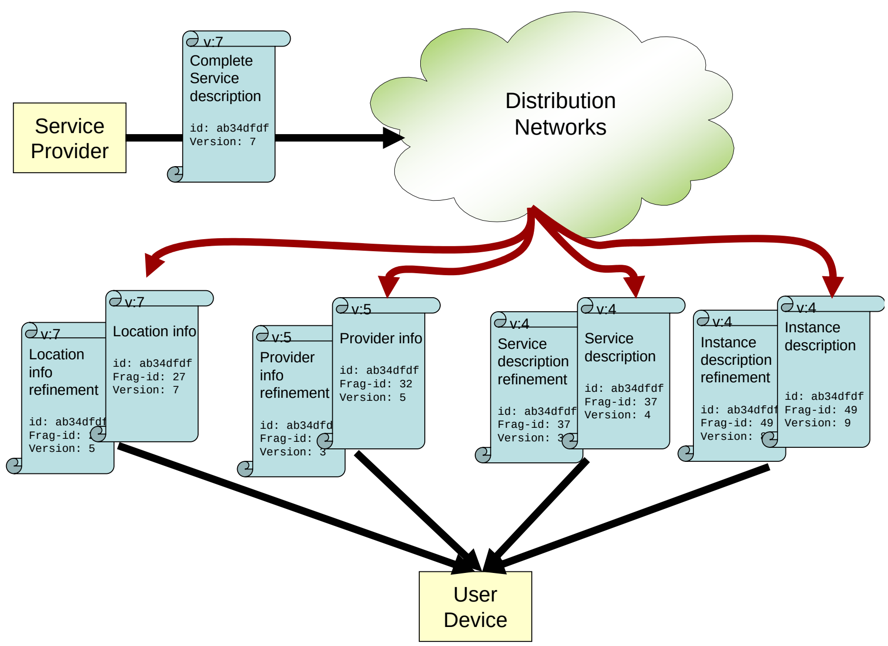


Figure 4: Specialization and Versioning of Service Descriptions

In addition to different specialization levels, our service description approach supports the notion of *versioning*: a service description (and its sub-parts) can change over time and thus be available in different versions that can be uniquely identified. In order to support efficient updates from a previous version of a service description (or from its sub-parts), we employ the concept of distributing *deltas* relative to a base version. Nodes that already have a base version only need to receive the corresponding delta, which can be obtained via one of the underlying transport mechanisms.

Figure 4 depicts the transport of service description fragments and their refinements to a receiver that selects the relevant sub-fragments and obtains the different fragments in oder to construct a complete service map, which is then fed into the construction of the overall regional service map.

The application-independent vocabulary leverages existing work where it is useful: for example, [Pet04] defines XML-based vocabulary for specifying different forms of location information

[12]For bootstrapping, the mobile node is initially configured with at least one well-known multicast transport address or interactively retrieves an initial set of service descriptions (including pointers to announcement services) via QUERY/RESOLVE when connected.

(geographic position, civic addresses etc.), and the Open Settlement Protocol (OSP, [ETS03]) defines XML vocabulary for describing pricing information, which can be built on.

The data model for service description consists of the following main components:

**Location specifications** are used to define named location records, e.g., for well-known public places, but also for arbitrary geographic positions, that can be referred by service instance descriptions. Locations can be represented as geographic location and/or civic addresses. In addition, it is possible to specify the *geographic scope* of a location, e.g., by defining a radius or a path.

**Provider specifications** are used to define named provider records for later referencing in service instance descriptions. The provider information is decoupled from the instance description because a single provider will often offer multiple service instances.

**Service descriptions** provide a provider-independent and location-independent description of a certain service, e.g., Eduroam access with UAM authentication or public WLAN access. This service can be offered at many different locations, by different providers and is thus only described in general. Service descriptions are named uniquely in order to be referenced in service instance descriptions.

**Service instance descriptions** are used for bundling a location, one or more providers, and one or more service descriptions to a specific service description for a given location. Service instance description reference previously defined location, provider and service descriptions.

Each of these information elements may be *refined* by augmenting the initially provided base information with detailed information. For example, location specification may be refined by descriptive information about a public place, provider specifications by contact details, and service descriptions by all sorts of application details. Finally, service instance descriptions may be refined with application-specific information that applies to a specific location. For an Eduroam scenario, the full list of access points with their geographic positions would be a good candidate for a refinement step.

All information elements may provide textual *tags* as a simple and flexible categorization mechanisms. For example, a WLAN network access service descriptions might be tagged with “WLAN” and “802.11”. These tags can later be used be receivers and other processing entities to select and filter service descriptions. It is expected that some kind of registry will guarantee a consistent usage of tags for the most common services. The following sample service description depicts the overall document structure and illustrates some rudimentary network service description vocabulary.[13]

```
<location id="uni-bremen-campus">
      <gp:location-info xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
       xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc">
         <cl:civicAddress>
          <cl:country>DE</cl:country>
          <cl:A1>Bremen</cl:A1>
          <cl:A3>Bremen</cl:A3>
          <cl:A6>Bibliothekstrasse</cl:A6>
          <cl:HNO>1</cl:HNO>
        </cl:civicAddress>
      </gp:location-info>

      <tag>Uni</tag>
      <tag>Universität</tag>
      <tag>Bremen</tag>
      <tag>HB</tag>
      <refinement
```

[13]Complete examples will be made available at https://prj.tzi.org/cgi-bin/trac.cgi/wiki/ServiceMaps.

```
        href="urn:img:example.org:20051051:service-map:location-uni-hb"/>
</location>

<provider id="uni-bremen" name="Universität Bremen"/>

<service id="local-access">
      <tag>802.11b/g</tag>
      <tag>local-link</tag>
      <refinement
       href="urn:img:example.org:20051041:provider:uni-hb"
</service>

<service id="internet-access">
      <tag>Internet</tag>
      <tag>Deutsche Telekom AG</tag>
      <dependencies type="all">
          <service-reference ref="local-access"/>
      </dependencies>
      <refinement
       href="urn:img:example.org:20051031:service-map:internet"
      </refinement>
</service>

<service-bundle id="uni-bremen-wireless-internet">
      <service-reference ref="local-access"/>
      <service-reference ref="internet-access"/>
</service-bundle>

<instance>
      <provider-reference ref="uni-bremen"/>
      <service-reference ref="uni-bremen-wireless-internet"/>
      <location-reference ref="uni-bremen-campus"/>
      <refinement
       href="urn:img:example.org:20051021:service-map:tcom-online-hbf-hb"/>
</instance>
```

The *service-bundle* element in the example is used to aggregate commonly used service combinations, such as local WLAN access and Internet access, into a single definition that can be referenced in *instance* definitions.

## 5 Conclusions

The network information service described in this paper can be characterized as a provider- and network-independent, and extensible approach that is built on the notion that receivers obtain service descriptions from arbitrary sources over different networks and compose *individual service maps* based on filtering with respect to current location, sought-after service, personal preferences, etc.

It differs from existing network information systems in its generality and network- and topology-independence, and it differs from existing service-location approaches in its applicability to wide-area, location-based service description distribution. The information service is based on a general service description information framework that provides different transport mechanisms for supporting heterogeneous network environments and on a data model for service description that enables receivers and transceivers to flexibly (re-) compose received service information with respect to different criteria.

We have developed a first implementation of the information system that is targeted at distributing network information for the campus WLAN an the university of Bremen. This implementation provides multicast service announcements (over the FLUTE-based ANNOUNCE transport) and HTTP-based QUERY/RESOLVE interactions. We are currently working towards to including network service information from other sources, e.g., from WLAN hotspot location databases.

The discussion in this paper has shown that with the emerging heterogeneity of wireless network environments (campus roaming, 3G-WLAN-DVB-H/DMB-based next generation networks) network selection and robust network association can become increasingly challenging. Networks differ with respect to fundamental services, higher-layer services such as VoIP and media-on-demand, association mechanisms, providers and tariff schemes, etc. At the same time, users are becoming more mobile, even in networks that have been designed for nomadic usage. Thanks to the increased availability of GPS and other positioning techniques (some of them requiring network attachment) users relying on a precise *map of available services in their region of interest* can be enabled to locate interesting access networks more quickly and can perform the actual network attachment more reliably: instead of falling back to time-consuming and error-prone probing processes they can learn of the available networks and their configuration in advance and perform educated decisions on network selection and handover in a *make-before-break* fashion.

Especially in campus-roaming scenarios, users can benefit significantly from comprehensive and universal network information systems. The heterogeneity in network topologies, authentication mechanisms, and network environments for campus WLANs call for a more structured and flexible approach for network information services. The network service maps approach presented in this paper allows sites to make their service information available for both on-site connected users and remote users, which can ultimately contribute to a higher acceptance and a better utilization of the existing infrastructure but can also support the introduction and deployment of new services in these networks. The next steps in further validating and expanding our approach are threefold: We seek to gather broader deployment experience by incorporating all the campuses presently contained in the Eduroam "phonebook" plus a selection of independent WLAN services in Bremen and Helsinki and then supply this information via a combination of ANNOUNCE and QUERY/RESOLVE mechanisms and also incorporate a corresponding client into our Drive-thru Internet environment. We want to validate the data model and the performance of the distribution mechanism by adding information about all known public hotspots in Germany. We finally want to explore support for selected higher layer services and experiment with both local and global service offerings where network service maps may serve both as a technical enabler but also as effective "marketing" instrument for introducing new service for mobile users in the future.

## 6 Acknowledgments

The authors would like to thank Mark Koch and Janico Greifenberg for valuable contributions to discussions about the network service maps concept.

## References

[ABS03] 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.

[BHLT04] Tim Bray, Dave Hollander, Andrew Layman, and Richard Tobin. Namespaces in XML 1.1. W3C Recommendation, February 2004. http://www.w3.org/TR/xml-names11/.

[BWSF03] Marc Bechler, Lars Wolf, Oliver Storz, and Walter J. Franz. Efficient Discovery of Internet Gateways in Future Vehicular Communication Systems. In *Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference (VTC 2003 Spring), Jeju, Korea*, April 2003.

[CFL$^+$05] Hemant Chaskar, Daichi Funato, Marco Liebsch, Eunsoo Shim, and Ajoy Singh. Candidate Access Router Discovery (CARD). RFC 4066, July 2005.

[Cor00] Microsoft Corporation. Universal Plug and Play Device Architecture. available online at http://www.upnp.org/, June 2000.

[DFHX05] Greg Daley, Stefano Faccin, Eleanor Hepworth, and Qiaobing Xie. Some Requirements for a Handover Information Service. Internet Draft draft-faccin-mih-infoserv-01.txt, Work in progress, October 2005.

[Dri] Drive-thru Internet Project. http://www.drive-thru-internet.org/.

[(Ed05] Rajeev Koodli (Ed.). Fast Handovers for Mobile IP. RFC 4068, July 2005.

[ETS03] ETSI. Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Open Settlement Protocol (OSP) for Inter-Domain pricing, authorization and usage exchange. ETSI TS 101 321 V4.1.1, November 2003.

[FW05] Licia Florio and Klaas Wierenga. Eduroam, providing mobility for roaming users. In *EUNIS 2005 Conference Proceedings*, 2005.

[GPVD99] Erik Guttmann, Charles Perkins, John Veizades, and Michael Day. Service Location Protocol, Version 2. RFC 2608, June 1999.

[IEE05] *IEEE P802.21/D00.01, Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services*. IEEE, 2005.

[KK05] James Kempf and Rajeev Koodli. NEighborhood Discovery (NED) for Wireless Networks. Internet Draft draft-kempf-mipshop-nhood-discovery-00.txt, Work in progress, June 2005.

[KO] Dirk Kutscher and Jörg Ott. Service maps for heterogeneous network environments. submitted for publication.

[KO03] Dirk Kutscher and Jörg Ott. Dynamic Device Access for Mobile Users. In *Proceedings of the 8th Conference on Personal Wireless Communications*, 2003.

[Mic01] Sun Microsystems. Jini Architecture Specification Version 1.2. available online at http://java.sun.com/products/jini/, December 2001.

[Mob03] TERENA Task Force Mobility. Preliminary selection for inter-nren roaming. TERENA Deliverable, December 2003.

[NWL$^+$04] Yuji Nomura, Rod Walsh, Juha-Pekka Luoma, Hitoshi Asaeda, and Henning Schulzrinne. A Framework for the Usage of Internet Media Guides. Internet Draft draft-ietf-mmusic-img-framework-08.txt, Work in Progress, July 2004.

[OK04a] Jörg Ott and Dirk Kutscher. Drive-thru Internet: IEEE 802.11b for „Automobile“ Users. In *Proceedings of the IEEE Infocom 2004 Conference, Hong Kong*, March 2004.

[OK04b] Jörg Ott and Dirk Kutscher. The “Drive-thru” Architecture: WLAN-based Internet Access on the Road. In *Proceedings of the IEEE Semiannual Vehicular Technology Conference May 2004, Milan*, May 2004.

[OK05a] Jörg Ott and Dirk Kutscher. A Disconnection-Tolerant Transport for Drive-thru Internet Environments. In *Proceedings of the IEEE Infocom 2005 Conference, Miami*, March 2005.

[OK05b] Jörg Ott and Dirk Kutscher. Exploiting Regular Hot-Spots for Drive-thru Internet. In *Proceedings of KiVS 2005, Kaiserslautern, Germany*, March 2005.

[OKGL05] Jörg Ott, Dirk Kutscher, Janico Greifenberg, and Kevin Loos. Networked Multimedia with Internet Media Guides. In *Proceedings of the TERENA Networking Conference, TNC 2005, Poznan*, June 2005.

[OKK] Jörg Ott, Dirk Kutscher, and Mark Koch. Towards Automated Authentication for Mobile Users in WLAN Hot-Spots. In *Proceedings of VTC Fall 2005*.

[Pet04] J. Peterson. A Presence-based GEOPRIV Location Object Format. Internet Draft draft-ietf-geopriv-pidf-lo-03.txt, Work in progress, September 2004.

[ST03] Terry Schmidt and Anthony Townsend. Why Wi-Fi Wants To Be Free. Communications of the ACM, Vol 46, No 5, 2003.

[Wei05] Aaron Weiss. The Battle for Broadband. *ACM netWorker*, 9.2, June 2005.

[Wil05] Michael G. Williams. Directions in media independent handover. *IECE Transactions Fundamentals*, E88-A(7), July 2005.

[Wir03] Boingo Wireless. Toward Ubiquitous Wireless Broadband. Boingo Wi-Fi Industry White Paper, September 2003.

# Vitae

## Dirk Kutscher

Dirk Kutscher is a researcher at TZI, Universität Bremen. He received his doctoral degree in Engineering (Dr.-Ing.) from Universität Bremen in 2003. He has worked in several national and international research projects in the areas of wireless and interpersonal multimedia communications, e.g., in the European FP5 IPv6 Wireless Internet Initiative (6WINIT). His dissertation focuses on local coordination for component-based systems. Dirk has continuously participated in IETF standardization since 1998 and has co-authored two books, several Internet Drafts, RFCs and scientific publications. His current research focus is on architectures and communication protocols for challenged environments, and he is participating in the on-going research project Drive-thru Internet. In 2005, Dirk has been invited to a research visit at KDDI R&D Labs. Inc. in Yokosuka Research Park, Japan, where he has investigated new approaches for simulating wireless communication protocols and media media-independent handover services for future heterogeneous networks.

## Jörg Ott

Jörg Ott holds a Diploma in Computer Science and in Economics. He received his Doctor in Engineering (Dr.-Ing.) in 1997 from Technische Universität Berlin. Since March 2005, he is Professor for Networking Technology with a focus on Protocols, Services and Telecommunications Software at the Networking Laboratory in the Electrical and Communications Engineering Department at Helsinki University of Technology. From 1997 through early 2005, he was Assistant Professor in the Computer Networks group at the Universität Bremen and member of the Center for Computing Technologies (TZI). From 1992 through 1997 he worked as a research staff member with teaching responsibilities at TU Berlin. His research interests are in protocol and system architectures for multipoint communications, content distribution, and multimedia conferencing, including Internet Telephony as special interest area. His current research focus is on communication in challenged networks, particularly on disruption-tolerant networking. In the IETF, he is co-chair of the MMUSIC working group since 1997 and has been co-chairing the SIP working group from its foundation in 1999 to October 2002.