Öffentliche Sicherheit: IKT-Unterstützung für hochkritische Aufgaben in Großschadenslagen

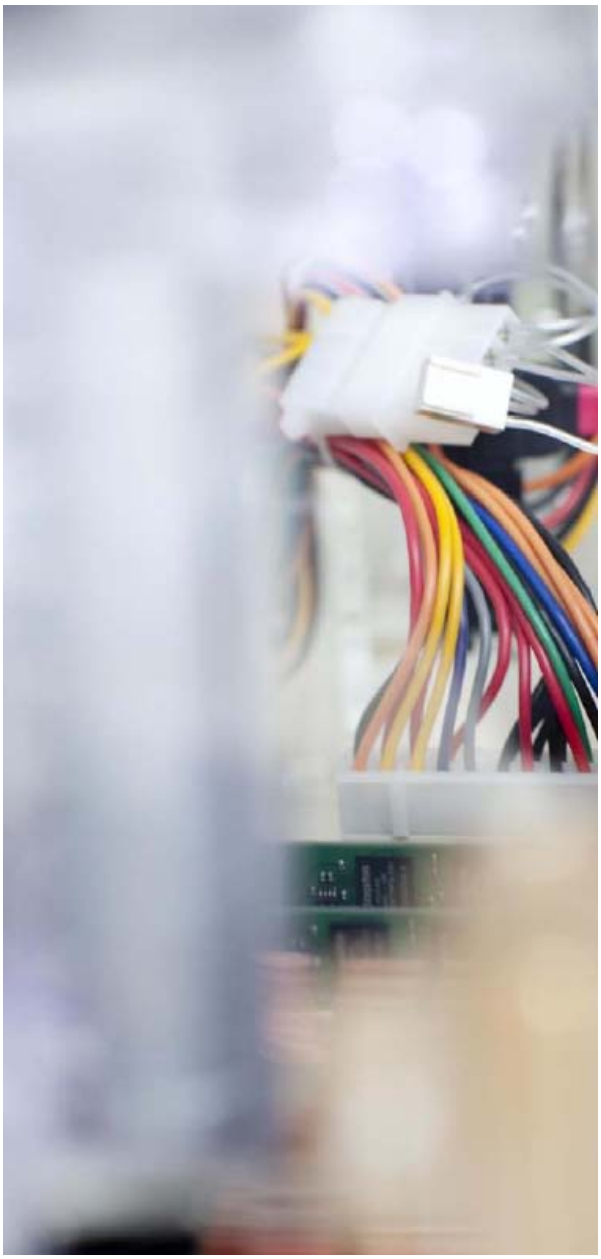
Prof. Dr. Max Mühlhäuser, Dr. Dirk Bradler, Dr. Melanie Hartmann
Technische Universität Darmstadt, Deutschland
Email: {max, bradler, melanie}@tk.informatik.tu-darmstadt.de

Kurzfassung

Bei einer Großschadenslage, wie z.B. einem Chemieunfall oder einem Großbrand, werden extreme Anforderungen an die Belastbarkeit der menschlichen Einsatzkräfte, an die Schnittstelle zwischen Mensch und Technik sowie an die Technik selbst gestellt. Notwendige Absprachen der Rettungskräfte sind aufgrund der von Stress geprägten Situation besonders fehleranfällig, dabei nicht selten überlebenskritisch, sie kosten wertvolle Zeit und lenken viel Aufmerksamkeit von der eigentlichen Aufgabe ab. Informations- und Kommunikationstechnik (IKT) für die Öffentliche Sicherheit kann auf verschiedene Weise helfen, diese Probleme zu reduzieren. Der folgende Beitrag gibt einen kurzen Überblick über entsprechende IKT-Einsatzfelder und bespricht zwei davon genauer.

Abstract

Major incidents, e.g., a chemistry accident or a major fire stipulate extreme requirements for the human ability to work under pressure, for the interface between humans and technology, and for the technology itself. Since emergency forces act under stress, interactions are particularly error-prone – albeit often survival critical; they consume precious time and distract attention from the actual task. A spectrum of approaches to ICT-support for public security can be applied to reduce these problems. The article provides a short overview to corresponding ICT areas and discusses two of them in more detail.



1 Einleitung

Öffentliche Sicherheit (auch: Zivile Sicherheit) bezeichnet – vereinfacht gesagt – alle Maßnahmen, die das öffentliche Leben vor erheblichen Störungen schützen. Ganz grob können zwei Maßnahmenbereiche unterschieden werden:

- Prävention d.h. Verhinderung von Störungen bzw. Vorbereitung darauf: hierunter fallen i) physischer Schutz (Brandlösch-Anlagen, Zugangskontrollen, …) ii) Planung (Katastrophenübungen, Rettungspläne, …), iii) Regulierung (Sicherheitsstandards und –vorschriften inkl. deren Durchsetzung) sowie iv) präventive Abwehr und Prüfung (z.B. Anschlagsvereitelung, Gebäude-Standsicherheitsprüfung, …),
- Reaktion d.h. Wiederherstellung des „Normalzustandes“ nach Unfällen und Katastrophen, welche durch Natur, Technik oder Menschen (fahrlässig oder mutwillig) verursacht werden: hierbei sind i) Koordination (in Stäben, Leitstellen, Zentralen …) und ii) Operation (Einsatz privater und staatlicher Rettungskräfte im Feld) zu unterscheiden;

ISBN 978-3-8007-3304-0

In allen genannten Bereichen der Öffentlichen Sicherheit nimmt die Unterstützung durch IKT, d.h. Informations- und Kommunikationstechnik zu:

1. Prävention: hier sind die verwendeten IKT-Konzepte sehr divergent: beim physischen Schutz kommt bspw. biometrischer Zugangskontrolle wachsende Bedeutung zu, in der Planung sind Rechnersimulationen unerlässlich, bei der Anschlagsvereitelung wird die Früherkennung krimineller Internet-Aktivitäten immer wichtiger (‚Dark Web Mining') usw.
2. Reaktion: dieser Bereich lässt sich – systematischer als die Prävention – in zwei Schwerpunkte gliedern:
   a. Koordinationsunterstützung in Zentralen: hier wird u.a. die Mensch-Technik- und Mensch-Mensch-Interaktion in Stabs- und Leitstellen verbessert durch multimodale Bedienkonzepte, interaktive Großdisplays, Entscheidungsunterstützungs-Software usw.
   b. Operative Unterstützung im Feld: ein wichtiges Forschungsfeld ist hier bspw. die Ersthelfer-Ausstattung mit Sensorik und digitaler Kommunikation sowie maßgeschneiderter Lagedarstellung;

   Neben dieser Zweiteilung sind zwei Teilbereiche innerhalb der Reaktions-Phase hervorzuheben, für welche IKT-Unterstützung besonders vielversprechend ist, weil hier an erfolgreiche IKT-Konzepte aus anderen großen Anwendungsbereichen angeknüpft werden kann (z.B. aus der Unternehmenssoftware):
   c. Prozess-Evolution: dabei werden relevante Abläufe zunächst modelliert, dabei allen Beteiligten eindeutig bewusst gemacht, und anschließend optimiert sowie (teil-) automatisiert
   d. Infrastruktur-Entwicklung: IKT-basierte Software-Infrastrukturen ersetzen und integrieren zunehmend herkömmliche, starre und voneinander isolierte Systeme, bspw. zur schnellen Kopplung aller für Leitstellen erforderlichen Dienste (Zugriff auf Lageinformation, Rettungskräfte und –maßnahmen, Einbeziehung Dritter wie Krankenhäuser, Hilfsgüter, Geoinformationssysteme, usw.), etwa auf Basis von Web-Services, künftig auch die Einbeziehung von IKT-Infrastrukturen für Gebäudemanagement bei Rettungsmaßnahmen, ausrollbare Gelände-Infrastrukturen u.a.

Ergänzend zum traditionellen Verständnis der Öffentlichen Sicherheit als Kombination aus Präventions- und Reaktionsmaßnahmen wird seit einiger Zeit besonderes Augenmerk auf kritische Infrastrukturen gelegt, d.h. Institutionen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Naheliegender Weise betrifft dies Verkehrs- und Energienetze bzw. –Knotenpunkte, darüber hinaus sind aber auch Kommunikation, medizinische und Nahrungsmittel-Versorgung für funktionierendes öffentliches Leben unerlässlich. Ausgangspunkt für den Schutz solcher Infrastrukturen ist i.a. das Verständnis des zu schützenden Gesamtsystems und seiner Funktionsweise, die weiter oben genannten Präventions- und Reaktionsmaßnahmen orientieren sich dann an identifizierten Schwachstellen, Risikoanalysen, Wirkzusammenhängen usw.

Auch der Schutz kritischer Infrastrukturen wird zunehmend von Fragestellungen der IKT durchzogen, allerdings ist IKT dabei aus Sicht der öffentlichen Sicherheit weniger die Lösung als das Problem:

- einerseits ist IKT zunehmend das ‚Nervensystem' kritischer Infrastrukturen; Ausfall, Störung oder Missbrauch dieses Nervensystems bedroht damit immer stärker diese Infrastrukturen als Ganzes
- andererseits ist das „Internet" als solches – auch jenseits seiner Funktion als Nervensystem anderer kritischer Infrastrukturen – zunehmend für das Öffentliche Leben so entscheidend, dass sein Schutz – bezeichnet als Cybersecurity – ins Zentrum des Interesses rückt; diese Problematik verschärft sich, weil das Internet zunehmend der ‚Marktplatz' des globalen Wirtschaftsgeschehens wird

Der Schutz kritischer Infrastrukturen ist mithin derjenige Bereich, bei dem sich Öffentliche Sicherheit und IT-Sicherheit ganz stark überlappen, denn IT-Sicherheit in diesem Bereich wirkt unmittelbar als Maßnahme der Öffentlichen Sicherheit. Dieses Thema soll aber im vorliegenden Artikel nicht vertieft werden. Stattdessen wird die weiter oben beschriebene Sichtweise beibehalten, wobei vor allem IKT-Unterstützung für die Reaktions-Phase innerhalb der Öffentlichen Sicherheit im Zentrum steht.

Dabei wollen wir aufzeigen, dass IKT-Unterstützung – und damit Technik – nicht losgelöst vom Menschen entwickelt werden kann, ja dass selbst die Einbeziehung der Mensch-Maschine-Schnittstelle noch nicht ausreichend ist für wirksame Konzepte. Stattdessen müssen die drei Bereiche Mensch, Interaktions-Schnittstelle und Technik im Zusammenhang mit Fragestellungen der Öffentlichen Sicherheit jeweils gezielt untersucht werden und entwickelte Konzepte müssen in allen drei Bereichen aufeinander abgestimmt werden.

In den folgenden zwei Kapiteln werden die zwei Bereiche Interaktion und Technik nicht nur beschränkt auf die Reaktions-Phase behandelt, sondern es werden zusätzlich spezielle Themenstellungen herausgegriffen, weil eine vertiefte Behandlung aller in dieser Einleitung genannten Aspekte der IKT-Unterstützung Öffentlicher Sicherheit den Rahmen völlig sprengen würde. Die Autoren versuchen, durch diese beispielhafte Behandlung stellvertreten-

ISBN 978-3-8007-3304-0

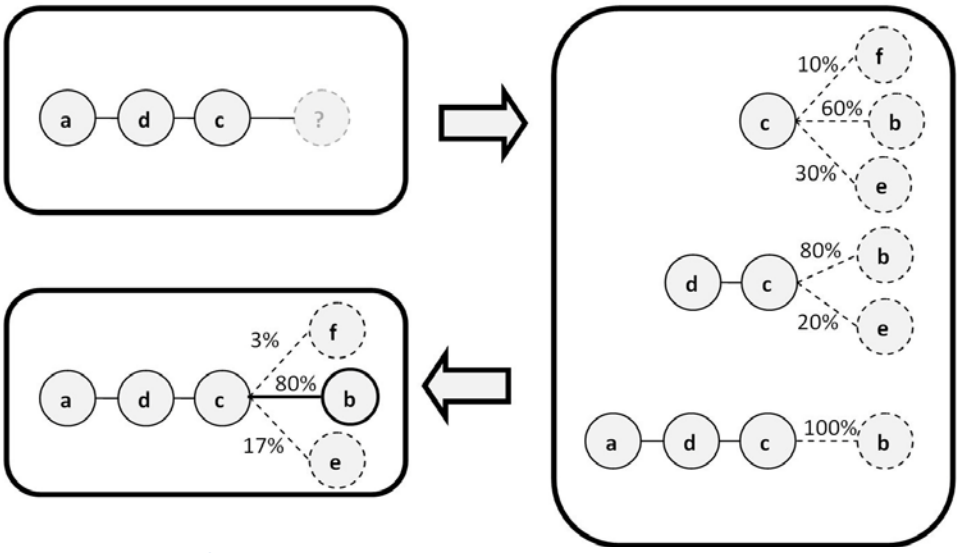


Abbildung 1- Vereinfachtes Mixed order Markov Model unter Verwendung von Markov Modellen erster bis dritter Ordnung und gleichen Gewichtungen

der Themen dennoch einen möglichst breiten Überblick über das Themenfeld zu geben. Konkret werden in den kommenden Kapiteln folgende Problembereiche behandelt:

- Kapitel zwei betrifft den Bereich „Interaktion“, ebenfalls schwerpunktmäßig für Zentralen; hier wird vertieft die Frage untersucht, wie Interaktionskonzepte mit „Proaktivität“ versehen werden können im Sinne einer Vorausschau auf kommende Ziele und Aktionen des Nutzers
- Kapitel drei behandelt den Bereich „Technik“ und konzentriert sich im Gegensatz zu den vorangegangenen auf die operative Unterstützung im Feld; mit neuesten Ansätzen zu höchst dezentralisierten so genannten Peer-to-Peer-Netzwerken wird hier effiziente und besonders schnell anpassbare Vernetzung unterstützt, die mit dem Eintreffen von Rettungskräften im Feld „mitwächst“.

2 Intelligente Interaktionsunterstützung

Das Ziel intelligenter Interaktionsunterstützung ist Fehlhandlungen in Stresssituationen zu minimieren, dem gefühlten Kontrollverlust entgegenzuwirken und den Stress der Einsatzkräfte durch die Erstellung strukturierter und intuitiver Benutzerschnittstellen zu reduzieren. In diesem Abschnitt werden wir uns auf proaktive Benutzerschnittstellen konzentrieren, d.h. auf Benutzerschnittstellen, die dem Benutzer Vorschläge zur Interaktion machen und nicht nur auf Benutzereingaben reagieren.
Die proaktive Unterstützung kann die Interaktion für Einsatzkräfte in der Zentrale wie auch im Feld vereinfachen. Im Folgenden wollen wir uns konzentrieren, wie er im Rahmen des Projekts AUGUR an der TU Darmstadt entwickelt wurde.

AUGUR ist zum einen in der Lage den Benutzer bei der Eingabe von Daten zu entlasten indem es dem Benutzer Vorschläge zur Eingabe unterbreitet (sieheAbbildung 2) oder direkt Eingabefelder für den Benutzer vorausfüllt [7]. Dadurch werden Fehleingaben reduziert und Daten können schneller übermittelt werden. Für das Vorschlagen von Eingabedaten werden eine Reihe von vorliegenden Kontextinformationen -wie z.B. der Aufenthaltsort oder anwesende Personen- herangezogen. Die Zusammenhänge zwischen Kontextinformationen und benötigten Eingabedaten können entweder vormodelliert sein [9] oder von AUGUR durch Beobachtung der Benutzerinteraktion mit der Zeit erlernt werden. Zudem kann AUGUR aus der Benutzung erlernen, welche Elemente einer Benutzeroberfläche in einem bestimmten Kontext relevant sind.

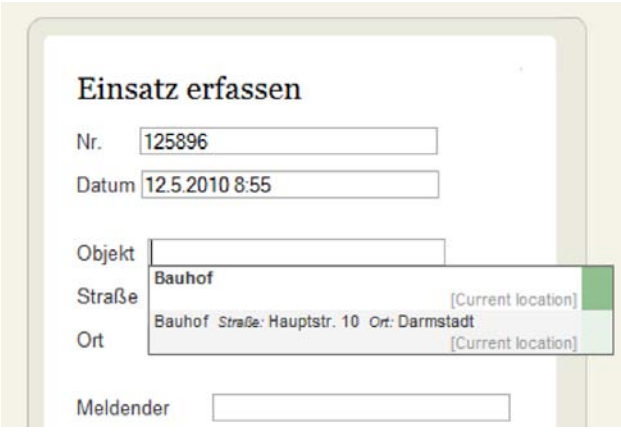


Abbildung 2 - Proaktive Eingabeunterstützung in AUGUR

ISBN 978-3-8007-3304-0

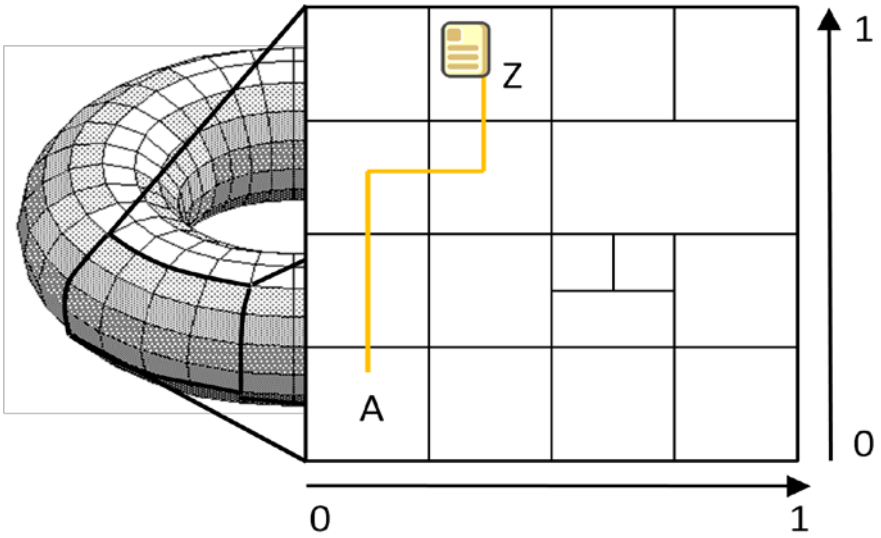


Abbildung 3- Ausschnitt des Schlüsselraumes einer verteilten Hashtabelle

Um die Benutzerschnittstelle auf die relevantesten Elemente reduzieren zu können, muss das System in der Lage sein, die nächsten Schritte des Benutzers vorherzusagen. Dazu wird aus den vergangenen Interaktionen des Benutzers ein Interaktionsmodel gelernt [8]. Mit Hilfe dieses Interaktionsmodels wird aus den letzten Aktionen des Benutzers $a_1 \ldots a_i$ (im Beispiel in Abbildung 1 die Aktionen a d c) die Wahrscheinlichkeit der nächsten Aktion a_{i+1} vorhergesagt. Dies kann z.B. mit Hilfe von Mixed-order Markovmodellen erfolgen. Diese berechnen die nächste Aktion unter Berücksichtigung von unterschiedlich vielen vorangegangenen Aktionen (im Beispiel in Abbildung 1 die letzten eins bis drei Aktionen).

Dies versetzt AUGUR in die Lage, automatisch eine reduzierte Benutzeroberfläche mit den wichtigsten Elementen zu generieren [6]. Zum einen vereinfacht dies die Interaktion auf mobilen Endgeräten und zum anderen kann es die kognitive Last des Benutzers weiter reduzieren, was in Stresssituationen wie Großschadenslagen entscheidend ist.

3 Selbstorganisierende Infrastruktur

Informationen während einer Großschadenslage müssen (i) zum gewünschten Zeitpunkt, (ii) an der verantwortlichen Stelle und (iii) in der benötigten Granularität vorliegen. Während in der Einsatzleitzentrale hauptsächlich Informationen geordnet, priorisiert und aggregiert werden und somit als Entscheidungshilfe dienen, müssen Rettungskräfte vor Ort primär Zugriff auf ihre aktuellen Aufgabenstellungen, Ressourcen und Bereichsleiter Zugriff haben[5]. Im Folgenden wird beispielhaft der Zugriff auf Informationen über das Objekt „Bauhof“ (vgl. Abbildung 2) durch ein verteiltes Netzwerk, welches ad-hoc während des Einsatzes erstellt wird im Detail betrachtet.

Die beteiligten Endgeräte im Feld (z.B. innerhalb eines Fahrzeugs, in der technischen Einsatzleitung oder tragbar in Form eines PDAs) sind Teil des P2P-Netzes und können für Informationsweiterleitung (Routing), Abfragen und zur Datenspeicherung verwendet werden. Diese Kombination der Verwendungsmöglichkeiten ist als Servent-Konzept (Kunstwort entstanden aus der Kombination der Wörter Server und Client) aus der P2P-Technologie bekannt. Nachdem das Endgerät eine Aktion des Benutzers entgegengenommen hat, z.B. durch Selektion des Objekts „Bauhof“, wird eine Route innerhalb des Netzwerkes zu dem Endgerät der dafür zuständigen Einsatzkraft gesucht. Das an der TU Darmstadt entwickelte P2P-Verfahren zur dezentralen Datenübertragung [3] tauscht zunächst nur Routingtabellen und Basisinformationen mit anderen Geräten in Reichweite aus. In einem zweiten Schritt wird das Gerät vollständig in das Netz integriert. Die Endgeräte nutzen das dezentrale und autonom arbeitende Netzwerk um Informationen zu finden oder zu veröffentlichen [2] (vgl. Abbildung 3).

Soll z.B. das Objekt „Bauhof“ aufgerufen werden, dann wird ein Pfad von dem anfragenden Endgerät zum Zielort innerhalb des P2P-Netzes gesucht. Um den gesuchten Zielort zu bestimmen nimmt eine Funktion (z.B. die Hashfunktion SHA-1) das Schlüsselwort „Bauhof“ entgegen und generiert eine eindeutige Adresse innerhalb des Netzwerks, diese dient als wichtigster Anhaltspunkt für die Nachrichtenweiterleitung (vgl. Abbildung 3). Dieses Konzept ist als Distributed Hash-Table bekannt und in unterschiedlichen Varianten untersucht worden [1][4]. Ist die Nachricht nach mehreren Übermittlungsschritten beim Empfänger angekommen, überprüft dieser ob bereits Informationen über das gesuchte Objekt vorliegen und informiert den Absender. Diese nichtprobabilistische Zugriffsmethode und die dynamische Erstellung eines dezentralisierten Kommunikationsnetzwerkes erhöht die Planungssicherheit der Ersthelfer und wirkt dadurch zusätzlich stressmindernd auf die Rettungskräfte.

ISBN 978-3-8007-3304-0

4 Zusammenfassung und Kontext

Gerade bei Großschadenslagen muss die IKT Unterstützung als ganzheitlicher Prozess verstanden werden, der sowohl den Menschen, die Interaktions-Schnittstelle als auch die zugrunde liegende Technik berücksichtigt. An der TU Darmstadt gelang durch die konsequente interdisziplinäre Zusammenarbeit der beteiligten Institute im vielschichtigen Bereich der Öffentlichen Sicherheit eine ganzheitliche Analyse der Problemstellung und die Entwicklung eines integrierten Lösungskonzepts mit besonderem Fokus auf die Reaktions-Phase. Im vorstehenden Artikel wurden zwei Bereiche herausgegriffen, die am Fachgebiet Telekooperation behandelt werden. Der Interessenverbund Öffentliche Sicherheit der TU Darmstadt umfasst aber eine Reihe weiterer Forschungsaktivitäten, die interdisziplinär koordiniert werden. Beispielhaft seien Arbeiten am Institut für Arbeitswissenschaft genannt: dort werden die Auswirkungen von Stresssituationen auf den Menschen analysiert; hieraus ergaben sich besonders hohe Anforderungen an die benötigten Interaktions-Schnittstellen. Hieran knüpft das Fachgebiet Telekooperation mit den im Beitrag beschriebenen kontextsensitiven und lernenden Benutzerschnittstellen unmittelbar an. Sie versprechen gerade in Extremsituationen eine Entlastung der Ersthelfer und verringern die Wahrscheinlichkeit von Fehleingaben. Hieran wiederum schließen sich die im Beitrag beschriebenen, auf P2P-Technologie fußenden Konzepte für die spontane Erstellung hochdynamischer Netzwerke am Ort der Großschadenslage an. Für Informationen über weitere Arbeiten, die im Darmstädter Interessensverbund an der Universität und weiteren (z.T. Industrie-) Forschungseinrichtungen durchgeführt werden, gibt der Zeitautor des Beitrags bei Bedarf gerne Auskunft.

5 Literatur

[1] Ratnasamy, S., Francis, P., Handley, M., Karp, R., and Shenker, S. 2001. A scalable content-addressable network. In Proc. of Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications. SIGCOMM '01. ACM, New York

[2] Bradler, D., Kangasharju, J., and Mühlhäuser, M. 2009. Optimally efficient multicast in structured peer-to-peer networks. In Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference (Las Vegas, NV, USA, January 11 - 13, 2009). IEEE Press, Piscataway, NJ, 123-127.

[3] Bradler, D., Krumov, L., Wagner, M., and Kangasharju, J. 2009. Hierarchical data access in structured P2P-networks. In Proceedings of the 2009 Spring Simulation Multiconference, San Diego, CA, 1-7.

[4] Stoica, I., Morris, R., Karger, D., Kaashoek, M. F., and Balakrishnan, H. 2001. Chord: A scalable peer-to-peer lookup service for internet applications. SIGCOMM Comput. Commun. Rev. 31, 4, 149-160.

[5] Huang, Y. and He, W. and Nahrstedt, K. and Lee, W.C.,2007, Requirements and system architecture design-consideration for first responder systems, IEEE Conference on Technologies for Homeland Security, pp. 39-44

[6] Hartmann, M. and Schreiber, D. 2010, AUGUR: Interface Adaptation for Small Screen Devices. In Advances in Ubiquitous User Modelling, p. 94-110, Springer, ISSN 0302-9743.

[7] Hartmann, H. and Schreiber, D. 2009, AUGUR: Providing Context-Aware Interaction Support. In Proceedings of Engineering Interactive Computing Systems (EICS'09), p. 123-131. ISBN 978-1-60558-600-7.

[8] Hartmann, M. and Schreiber, D. 2007. Prediction Algorithms for User Actions. In: Proceedings of Lernen Wissen Adaption, ABIS 2007, p. 349--35.

[9] Hartmann, M., Schreiber, D. and Kaiser, M. 2007. Task Models for Proactive Web Applications In: Proceedings of WEBIST 2007, INSTICC Press.

Prof. Dr. Max Mühlhäuser leitet seit 2000 das Fachgebiet Telekooperation an der TU-Darmstadt. Seit 2008 ist er Leiter des Arbeitsbereichs „Sichere Dienste“ des Forschungszentrums CASED.

Dr. Dirk Bradler ist Leiter der Gruppe Smart Civil Security am Fachgebiet Telekooperation an der TU-Darmstadt. Er hat 2010 seine Promotion zum Thema „P2P Concepts for Emergency Response“ abgeschlossen.

Dr. Melanie Hartmann ist Leiterin der Gruppe Smart Interaction am Fachgebiet Telekooperation. Sie hat 2010 ihre Promotion zum Thema „Context-Aware Intelligent User Interfaces abgeschlossen“.

ISBN 978-3-8007-3304-0