Improving Access Discovery by Analysing World-Model Information

Stephan Lück, Andreas Gutscher

University of Stuttgart
Institute of Communication Networks and Computer Engineering
Pfaffenwaldring 47, D-70569 Stuttgart
e-mail: {lueck,gutscher}@ikr.uni-stuttgart.de

Abstract

So far, mobile terminals discover available access networks mainly by means of measurements at their physical interfaces. Information acquired by these measurements are often not sufficient to perform optimal access network selection decisions. Therefore, we present an approach, which uses world-model data to provide access selection algorithms with more information. Because this world-model information, originating from different sources, can be contradictory, we propose to use a reputation system to rate the quality of these different data sources.

1. Introduction

Platforms providing location-based and context-aware services make only sense if there are mobile terminals, which have network access at almost every place with the highest bitrate as possible. Unfortunately, large coverage area and high bitrate are often conflicting requirements. Cellular networks cover large areas but offer a rather low bandwidth and high delays, whereas Wireless LANs (WLANs) often provide considerably more bandwidth and lower delays but cover only small areas. Therefore, it is desirable to enable mobile terminals to dynamically select the access network, which offers for example the best bitrate-delay-combination suited for the applications currently running on this terminal. In addition, to make context-aware and location-based services affordable to the user, communication costs should be minimized. Terminals that have access to multiple access networks of heterogeneous technology and try to select the currently most appropriate access network are often called to be *Always Best Connected* [1].

We subdivide the functionality needed to realise Always Best Connected communication into three sub-problems: *Access Discovery*, *Access Selection* and *Protocol Mechanisms*. Access Discovery serves to discover access networks available to a mobile terminal and to determine parameters describing the characteristics of the discovered access network. The information gathered by the access discovery function is processed by access selection algorithms. Access selection algorithms choose the access network, which is best suited for a given application and then apply protocol mechanisms to realise their access selection decision. This paper describes our approach concerning Access Discovery.

Our work is part of the center of excellence *Spatial World Models for Mobile Context-Aware Applications (Nexus)* [4] at University of Stuttgart. An important element of research activities within this center of excellence is a data model — the *Augmented World Model (AWM)* — describing physical objects assigning location, extent, and additional attributes to them. In particular, it is possible to describe access networks. Hence, our idea is to improve access discovery by analysing world-model information.

When introducing world-models describing access networks, the question arises how to acquire the needed data. Basically, two approaches are possible. Firstly, network operators could feed data they have extracted from their network management systems into the world-model. Secondly, model information could be generated by third parties, especially users, which are moving around in radio cells of a certain network taking signal strength measurements and making them available to other users.

The Nexus platform was designed to be an open system, this means, everybody can use the platform to retrieve information, offer services and contribute to the content of the Augmented World Model (AWM). Therefore, we cannot simply rely on the correctness of information provided by unknown users. We propose the integration of a reputation system into the AWM in order to improve the ability to distinguish trustworthy from unreliable information.

The paper is subdivided into two parts. Section 2 describes how the content of world model can be used to improve access discovery whereas Section 3 focuses on how the reputation system determines the trustworthiness of model information.

2. World-Model-Based Access Discovery

Access discovery methods typically take into account only measured values taken on the physical interface on a mobile terminal such as signal-to-noise-ratio and evaluate access technology specific data broadcasted within a beacon signal. We call such methods *Measurement-Based Access Discovery*.

Measurement-based access discovery is well-suited for terminals, which can use one access technology only, such as most of todays cell phones. Terminals that can handle multiple access technologies possibly provided by different network operators can make better network selection decisions if they have additional information about access networks, which cannot be acquired by simply listening to beacon signals. This information comprehends among other things the location and the extent of radio cells, QoS-related information, such as bitrate and delay, the description of available services, and the cost of usage of an access.

This information can be represented by a data model [3], which is part of the Nexus Augmented World Model. Therefore, we call the access discovery approach, which uses this additional information *Model-Based Access Discovery.*

The access network data model also contains unique *Technology Specific Access Identifiers (TSAIs)*, which are different for each access technology. WLANs, for example, use access point MAC-addresses to identify a cell and GSM/UMTS use the so-called *cell global identification*. Because they do not only appear in the world-model but also appear in beacon signals, TSAIs serve as links between measurement-based access discovery and model-based access discovery.

Using TSAIs as links between measured data and world-model objects allows for realising one certain type of access discovery scenario: the augmentation of measured data with model data by combining measurement-based and model-based access discovery. In these scenarios, the mobile terminal uses measurement-based access discovery to determine the set of networks it currently has access to. Then it extracts from these data one TSAI for each access network. Using the TSAIs, the terminal queries the world-model for additional information about each access network.

Another type of scenarios queries the world-model for data about networks, which are currently not visible to the mobile terminal. In particular, if it can determine its position, the terminal can access information about neighbouring networks. For example, if a terminal has access to a quite slow cellular network such as GRPS or UMTS but knows because of world-model information that there is a WLAN cell some meters away from its actual position, it can postpone a data transmission expecting the user will eventually enter the WLAN cell. Alternatively an application running on the terminal could even ask the user to move to the WLAN.

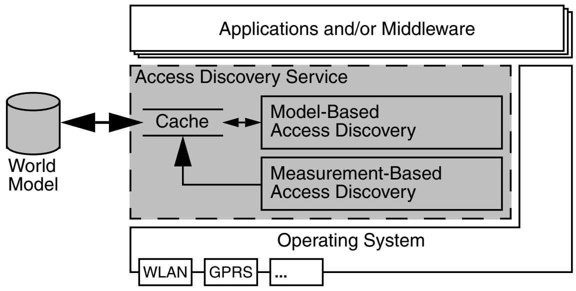

Fig. 1: Mobile Terminal Software Architecture

Figure 1 shows the software architecture, realising model-based access discovery. We believe that in future not only access technology will be heterogeneous but also protocols will be. In particular, there are multiple protocols providing mobility support working at different protocol layers such as Mobile IP, which is working at the IP-layer or SIP, which is an application layer protocol.

Therefore the access discovery function is placed in a separate component called *Access Discovery Service*. This approach allows for combining different access selection policies and protocol mechanisms with this access discovery service. Access selection and protocol mechanisms can be realised either by middleware or by special applications, which are adaptive in respect to available communication resources. The cache in figure 1 allows the terminal to maintain a local world-model. It is even thinkable to operate on the local world-model only without accessing a distributed world-model.

3. Reputation System

In Section 2 we showed, that world-model information can indeed improve access discovery, but obviously, the model information will not be useful unless it is correct. The AWM, however, is part of an open platform, i.e., everybody can insert data into the AWM and users will not be able to distinguish between correct and wrong information. Users have to cope not only with inadvertently entered invalid data but also with intentionally manipulated access network information in the AWM.

One promising approach to cope with this problem is the integration of a reputation system into the platform allowing users to exchange their opinions about the correctness of the information in the AWM. The basis of the reputation system is provided by a mathematical model for opinions. Different models for expressing and calculating with opinions and trust have been proposed (e.g. [5], [6]) and we are currently analysing the suitability of the models for our platform. Although there are significant differences between these models, the basic approach is similar. Each model defines basically two aspects:

1. It defines how to formally express opinions. Apart from naming a subject, a proposition and a property (*"Who beliefs, that which proposition has which property?"*), the degree of belief has to be expressed quantitatively, which is done for example by mapping an opinion to one or two values in the interval between zero and one.
2. It provides a set of operations which can be performed on opinions or defines a set of rules specifying which new opinions can be derived from a set of given opinions. This allows the user to calculate with opinions, e.g., to merge two opinions into a single resulting opinion.

Using this model, users can express their opinions about two issues: Firstly, they can express whether and to which extent they consider some model information to be correct (*information rating*) and secondly, whether and to which extent they trust the opinion of some other user (*trust rating*). Here, two types of trust can be distinguished: *Direct trust* refers to the honesty and competence of the other user to issue useful information ratings, whereas *indirect trust* (or *recommendation trust*) refers to the honesty and competence of the other user to give useful recommendations for a third user issuing useful information ratings. It is possible and useful, to limit the number of allowed indirection hops.

The general approach for validating the trustworthiness of a given information is to search for chains of recommendations, trust ratings and information ratings starting from the user himself and leading to the indicated information, calculating the resulting trust value and deciding whether this value is equal or higher than the required value.

Initially, each user stores his own ratings in a local reputation database. In order to share their knowledge, users can transmit all or a subset of their ratings in the form of digitally signed certificates to the reputation database of the AWM. Users can search the AWM reputation database for ratings concerning a given information or user, download the certificates and cache them in their local reputation database.

The access discovery function can then try to determine the trustworthiness of a given information in the AWM by applying the rules to the ratings in the local reputation database. However, there is no guarantee that the evaluation will be successful. It can happen, that the required ratings are not present, but often the problem can be solved by searching specifically for missing links of almost complete certificate chains.

The use of a reputation system can certainly help to distinguish trustworthy from unreliable information and improve the quality of the information passed to the access selection function, however it involves also some inconveniences. Apart from the fact, that it should be avoided to consume too much bandwidth and computing power of mobile devices, the choice of the own trust ratings could turn out to become a major problem. Users might find it to be difficult to decide, whom they should trust, to which extent and whether this trust also applies for recommendations because the don't have the necessary insight into the functioning of reputation systems. Unfortunately, this question cannot be adequately answered by an algorithm and it is not possible to name a useful default value. Considering everybody trustworthy does not protect the user from untrustworthy information at all, whereas considering everybody as untrustworthy classifies any information untrustworthy. Reputation systems cannot provide benefits unless the user is able to rank the trustworthiness of other users.

4. Conclusions

This paper shows how world-models can provide additional information to improve access discovery. If potentially untrustworthy individuals contribute to the content of the world-model, an integrated reputation system can help to distinguish trustworthy from unreliable information. However, this approach requires applications and middleware to be adapted so that they can coordinate their communication activities with the access discovery service.

References

[1] Eva Gustafsson and Annika Jonsson: "Always Best Connected", IEEE Wireless Communications February 2003

[2] Licia Capra, Wolfgang Emmerich, Cecilia Mascolo: "CARISMA: Context-Aware Reflective mIddleware System for Mobile Applications", IEEE Transactions on Software Engineering, 2003

[3] Stephan Lück, Susanne Bürklen, Frank Dürr, Matthias Großmann, Michael Scharf: "Ein Schema zur Beschreibung von Zugangsnetzen für das Nexus-Umgebungsmodell", Nexus-Projektbericht, April 2004

[4] Center of Excellence "Spatial World Models for Mobile Context-Aware Applications", University of Stuttgart, `http://www.nexus.uni-stuttgart.de`

[5] Audun Jøsang: "Artificial Reasoning with Subjective Logic", 1997

[6] Ueli Maurer: "Modelling a Public-Key Infrastructure", 1996