Shaping the Future Internet

Erwin Aitenbichler, Alexander Behring, Dirk Bradler, Melanie Hartmann,
Leonardo Martucci, Max Mühlhäuser, Sebastian Ries, Dirk Schnelle-Walka,
Daniel Schreiber, Jürgen Steimle, and Thorsten Strufe

Telecooperation Lab, Technische Universität Darmstadt,
64289 Darmstadt, Germany

Abstract. The Internet of Things (IoT) and the Internet of Services (IoS) are two well-known exemplars of the emerging 'Internet variants'. These variants will be tightly interwoven yet specific with respect to the supporting technologies needed. The present paper discusses the five variants identified as essential by the authors: IoT, IoS, Internet-of-Humans, Internet-of-Crowds, and Internet-of-Clouds. For each variant, a non-comprehensive set of research challenges is cited and related to the state of the art and to ongoing projects of the lab.

1 Introduction

Academic research about and public and commercial interest in the Future Internet is obviously split into two camps. The first camp sees a pressing need for the (r)evolution of the IP and related network protocols plus corresponding concepts in order to satisfy perceived future traffic characteristics and quality demands. Others look at future challenges more from an application perspective and see an urgent need to provide support for several interwoven 'special variants' of the Future Internet - each of which is likely to eventually outgrow the entire Internet as it is today. In the eyes of the second camp, the concepts developed by the first camp shall provide the 'bit pipe' for the concepts they work on. The authors of the present paper consider themselves members of the second camp. The paper will discuss five 'Internet variants' which the authors identified as essential. After a brief introduction of these variants below, the remainder of the paper will strictly follow the sequence of these five variants. For each variant (and paper section), major research challenges will be identified and the state of the art and relevant projects will be cited. Due to space constraints, the treatment of these challenges can by no means be comprehensive. Nevertheless, interested readers should be able to get an interesting insight into the issues of relations among ('second-camp') Future Internet research. As depicted in Fig. 1, the following five 'Future Internet variants' shall be considered:

1. Internet-of-Things: this 'oldest' variant relates to non traditional entities connected to the Internet (neither desktop computers nor servers nor humans using them): in terms of ubiquitous computing, IoT elements can be separated into "things worn" (mobile devices, biosensors, wearables) and "things encountered" (smart labels, networked sensors, and embedded devices). While smart

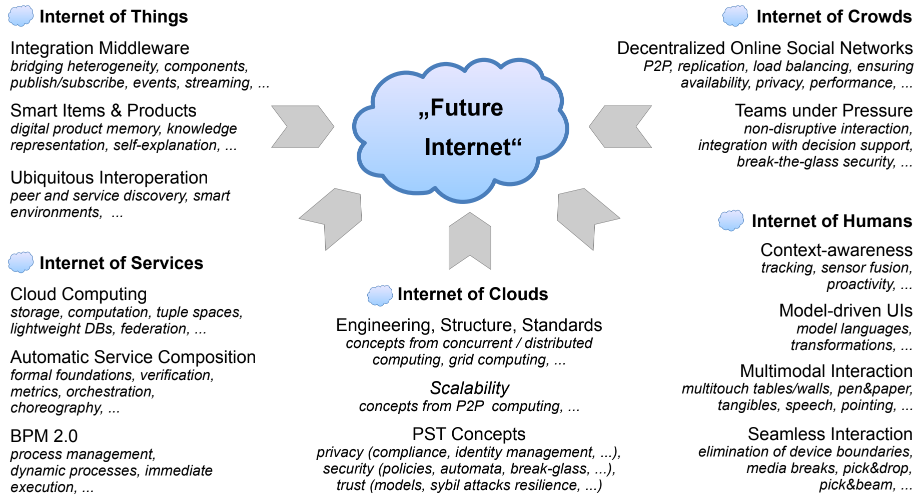
„Future Internet“
Internet of Things
Integration Middleware
bridging heterogeneity, components, publish/subscribe, events, streaming, ...
Smart Items & Products
digital product memory, knowledge representation, self-explanation, ...
Ubiquitous Interoperation
peer and service discovery, smart environments, ...
Internet of Services
Cloud Computing
storage, computation, tuple spaces, lightweight DBs, federation, ...
Automatic Service Composition
formal foundations, verification, metrics, orchestration, choreography, ...
BPM 2.0
process management, dynamic processes, immediate execution, ...
Internet of Clouds
Engineering, Structure, Standards
concepts from concurrent / distributed computing, grid computing, ...
Scalability
concepts from P2P computing, ...
PST Concepts
privacy (compliance, identity management, ...), security (policies, automata, break-glass, ...), trust (models, sybil attacks resilience, ...)
Internet of Crowds
Decentralized Online Social Networks
P2P, replication, load balancing, ensuring availability, privacy, performance, ...
Teams under Pressure
non-disruptive interaction, integration with decision support, break-the-glass security, ...
Internet of Humans
Context-awareness
tracking, sensor fusion, proactivity, ...
Model-driven UIs
model languages, transformations, ...
Multimodal Interaction
multitouch tables/walls, pen&paper, tangibles, speech, pointing, ...
Seamless Interaction
elimination of device boundaries, media breaks, pick&drop, pick&beam, ...

Fig. 1. Research Challenges to Shape the Future Internet

labels and particularly RFIDs and corresponding infrastructures attracted the majority of focus due to perceived immediate commercial benefit, they are only the forefront of a vast variety of IoT elements to joint the net.

2. Internet-of-Services: while the Internet has penetrated enterprises for years, not much of our economy has migrated its ‘core of business’ onto the net. WebServices are often a mere ‘window’ onto the offerings of an enterprise that remain a hidden vast web of digital and real assets. IoS goes a significant step further towards providing a fully-fledged digital equivalent to offerings (i.e. services in the economic sense) of the enterprise. This means that human and software based entities alike can process these economic-services: negotiation, bidding and contracting, and global interweaving towards composite services can now happen in the Internet, it becomes the full-fledged market place of the changing economy.

3. Internet-of-Humans: This one is probably the most ‘forgotten’ variant of the Future Internet. However, in order for the IoT and IoS to happen on a global scale, Humans must be empowered with a service-independent ubiquitous access to the Future Internet. This access and use concept has to hold and enforce the user’s wishes and needs in a fully trusted way independent of any ‘provider’ but compatible with all the services and ‘smart things’ encountered on the globe.

4. Internet-of-Crowds: As digital devices and services interweave around the globe, two global-network trends come into focus: one of them is the combination with social networks. Both users and providers of services (and ‘smart things’) can draw considerable benefit from the inclusion of social networks of all kinds, and social networks, at a closer look, suggest a wealth of ‘connection points’ to IoT and IoS offerings.

5. Internet-of-Clouds: The second 'logical consequence' of a globally interwoven IoS/IoT infrastructure is the use of Cloud Computing as an 'obvious' platform of choice. The paper will briefly sketch the reasons for which a highly dynamic infrastructer - an hence, 'the cloud' - is indispensible as a foundation for both IoS and IoT.

All five variants mentioned above are particular and self-contained enough to require specific concepts and support (and thereby, dedicated research). Therefore, we will dedicate a separate section to each of them. On the other hand, they overlap considerably, e.g., regarding their need for privacy, security, and trust concepts. This aspect will be furthered where appropriate in the paper.

2 Internet of Things (IoT)

The IoT operates on a wide spectrum of computing platforms, vastly different in terms of size, mobility and usability. The lower end of this spectrum is marked by computers embedded into everyday objects and small sensor nodes with limited processing capabilities. Most importantly, the real power of the IoT emerges from the cooperation of many devices. Hence, communication and federated computing are fundamental requirements. Because the communication requirements of devices are as diverse, several different wireless networking technologies are in place. To address the high degree of heterogeneity of platforms and networking technologies, we have created the communication middleware MundoCore [1]. It is based on a microkernel design, supports dynamic reconfiguration, and provides a common set of APIs for different programming languages on a wide range of different devices. The architectural model addresses the need for proper language bindings, different communication abstractions, peer-to-peer overlays, different transport protocols, different invocation protocols, and automatic peer discovery.

We also observe today that Smart Items are evolving into Smart Products. While Smart Items show a rather passive behavior, i.e., giving goods identity, monitoring, or logging, Smart Products have more self-awareness and can actively interact with their surroundings. They are real-world objects, devices or software services bundled with knowledge about themselves, others, and their embedding [2]. They are motivated by the increased complexity of technical products today. The ongoing EU FP7 project *Proactive Knowledge for Smart Products* [3] aims to create products that can accumulate and use knowledge during their entire lifecycle, from manufacturing, through usage by the end user, through maintenance, to recycling.

While the technical design of the building blocks and that of suitable communication middleware of the IoT is already well understood, the sensible integration and cooperation of artifacts still remains an open issue. Concepts for the interoperation on a semantic level, allowing artifacts to cooperate in truly open environments, are needed.

3 Internet of Services (IoS)

The reuse of software components has already been a subject of research for decades now. However, the Service-oriented Architecture (SOA) architectural style moves away from a purely technical viewpoint. It aims to bring the worlds of business and information technology together. In contrast to, e.g., Distributed Object Computing systems, SOA models components "at the right" granularity. Components have a concrete meaning as a business artifact and at the same time, they have a clearly defined technical functionality. Hence, this helps business analysts and software engineers to speak the same language.

Because Web Services are based on widespread Internet technologies, they have the power to bring SOA to the Internet. However, today, Web Services are hardly used across the boundaries of multiple organizations. This aspect is currently addressed by large research projects, such as Theseus/TEXO [4]. TEXO envisions the IoS, where services become tradable goods. Participants can offer or acquire services through marketplaces in the Internet. The IoS may boost modern economic concepts to unprecedented levels, revolutionizing global commerce, virtual enterprises, and ultra lean businesses. One concrete IoS challenge will be cited here as an example: if an enterprise searches for an outsourcing partner, it needs the appropriate instruments to do so. Among the most important criteria is process compatibility, which ensures that the processes of different enterprises seamlessly link into each other and finally lead to the desired goal. Current research in our lab investigates techniques for process matching, measuring process similarity, and automatic service composition.

A prerequisite for matching processes is a formally-founded description of processes. However, most modeling languages used today do not fulfill this criterion. For example, BPMN was designed to document processes among humans, but only part of its semantics is well-defined and therefore executable and verifiable. Petri Nets are at a low semantic level and therefore not very vivid, miss message semantics, mix aspects, and lack concepts for hierarchy. Subject-oriented BPM [5] is a promising new approach to build future SOA systems.

4 Internet of Humans (IoH)

One of the main challenges is to enable users to interact with the future Internet. The number of services, appliances, devices and situations supported ("usage contexts") keeps proliferating at an enormous speed. As a consequence, improved support for the humans in the loop becomes a prevailing challenge: How to create natural and usable UIs for all these contexts? How will future user interfaces for multiple contexts of use be created? How to adapt the layout and the behavior of UIs? And how to provide interactive, non-obstrusive access to the increasing wealth of services to the nomadic user? Approaches to these questions will be addressed below.

Model Driven Development of User Interfaces: In our point of view, model-driven development approaches can address these issues. Mapache [6] is a research platform and framework for model-driven UI development, created in our group and based on our previous work in eMode. Through Mapache, one application can be enhanced with multiple user interfaces. Modifications can "mechanically" or "computationally" be distributed to multiple of these UIs. Above this, we put an emphasize on the conjoint refinement of layout and behavior. Consequently, behavior can be modified for every UI when needed.

UIs for new usage contexts can automatically be generated with Mapache's Solverational approach, a transformation engine and language based on constraints and optimization [7]. Hereby, usability rules are encoded into the transformations. The look and feel can nevertheless be controlled very fine-grained, as the UI developer is in charge and can modify all Mapache artifacts.

Ubiquitous Computing and Smart Products: In terms of natural interaction, an emphasis must be put on the natural integration of computers and environment, as they are not separated by dedicated interaction devices anymore. Having computers tightly integrated into the environment will change our expectation about them, e.g., regarding usability, combinability, robustness and responsiveness.

The above-mentioned Smart Products project [3] addresses these issues. Smart Products are designed to facilitate the interaction between human and product; hence, they have to convey the user's interaction with respect to these challenges. Smart Products are able to explain themselves to the user and offer proactive advice. The challenge hereby is how to best use the limited available input and output capabilities, e.g., by leveraging interaction devices in their environment.

Voice-based Interfaces are an important concept towards the invisible computer. Users may have their hands busy while performing everyday tasks, thus severely limiting their ability to interact with traditional hands&eyes devices, i.e., mouse and keyboard.

Voice UIs (VUIs) are difficult to build due to their *transient* and *invisible* nature. Unlike visual interfaces, once the commands and actions have been communicated to the user, they "are gone". Beside objective limitations of a voice channel, human factors play a decisive role: auditive and orientation capabilities, attention, clarity, diction, speed, and ambient noise. These aspects can be grouped into *technical challenges* and *audio inherent challenges* [8].

In mobile environments, aspects such as computational power and memory pose strong limitations that cannot be handled by conventional implementations. To solve this, most of the research utilizes a speech service running in the network, and employing traditional client/server architectures [9]. The fact that there may be multiple audio input and output devices, and multiple text-to-speech engines and speech recognizers with different capabilities in a given environment remains untouched in most of the current techniques and is the focus of our research towards a ubiquitous computing speech API.

Pen and Paper Interaction: In the domain of ubiquitous computing, augmenting everyday objects by electronic functionality is a viable approach. Paper, a ubiquitous medium, which is used for thousands of years is more powerful than computers in many respects [10]. To cite only some examples, paper is cheap, mobile and can be easily written and sketched on.

Previously researched issues like, e.g., support for taking handwritten notes, annotating paper documents or mapping paper contents to digital contents is rather well-understood. But there still exist fundamental challenges of bridging paper with the internet. This comprises first how people can collaborate over the distance using real paper and second how digital feedback can be provided on the paper medium.

Previous and ongoing work of our group addresses the first issue. We have developed novel interaction techniques and implemented a system prototype which allows users to collaboratively annotate, link and tag documents, both in printed and digital form [11]. Users can work locally with paper and share information over the Internet. Remote information is displayed in several novel visualizations for user generated content which is created on paper. In order to integrate paper-based input and display-based output channels, we contribute pen-based interaction techniques which closely integrate paper with displays. This brings the integration of paper with the Net a significant step further.

The second issue, how to provide digital feedback, has initially been addressed using voice-based feedback or separate displays. Recent approaches use mobile projectors to overlay visual contents directly on paper. In our group, we are currently developing a software framework which supports application developers in flexibly providing different types of feedback, using audio, mobile phones, nearby displays, and mobile projectors.

Secure Communication & Anchor of trust: In the Internet of Humans, an important aspect is also how people can securely communicate with smart environments. As part of the Mundo project, we have created the notion of the "Minimal Entity" (ME) and as prototypical implementation the Talking Assistant device. The ME acts as the user's representative in the digital world. It carries the user's digital identity and is able to perform operations such as authenticating the user to other parties. The ME is designed as a *secure terminal* and thus allows to securely perform transactions - possibly with legal impact - in an Ubicomp world. We believe that interaction with the ubiquitous infrastructure will mainly happen through a personal device, owned by each user, that may serve as an anchor of trust. This is because it will represent the user in the digital world and carry out transactions, sometimes with only implicit consent of the user. Hence, it is vital that a user is able to trust the device carrying out these actions. The easiest way to instill this trust in users is to have them actually own the device instead of relying on a networked service, which may remain an abstract concept for many users.

5 Internet of Crowds (IoC)

The social networks of the communicating users and information on their characteristics can be a powerful aid for any network operation. The social services have to be provided in a decentralized fashion at the same time, since a reliable end-to-end connectivity can not be expected. Centralized services additionally represent a single point of failure and a possible threat to the privacy of users [12].

The initial challenge in the field is to implement a decentralized online social network providing both availability and a minimum level of privacy. Keeping all needed services and applications that are implemented inside the social networking services available is a difficult challenge. Especially considering the fact that parts of the network may temporarily be disconnected demands solutions for the migration and load balancing of services and applications in an unmanaged environment, using concepts of self-organization and distributed control.

Safebook [13] currently tackles the challenge of implementing online social networks without centralized control, among only four predominant projects [13–16]. However, none of the approaches proposed so far provides for the distributed execution of applications and added services. The question of how such services would have to be distributed, migrated, kept alive for each subnetwork with a temporary lack of connectivity to the rest of the system, and load-balancing between the participating nodes in a disconnected partition additionally remains completely unreflected upon.

Online social network technologies can also provide numerous benefits for Teams Under Pressure. However, this application field poses additional challenges. First Responders, especially in the case of large scale disasters tend to avoid both, novel communication technology and software systems and still prefer their traditional workflow including the use of pen and paper. We identified three main challenges which need to be addressed in order to improve the quality and speed of the decision-making process in large scale catastrophes and improve the acceptance of new technologies in this domain:

(i) *Novel and non-disruptive interaction strategies:* Although there is a variety of software specialized on nearly all important tasks of disaster relief, pen and paper is not yet replaced and is unlikely to disappear in the next couple of years. The challenge is to support teams under pressure with novel IT interaction mechanisms and aggregated sensor information without forcing them to abandon their traditional workflows.

(ii) *Integration of sensors, communication devices and decision support systems:* Commercially available closed solutions do not support incidents of organizationwide or nationwide scale. This requires a clean and smart interface between different categories of data sources and sinks, each one from different vendors and in different levels of sophistication. In particular, sources and sinks must be able to interact and dynamically adapt in terms of prioritization, scaling and QoS. Due to fast changes in information needs and in network quality, adaptation must be possible at much higher rates than with common approaches.

(iii) *Break the glass security:* Imagine a large scale chemical disaster where perilous gas is about to enter the environment. It is good practice to give the first responders an emergency authorization, which allows them, e.g., to enter every office/laboratory, destroy valuable assets, or flood a floor if necessary. Hence, under certain circumstances, it is possible to overrule all security restrictions. Since more and more systems are based on IT, the demand for an electronic equivalent of an *emergency hammer* rises from day to day.

6 Internet of Clouds

Two driving forces suggest Internet-based Cloud Computing as a foundation for the Future Internet: i) resource-poor IoT devices must be "surrounded" by data and processing capabilities of vastly varying amount and origin, often 'owned' by other parties than those (currently) hosting an IoT entity and ii) global and highly unpredictable demand for IoS services cannot be reliably and cost-effectively met by an IoS provider, particularly by a 'new economy' provider.

While the Internet of Clouds will leverage off its "predecessors" Concurrent and Distributed Computing and Grid Computing for much of its structural components, standards, and engineering concepts, we strongly believe that it will inherit from Peer-to-Peer computing with respect to highly scalable basic mechanisms and from Ubiquitous Computing with respect to Privacy, Security, and Trust (PST).

PST can be seen as a key challenge of the Future Internet, orthogonal to all the ingredients discussed up to now. Thereby, the Internet-of-Clouds is to be considered the final deathblow for long-established foundations of IT security: enterprise firewalls become questionable in view of interleaving enterprises, and classical security means (PKIs, certificates, End-to-End security concepts etc.) are of limited use in view of 'other Ends' in End-to-End communication is a priori not trustworthy. These trends arose with the first four Future Internet components discussed, but now with the Internet-of-Clouds even the entire computing and communication foundation becomes unreliable from a PST point of view. In the remainder, we will select a few of the related issues for more detailed discussion, starting with security due to its long standing history in classical IT (compared to trust and privacy).

Security in the Future Internet is clearly beyond confidentiality, integrity, and authentication, but (e.g.) also on the reliable enforcement of the interest of users and service providers. This should lead to an extended research on security policies and remote policy enforcement - especially considering distributed environments. In order to reason about and proof the enforcement of policies, security automata are a promising concept. Major research challenges in the areas of *secure data, things, and services* are in the focus of researchers working at CASED (Center for Advanced Security Research Darmstadt).

Trust concepts become even more vital when systems become more decentralized. With an increasing number of service providers the customer has the choice to select her preferred service provider out of many. However, especially a first time customer has little information about the quality of service that those providers offer as traditional hints, as they are known from the real world, are missing. Here, the concepts of trust and reputation have been shown to be excellent concepts in order to support the customers as well as the service providers.

In previous and on-going work, we are developing innovative concepts which are the basis for integrating reputation and trust information in (semi-)automatic decision making processes. Thus, we recently developed a novel representation for Bayesian trust models that can be adjusted to the characteristics of different application contexts and that can easily be integrated in graphical user interfaces [17]. Furthermore, we provide a new approach to limit the impact of Sybil attacks [18], i.e., an attacker tries to increase the influence of her ratings being represented by a high number of seemly independent entities.

Informational Privacy is related to the person's right to determine when, how and to what extent information about him or her is communicated to others. The upcoming of the future Internet has a deep implication on how personal data is collected, handled and eventually used. In Ubicomp environments, many seemingly invisible devices capture information about users to identify their demands and to personalize services. Nevertheless, service providers operating within the EU need to comply with the regulatory obligations of the *EC Privacy and Electronic Communications Directive 2002/58/EC* and the *EC Data Protection Directive 1995/46/EC* if personally identifiable data is processed. It is thus fundamental to identify the privacy threats in the emerging Internet and design suitable privacy-enhancing technologies [19, 20]. Furthermore, it is necessary to analyze if the digital identifiers and identity management systems used nowadays are sufficient.

7 Conclusion

Due to the limited space available, the paper could only 'open the door' to each of the 'Future Internet variants', to relevant research topics, and to interesting relationships between these variants.

In summary, the most substantial insight gained by the authors over recent years is the fact that despite the broad spectrum of applications and challenges that characterize the five 'Future Internet variants', three core research areas turn out to be the 'persistent backbone' of Future Internet research (for what was called the 'camp two viewpoint' of the Future Internet):

1. Distributed Computing Mechanisms, Platforms, and Devlopment Aids
2. Human-Computer-Interaction, and
3. PST (Privacy, Security, and Trust).

Notably, these three areas were formerly rather separate. While the first and third became related since several decades, it is only recently the HCI - with the Future-Internet relevant topics mentioned - started to 'team up' with the other two fields. This observations leads us towards a strong quest for interdisciplinary research in the three fields mentioned - and (in the light of the Internet-of-Humans and -Crowds) towards a quest for interdisciplinary research beyond Computer Science, i.e. with both Humanities and Economics.

References

1. Aitenbichler, E., Kangasharju, J., Mühlhäuser, M.: MundoCore: A Light-weight Infrastructure for Pervasive Computing. PMC **3**(4) (2007) 332–361
2. Aitenbichler, E., Lyardet, F., Austaller, G., Kangasharju, J., Mühlhäuser, M.: Engineering Intuitive and Self-Explanatory Smart Products. In: Proc. of the 22nd ACM Symposium on Applied Computing (SAC), ACM Press (2007) 1632–1637
3. The SmartProducts Consortium: Proactive Knowledge for Smart Products. http://www.smartproducts-project.eu/ (2009) last visited: 11.11.2009.
4. Theseus Pressebüro: Theseus Programme. http://theseus-programm.de/ (2009) last visited: 11.11.2009.
5. Schmidt, W., Fleischmann, A., Gilbert, O.: Subjektorientiertes Geschäftsprozessmanagement. HMD - Praxis der Wirtschaftsinformatik (266) (April 2009)
6. Behring, A., Petter, A., Mühlhäuser, M.: Rapidly modifying multiple user interfaces of one application. In: ICSOFT 2009, INSTICC Press (Jul 2009) 344–347
7. Petter, A., Behring, A., Mühlhäuser, M.: Constraint Solving in Model Transformations. In Paige, R.F., ed.: ICMT, Springer (2009)
8. Schnelle, D.: Context Aware Voice User Interfaces for Workflow Support. VDM Verlag Dr. Müller (2008)
9. Mühlhäuser, M., Gurevych, I.: Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises. IGI Information Science Reference (2008)
10. Sellen, A.J., Harper, R.H.: The Myth of the Paperless Office. MIT Press, Cambridge, MA, USA (2003)
11. Steimle, J., Brdiczka, O., Mühlhäuser, M.: CoScribe: Integrating Paper and Digital Documents for Collaborative Learning. IEEE Transactions on Learning Technologies **2**(3) (2009) 174–188
12. Cutillo, L.A., Molva, R., Strufe, T.: Safebook: a Privacy Preserving Online Social Network Leveraging on Real-Life Trust. IEEE Comm. Magazine (December 2009)
13. Cutillo, L.A., Molva, R., Strufe, T.: Safebook: Feasibility of Transitive Cooperation for Privacy on a Decentralized Social Network. In: WoWMoM. (2009)
14. Baden, R., Bender, A., Starin, D., Spring, N., Bhattacharjee, B.: Persona: An online social network with user-defined privacy. In: ACM SIGCOMM. (2009)
15. Buchegger, S., Schiöberg, D., Vu, L.H., Datta, A.: PeerSoN: P2P Social Networking. In: Social Network Systems. (2009)
16. Graffi, K., Mukherjee, P., Menges, B., Hartung, D., Kovacevic, A., Steinmetz, R.: Practical Security in P2P-based Social Networks. In: LCN. (2009)
17. Ries, S.: Extending Bayesian Trust Models Regarding Context-Dependence and User Friendly Representation. In: Proc. of the 24th ACM SAC. (2009)
18. Ries, S., Aitenbichler, E.: Limiting Sybil Attacks on Bayesian Trust Models in Open SOA Environments. In: Proc. of CPI-09. (2009)
19. Martucci, L.A., Andersson, C., Fischer-Hübner, S.: Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks. In: Proc. of IWSEC, Information Processing Society of Japan (IPSJ) (2006) 123–134
20. Martucci, L.A., Kohlweiss, M., Andersson, C., Panchenko, A.: Self-Certified Sybil-Free Pseudonyms. In: Proc. of WiSec'08, ACM Press (2008) 154–159