Telematik
Technische Informatik

DBIS

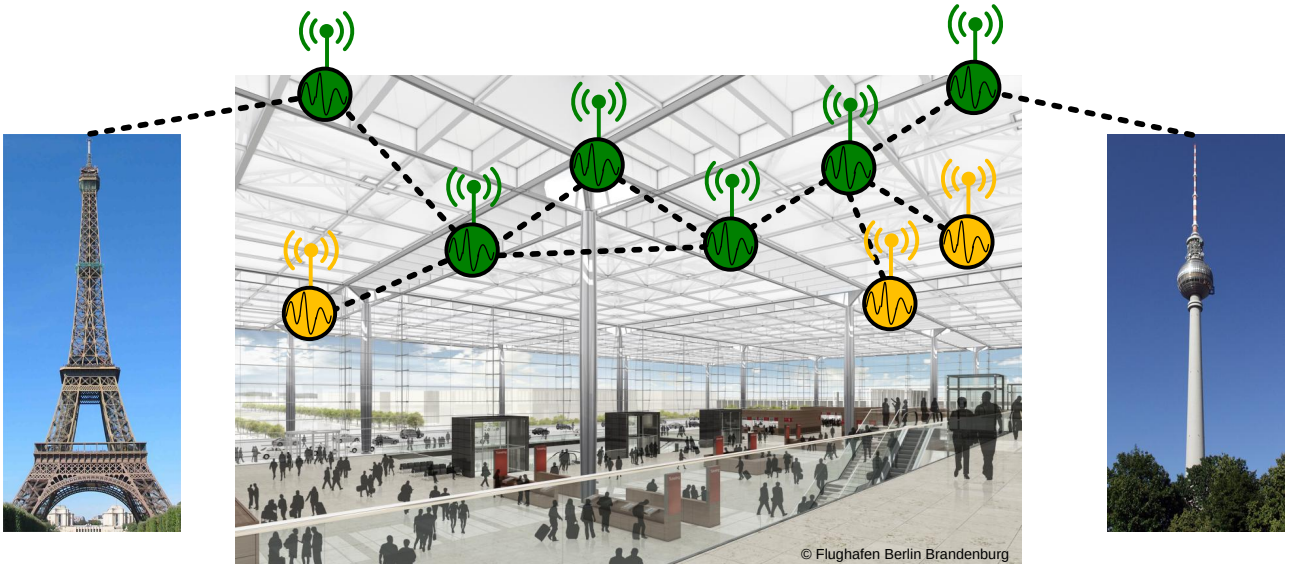
Forschungsforum
Öffentliche Sicherheit

Freie Universität Berlin

Abschlussbericht zur BMBF-Fördermaßnahme: Kooperation in der zivilen Sicherheitsforschung zwischen Deutschland und Frankreich

SAFEST – Social-Area Framework for Early Security Triggers at Airports

Teilprojekt: Sensorik und Wissensfusion zum Schutz von Verkehrsinfrastrukturen unter gesellschaftlichen Randbedingungen (Förderkennzeichen: 13N12235)



Berichtszeitraum: 1. Mai 2012 bis 30. September 2015

Prof. Dr.-Ing. Jochen Schiller
Freie Universität Berlin, Institut für Informatik
Takustr. 9, 14195 Berlin
Tel.: +49 30 838 75 213
eMail: jochen.schiller@fu-berlin.de

Inhaltsverzeichnis

1 Kurzdarstellung

1.1 Aufgabenstellung

Das übergeordnete Ziel des Projekts SAFEST liegt in der gesellschaftswissenschaftlich–technisch abgestimmten Gestaltung und der experimentellen Verifikation eines umfassenden Gefahrenerkennungs- und Krisenmanagementsystems für die Sicherheit in stark frequentierten öffentlichen Bereichen kritischer Verkehrsinfrastrukturen. SAFEST adressiert das Problem der Flächenüberwachung unter Einschluss von Einbruchserkennung und der Abwehr von Massenpaniken, indem es in seinem interdisziplinären Ansatz ein akzeptanzorientiertes verteiltes System für die Beobachtung öffentlicher Plätze und ein Frühwarn-Leitsystem für den Gefahrenfall entwickelt.

Das Teilvorhaben „Sensorik und Wissensfusion zum Schutz von Verkehrsinfrastrukturen unter gesellschaftlichen Randbedingungen“ hat zum Ziel, durch intelligente, verteilte Sensoren Gefahren am Flughafen rechtzeitig zu erkennen, diese mittels Wissensfusionierung auszuwerten und Passagiere in Kombination mit einem leichtgewichtigen Leitsystem zu schützen. Infrarotvideokameras sollen Menschenaufläufe im Falle eines ungewöhnlichen Ereignisses in umliegender Nachbarschaft (z.B. Feuer, Explosion) identifizieren, wobei Massenpaniken durch das zielgerichtete Lenken der Betroffenen verhindert werden. Perimetersensoren sollen helfen, sicherheitskritische Areale des Flughafens zu überwachen und somit Sabotage und Einbruch zu verhindern. Eine soziologische Begleitstudie wird das Akzeptanzverhalten der eingesetzten technischen Lösungen innerhalb der Bevölkerung untersuchen und Handlungsempfehlungen für Entwickler und mögliche Betreiber eines solchen Krisenmanagements ableiten.

Zentrale Komponenten für die Umsetzung des Gesamtziels sind bildbasierte Erkennungsverfahren zur Identifizierung von Menschenansammlungen sowie leitsystem-gesteuerte Alarmverfahren für die geordnete Auflösung gefährlicher Massensituationen. Schützenswerte Außenbereiche des Flughafens sollen mittels Perimetersensoren (Beschleunigungs-/Bewegungssensoren etc.) abgesichert werden.

1.2 Voraussetzung für das Vorhaben

Öffentliche Räume wie Flughäfen, Bahnhöfe oder Stadien bringen eine große Zahl von Menschen auf beschränktem Raum zusammen, welche häufig sicherheitskritische Infrastrukturen nutzen. Solche Plätze fordern die öffentliche Sicherheit in zwei Weisen heraus: (a) die Verhinderung von Massenpaniken im Fall bedrohlicher Ereignisse und (b) die Erkennung des Zutritts zu unerlaubten Bereichen. Intelligente und flexible sensorgestützte Systeme können helfen, diese Risiken rechtzeitig zu identifizieren und Menschen vor weiteren Gefahren zu bewahren. Der Einsatz dieser Technologien erzeugt aber in der Bevölkerung typischerweise Vorbehalte, da sie eine Beeinträchtigung ihrer Privatsphäre fürchten.

Die erfolgreiche Umsetzung ziviler Sicherheit ist an soziologische und technologische Randbedingungen gebunden. Überwachungssysteme sind einerseits negativ konnotiert, da sie die Bevölkerung einer schwer einschätzbaren externen Beobachtung aussetzen, deren Nutzen oft verborgen bleibt. Andererseits sind funkbasierte Komponenten, wie sie für einen flexiblen Einsatz benötigt werden, physikalischen Störungen ausgesetzt, welche in öffentlichen Räumen mit einer hohen Menschendichte verstärkt werden. Maßnahmen zur Erhöhung der zivilen Sicherheit müssen demnach beide Aspekte berücksichtigen. Diesen Ansatz verfolgt SAFEST, indem es ein robustes Frühwarnsystem mit autonom operierender Sensorik entwickelt, das die Bevölkerung in der Gefahreneinschätzung einbindet und in der Abwehr direkt unterstützt. Die intelligente Sensorarchitektur und das konzipierte Alarmsystem werden technische Hilfsmittel bereitstellen, um kritische Verkehrsinfrastrukturen sicherer zu betreiben.

Es wurde eine Patentrecherche vor dem Projektstart durchgeführt. In dem vorliegenden Verbundvorhaben werden keine eigenen oder Schutzrechte Dritter verletzt. Die zu entwerfenden Algorithmen unterliegen keinen Patentstreitigkeiten. Die Ergebnisse der sozialwissenschaftlichen Studie berühren keine Patente.

1.3 Planung und Verlauf des Vorhabens

Die Freie Universität Berlin wird sich mit drei Arbeitsgruppen an dem Projekt SAFEST beteiligen: AG Technische Informatik und Telematik, AG Datenbanken und Informationssysteme und dem Forschungsforum Öffentliche Sicherheit (FÖS).

Das Projekt SAFEST gliedert sich in acht Arbeitspakete. Die Arbeitspakete wurden kooperativ, aber in klarer Verantwortungsverteilung mit den beteiligten Projektpartnern durchgeführt. Die acht Arbeitspakete (AP) sind thematisch wie folgt organisiert:

AP 1: Vorbereitende Analysen und Arbeiten
AP 2: Einsatzspezifische Anforderungsanalyse
AP 3: Akzeptanz, Datenschutz, legale und soziale Auswirkungen
AP 4: Plattformumsetzung
AP 5: Wissensfusionierung und Alarmkomponenten, Leitsystem
AP 6: Zuverlässigkeit, Sicherheit und Selbstschutz
AP 7: Demonstrator, Einsatzerprobung und Evaluation
AP 8: Projektkoordination, -dissemination und Berichterstattung

Das Vorhaben wurde zuwendungsneutral verlängert, da es durch die verspätete Eröffnung des Demonstrator-Geländes zu Verzögerungen kam.

1.4 Wissenschaftlicher und Technischer Stand

Betriebssysteme Klassische Betriebssysteme wie Linux und Windows sind für ressourceneingeschränkte Endgeräte, wie sie in SAFEST zum Einsatz kommen sollen, ungeeignet. Um diesem Problem zu begegnen, wurden in der Verangenheit spezialisierte Betriebssysteme (z.B. Contiki oder TinyOS) von der Fachgemeinschaft entwickelt. Solche Systeme verlangen aber vom Programmierer Spezialwissen und weisen proprietäre Software-Schnittstellen auf. Damit lassen sich Sicherheitslösungen flächig nur unzureichend einsetzen und bestehende Anwendungen nur mit sehr hohem Aufwand portieren. Die Freie Universität Berlin hat in dem vorangegangenen Forschungsprojekt FeuerWhere einen Micro-Kernel entworfen. In SAFEST konnte von den Erfahrungen der Vorarbeiten profitieren. Es wurde möglich, ein sehr leichtgewichtiges und dennoch hochstehendes Betriebssystem zu entwerfen und zu implementieren, das für Sensornetze und das Internet der Dinge den gleichen Komfort wie Linux bietet.

Sensornetze Die Freie Universität Berlin kann auf langjährige Erfahrungen im Bereich der Mobilkommunikation, insbesondere der Mesh und funkbasierten Sensornetze, zurückblicken. Dies schließt sicherheitskritische Anwendungsfelder ein. In vorangegangenen Arbeiten wurden erste Schritte für die Umsetzung der Vision einer verteilten, qualitativ hochwertigen Ereigniserkennung unternommen, welche in einem ARM7-Demonstrator erheblich verbessert werden konnten.

Öffentliche Sicherheit Seit 2009 ergänzt das Forschungsforum Öffentliche Sicherheit die sozialwissenschaftliche Perspektive der Sicherheitsforschung am Lehrstuhl Technische Informatik der Freien Universität Berlin. Im Rahmen des Forums wurden Studien zum Thema Kritische Infrastrukturen (2010), Pandemien (2011) und Wahrnehmung von und Kommunikation über Risiken und Gefahren in der Bevölkerung (2010, 2011) erarbeitet, welche in der Schriftenreihe Sicherheit (www.schriftenreihe-sicherheit.de) erschienen sind. Die hierbei gewonnenen Erkenntnisse haben geholfen, eine fundierte soziologische Begleitstudie in SAFEST durchzuführen.

Verwendete Fachliteratur Für die notwendigen Recherchen im Verlauf des Projekts SAFEST wurde auf die digitalen Bibliotheken der ACM (http://dl.acm.org) und IEEE (http://ieeexplore.ieee.org) sowie einschlägige Journale und Online-Quellen zurückgegriffen. Veröffentlichungen zu aktuellen Forschungsergebnisse und Erkenntnisse konnten die Arbeitsgruppen der FU Berlin aber auch durch die Teilnahme an internationalen Konferenzen und Workshops im Zuge eigener Publikationen erhalten.

Zudem wurden im Projektverlauf ausgewählte Fachbücher insbesondere aus den Bereichen Soziologie sowie Sicherheit, Computer-Netzwerke, verteilte Systeme und eingebettete Programmierung verwendet.

1.5 Zusammenarbeit mit anderen Stellen

Das deutsche Projektkonsortium bestand aus vier Wissenschaftseinrichtungen und zwei Industriepartnern. Das französische Teilprojekt wurde von einer Wissenschaftseinrichtung und einem Unternehmen getragen. Alle Projektpartner waren einander langjährig bekannt und arbeiteten wissenschaftlich, praktisch und im persönlichen Austausch intensiv miteinander. Die Freie Universität Berlin hat mit allen Partnern intensiv zusammengearbeitet. Mit der HAW Hamburg wurden vornehmlich Sicherheitskonzepte erarbeitet; mit Fraunhofer FOKUS wurde gemeinsam an der Ereigniserkennung gearbeitet; mit der daviko GmbH wurden Lösungen für die Menschenmengenerkennung erforscht; mit SAGEM die Infrarotkamera optimiert; mit INRIA primär zum Routing Analysen durchgeführt. Der BER Flughafen bot eie Umgebung für reale Tests.

Neben den Projektpartnern wurden die Forschungsergebnisse mit Dritten diskutiert, sowohl national (z.B. Universität der Bundeswehr München) als auch international (z.B. UCLA, PARC).

2 Aufzählung der wichtigsten wissenschaftlich-technischen Ergebnisse und anderer wesentlicher Ereignisse

In den folgenden Abschnitten werden die wichtigsten Arbeiten und Ergebnisse der *Freien Universität Berlin* vorgestellt. Die Arbeiten wurden von den Arbeitsgruppen "Technische Informatik und Telematik", "Datenbanken und Informationssysteme" sowie dem "Forschugsforum Öffentliche Sicherheit" in enger Zusammenarbeit mit den weiteren Projektpartnern durchgeführt.

2.1 Erzielte wissenschaftlich-technische Ergebnisse

2.1.1 AP1 – Vorbereitung: Analyse und Aufarbeitung des aktuellen Wissenstandes

AP1.1 – Erstellung einer Internet-Präsenz und von Informationsmaterial

Es wurde eine öffentliche Projekt-Website mit einer ausführlichen Projektbeschreibung sowie Informationen zu den Partnern unter `http://safest.realmv6.org/` eingerichtet und über die Projektlaufzeit gepflegt.

AP1.2 – Auswahl einer Online-Plattform zur Kollaboration und Bereitstellung von Mailing-Listen

Für die interne Zusammenarbeit wurde das *Project Management Tracking System (trac)* sowie eine projektweite Mailingliste eingerichtet.

2.1.2 AP2 – Einsatzspezifische Anforderungsanalyse

AP2.1 – Interviews

Gegenstand des Arbeitspaketes waren Interviews mit Experten, die aus dem Umfeld von "Sicherheit in Verbindung mit Flughäfen" stammten. Bei den Interviews mit den Sicherheitsexperten standen die zu erarbeitenden Sicherheitsfragen und die der Sicherheitssensorik sowie die Wahrnehmung derer durch die Experten im Mittelpunkt. Hierzu wurden 15 leitfadengestützte Interviews mit Personen aus dem Sicherheits(um-)feld von Flughafenakteuren geführt, bei denen die Verbindung von technischen Artefakten in Verbindung mit Sicherheit im Allgemeinen und sozialer Aspekte im Flughafenkontext

adressiert wurden. Die Teilnehmer setzten sich aus folgenden Bereichen zusammen: Datenschutz, Bodendienstleistende, Feuerwehr, Sicherheitsdienste, Bau- und Facility-Management, Flughafenbetreiber, IuK. Die Interviews wurden transkribiert und mit MAXQDA ausgewertet.

AP2.2 – Szenarienkatalog

AP2.2.1 – Video- und Geländeüberwachung In diesem Arbeitsschritt wurden die Anwendungsszenarien für das Überwachungssystem identifiziert, formalisiert und katalogisiert. Hierfür wurde ein Szenarien-Template, das die Risiken und Gefahren am Flughafen im Projektkontext zusammenfasst, erstellt und an die Projektpartner verteilt. Die Vorlage enthält eine detaillierte, formale und auf die einzelnen Komponenten zerlegte Beschreibung des Überwachungssystems, der Beobachtungen und der Umgebung. Die Szenarien zur Verhinderung von Massenpaniken und Einbrüchen auf das Flughafengelände sind mit Hilfe der Vorlage zu beschreiben. Die Szenarien werden nicht nur durch die intuitiven Eigenschaften wie Zeit und Ort, sondern auch durch die genaue Angabe von Abläufen, die als erwartet und ungewöhnlich eingestuft werden, und die genaue Reaktion des Systems definiert.

AP2.2.2 – Data-Mining-Szenarien Die Szenarien für die Datenfusion wurden von Fraunhofer FOKUS basierend auf der allgemeinen Szenarienvorlage vorgeschlagen und in den Szenarienkatalog eingepflegt. Es wird zwischen Daten- und Wissenskonzepten unterschieden. Das System profitiert von der gemeinsamen Anwendung dieser Konzepte. Es sind die lokalen und die globalen Daten, das aktuelle und das gesammelte Wissen, die unerwarteten und die ungewöhnlichen Ereignisse formalisiert und beschrieben.

AP2.3 – Erweiterungen des Anwendungsbereiches

AP2.3.1 – Videoüberwachung Es wurde untersucht, wie die in Abschnitt 2.1.2 zusammengefassten Szenarien nicht nur im Flughafengebäude und Flughafengelände eingesetzt werden können. Das Crowd-Monitoring-System kann auch der Erkennung von ungewöhnlichen Situationen in Räumen dienen, wobei das gewöhnliche Verhalten der Menschen bzw. der Menschenflüsse gegeben ist (z.B. Beobachtung der Menschen in den Wartehallen aller Art, Beobachtung von den Warteschlangen an den Schaltern aller Art). Falls sich der Einsatzbereich nach draußen verlagert, muss das System hierfür allerdings erweitert werden: Offene Bahnsteige, Warteschlangen vor den Eingängen und den Ticketkontrollen an Veranstaltungsorten. Eine konkrete Erweiterung des Crowd-Monitoring-Systems stellt das Szenario am Flughafengelände dar: Die Beobachtung und das Zählen der Menschenmasse am Fluchttunnelausgang.

AP 2.3.2 – Geländeüberwachung Es wurde wie bei der Videoüberwachung untersucht, inwieweit das System in anderen Anwendungsbereichen eingesetzt werden kann. Hierbei konnten u.a. folgende Anwendungsfälle identifiziert werden: Veranstaltungen, Bahn- oder Baustellenüberwachung. Da die Umgebung und die Funktion des zu überwachenden Zielobjektes eine große Rolle bei der Leistung und der Zuverlässigkeit jedes physikalischen Überwachungssystems spielen, müssen diese Gegebenheiten bei der neuen Anwendung berücksichtigt werden. Ein universelles Überwachungssystem, das für alle Einrichtungen und alle Situationen geeignet ist, kann aus heutiger Sicht nicht realisiert werden.

2.1.3 AP3 – Akzeptanz, Datenschutz, legale und soziale Auswirkungen

AP3.1 – Interviews

Im Anschluss an die Experteninterviews wurden 18 weitere Interviews mit Flugpassagieren im Sicherheitsbereich des Flughafen Schönefeld durchgeführt, in denen u. a. erste Erkenntnisse zur Wahrnehmung von Sicherheit aus der Expertensicht aufgegriffen, aber auch Forschungsergebnisse aus der

einschlägigen Literatur berücksichtigt wurden. Insgesamt stand die subjektive Wahrnehmung und Bewertung der Sicherheitsmaßnahmen am Flughafen im Fokus. Die Interviews wurden transkribiert und mit MAXQDA ausgewertet.

AP3.2 – Befragung

Die erarbeiteten Kategorien und die Transkription derer mittels MAXQDA wurden in Aussagen transferiert und Themenblöcke zu Sicherheitsmaßnahmen gebündelt. Der Fragebogen umfasste neben persönlichen und sozioökonomischen Angaben auch die der „Fluggewohnheiten". Zudem deckte er die Bereiche „Vertrauen", „Videoüberwachung", „Wahrnehmung von Sicherheitsmaßnahmen", „Werte und Präferenzen", „Diskriminierung", „Privatsphäre" ab, die dem Modell folgend letztlich in der Gesamtschau Auswirkungen auf die Akzeptanz der Befragten hinsichtlich von Sicherheitstechnologien besitzen. Die Befragung wurde an sechs Wochentagen im Zeitraum vom 6. bis 28. Mai 2014 am Flughafen Berlin-Schönefeld durchgeführt. Die Anzahl der Befragten übertraf mit 1.067 Personen (ab 18 Jahren aus insgesamt 60 Nationen) bei weitem die Vorgabe von 300 Passagieren. Der Fragebogen lag in zweisprachiger Ausführung (deutsch und englisch) vor, um in der Analyse darauf aufbauende Vergleiche zu ermöglichen. Das Verhältnis der deutschen zu den englischen Fragebögen betrug dabei etwa 50/50.

AP3.3 – Analyse

Die in einem Datensatz zusammengefassten Ergebnisse wurden statistisch ausgewertet und grafisch dargestellt. Des Weiteren wurden nationale Vergleiche angestellt, Indizes zur Akzeptanz von Sicherheitsmaßnahmen gebildet sowie mehrere lineare Regressionsmodelle generiert. Diese wurden in berichtsform festgehalten und spiegeln Anhaltspunkte sozialer Aspekte von Sicherheit wider. Hierzu zählen auch Muster von Einstellungen, die auf relevante Akzeptanzfaktoren der im Gesamtprojekt zu entwickelnden Sensortechnik schließen lassen, den Projektpartnern übermittelt wurden und als Voraussetzung für das weitere Vorgehen im Projekt dienlich waren.

Erzielte Ergebnisse

Die in SAFEST durchgeführte Befragung von Flughafensicherheitsexperten erstreckte sich auf den Zeitraum zwischen dem 14. Oktober 2012 und dem 21. Januar 2013. Insgesamt wurden 15 leitfadengestützte Interviews mit 17 Personen geführt, von denen zwei in englischer Sprache stattfanden. Unter den Interviewten befanden sich hauptsächlich ausgewählte Experten des Projektpartners Flughafen Berlin Brandenburg (FBB) sowie zwei Mitarbeiter des Projektpartners Safran/Sagem. Die durchschnittliche Interviewdauer betrug etwa 45 Minuten. Der Fokus lag dabei in erster Linie auf den technischen Anforderungen, die bei der Implementierung und dem Betrieb von Sicherheitstechnologien relevant erscheinen. Eine Strukturierung des Interviewmaterials mit MAXQDA wird in Abbildung 1 dargestellt.

Ein weiterer Schwerpunkt lag auf der Thematik von Sicherheitsmaßnahmen an Flughäfen und der Diskussion darüber, welchen Beitrag die Maßnahmen im Einzelnen leisten. Des Weiteren sollte ihre Notwendigkeit und ihr sicherheitsrelevanter Mehrwert von den Experten nachgezeichnet werden. Zusammenfassend lässt sich hierbei festhalten, dass die Experteninterviews auf unterschiedliche Zielkonflikte hindeuten, die es für einen Flughafen zu lösen gilt. Sicherheit bewegt sich hierbei im Spannungsfeld zwischen aviation (Transport) und non-aviation (Ökonomie). Das bedeutet, dass nicht zwangsläufig die beste Sicherheitslösung angestrebt werden kann, die unter Umständen auch weniger Nebeneffekte mit sich bringen würde, sondern Sicherheit als Optimum einer Kosten-Nutzen-Rechnung zu sehen ist: Was technisch möglich und aus Expertensicht sinnvoll ist und zudem Kosten einspart, wird implementiert. Die Ausgestaltung der Sicherheitsmaßnahmen am Flughafen ist demnach ökonomisch begrenzt und nicht durch ethische oder moralische Maßstäbe. Lediglich die Unzufriedenheit der Konsumenten – also der Flugpassagiere – könnte, dieser ökonomischen Logik folgend, eine Veränderung bewirken. Diese Tatsache rückt schließlich auch Fragen der Akzeptanz oder des Protests wieder

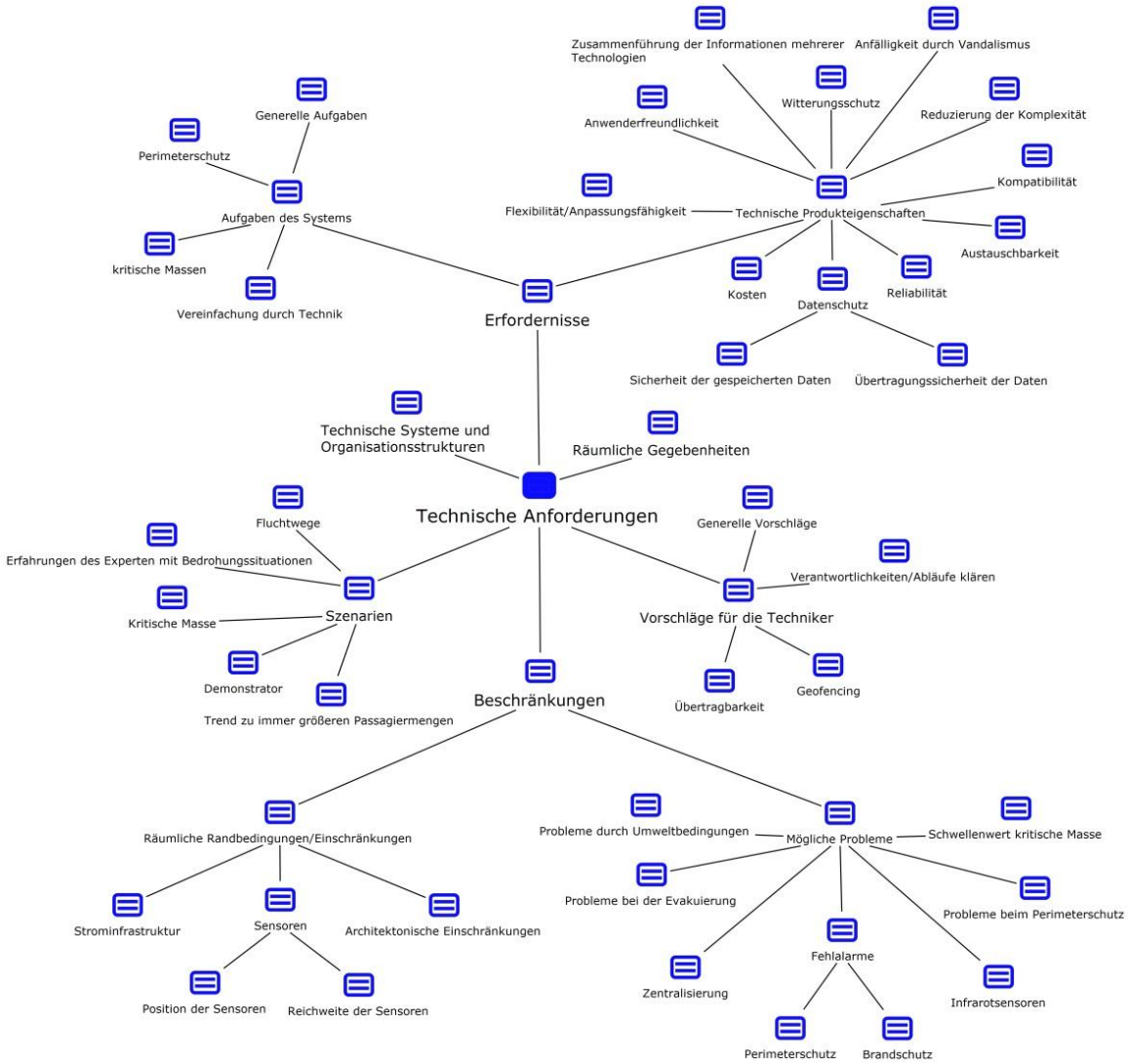


Abbildung 1: Technische Anforderungen von Sicherheitstechnologien aus Expertensicht.

deutlicher in den Fokus der Betrachtung; dies allerdings nur unter ökonomischen Gesichtspunkten. Auch die zunehmende Technisierung von sicherheitsrelevanten Aspekten ist somit nicht einzig und allein als technokratische Einstellung interpretierbar, sondern unterliegt mindestens genauso stark einer ökonomischen Rationalität, die darauf basiert Personalkosten einzusparen. Es überrascht auch wegen dieser Logik nicht, dass alle Experten die Möglichkeit absoluter Sicherheit negierten. Dieses Bild passt auch ganz generell zu einer veränderten Expertenkultur, die sich zunehmend dem Typus des reflexiven Experten zuwendet. Risiko wird in diesem Zusammenhang nicht ausschließlich als Wahrscheinlichkeitskonstrukt operationalisiert, das sich aus den vorhandenen Wissensbeständen errechnen lässt, sondern ebenso als Produkt, das aus Nicht-Wissen resultiert und somit niemals hundertprozentig bestimmbar sein kann.

Um den Blickwinkel von den Sicherheitsexperten auf die von den Sicherheitsmaßnamen betroffenen Passagiere zu wechseln, wurden zwischen dem 9. und dem 13. September 2013 im Wartebereich des Flughafens Berlin Schönefeld 18 problemzentrierte Interviews durchgeführt. Auf Basis der problemzentrierten Interviews konnte ein nicht deterministisch zu interpretierendes Modell erstellt werden, mit dem unterschiedliche Dimensionen aufgezeigt wurden, die die Akzeptanz bzw. die Wahrnehmung von Sicherheitsmaßnahmen beeinflussen können. Als Ausgangspunkt des Modells diente die Unterscheidung in Makro- (Sicherheitskultur) und Mikroebene (persönliche Erfahrungen). Diese beiden Ebenen sind innerhalb des Modells den Einflussfaktoren Werte und Präferenzen (hierunter wurde auch Ver-

trauen subsumiert) vorgelagert. Vertrauen und Werte wirken weiterhin auf die subjektive Risiko-/Sicherheitswahrnehmung ein, während die Risiko-/Sicherheitswahrnehmung ihrerseits auf die Akzeptanz im Kontext der Sicherheitsmaßnahmen am Flughafen wirkt. Die Akzeptanzformen lassen sich schließlich in verschiedene Typen differenzieren, welche aus der Akzeptanztypologie Luckes (1995) entstammen.

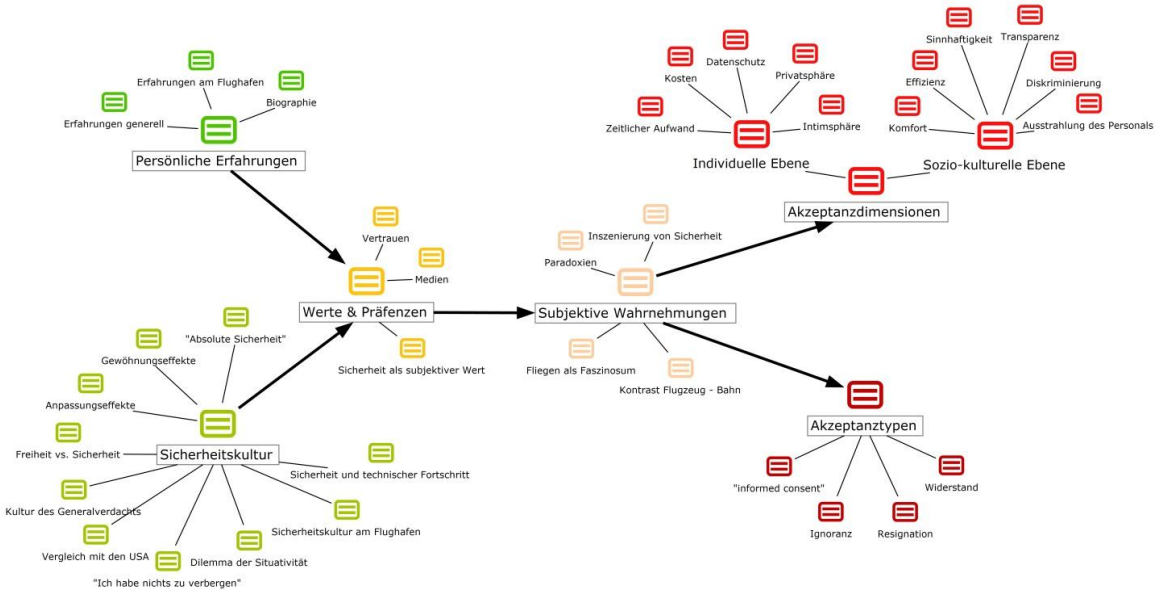
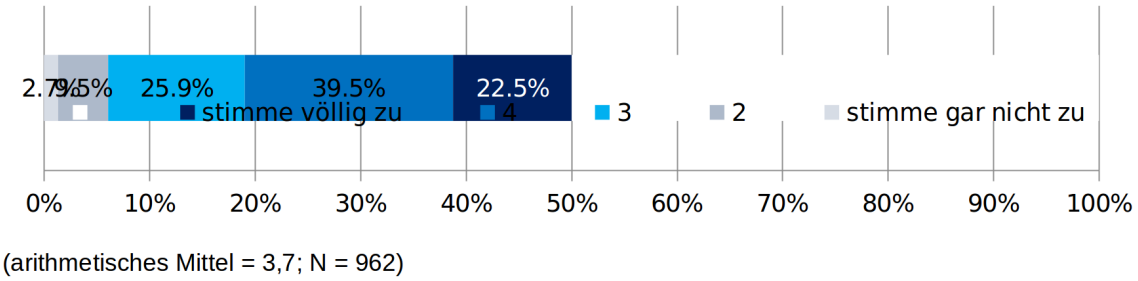


Abbildung 2: Modell zu Akzeptanzfaktoren als Ergebnis der problemzentrierten Interviews.

Auf der Grundlage des Modells konnten erste Anhaltspunkte für die Beurteilung der Maßnahmen identifiziert und die Perspektive, mit denen die jeweiligen Befragten auf die Thematik blicken, gedeutet werden, die schließlich Eingang in die Überlegungen innerhalb des AP 3.2 fanden.

Auf die einzelnen quantitativen Ergebnisse bezogen, kann vorweggenommen werden, dass ca. drei Viertel der Befragten Sicherheitsmaßnahmen an Flughäfen befürworten und sie als akzeptiert gelten können. Eine differenziertere Betrachtung zeigt Felder auf, bei denen Unstimmigkeiten in der Bewertung festgestellt wurden bzw. Ausprägungen, die kritischer betrachtet werden als andere. Hierzu zählen vor allem im internationalen Vergleich die Beurteilung des „Körperscanners“, die Zuschreibung der Erhöhung von Sicherheit durch Video-/Kameraüberwachung oder der Eingriff von Maßnahmen, die die Intimsphäre berühren. Ebenso ließ sich festhalten, dass ein höheres Bildungsniveau eher zur Ablehnung von Maßnahmen führt sowie sich altersbedingte Unterschiede in Bezug auf die Akzeptanz von Sicherheitsmaßnehmen feststellen lassen. Hinsichtlich der Akzeptanz wurde ein additiver Akzeptanz-Index (Cronbach's Alpha = 0.7) gebildet, der sich aus zwei Variablen zusammensetzt (Abbildung 3 und 4).



(arithmetisches Mittel = 3,7; N = 962)

Abbildung 3: Variable 1 – „Die Ausgestaltung der Sicherheitsmaßnahmen finde ich annehmbar.“

Die Generierung dieses Akzeptanz-Index‘ war die Grundlage für die statistische Berechnung diver-

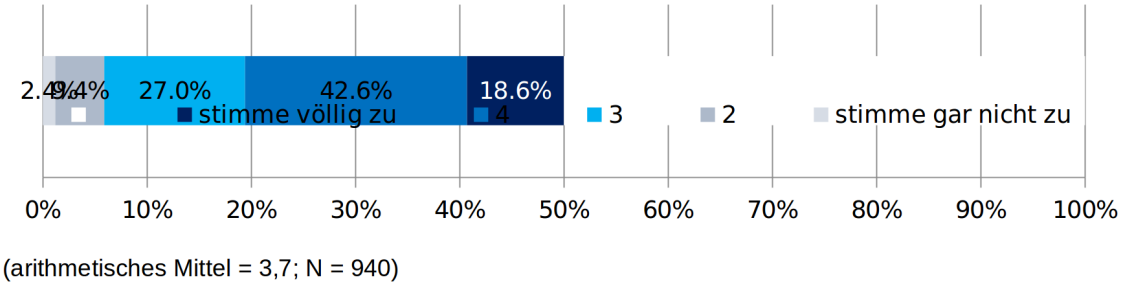


Abbildung 4: Variable 2 – „Ich finde die Ausgestaltung der Sicherheitsmaßnahmen am Flughafen sinnvoll.“

ser Regressionsmodelle, welche unterschiedliche Faktoren (in Form unabhängiger Variablen) beinhaltete. In Tabelle 1 sind die empirischen Ergebnisse der Fragebogenstudie innerhalb eines stufenweisen Regressionsmodells aufgeführt, das pro Stufe unterschiedlich thematisch gelagerte Indikatoren beinhaltet.

Insgesamt deuten die Modelle sowie die weiteren empirischen Befunde auf folgende Kernaspekte hin:

- ... sprechen sich eher für die Nutzung und die positiven Auswirkungen von Videoüberwachung aus.
- ... haben eine höhere Sicherheits- bzw. Risikowahrnehmung (z.B. in Bezug auf Terrorismus).
- ... weisen sie ein höheres Niveau an institutionalisiertem Vertrauen und Vertrauen in die zuständigen Sicherheitsakteure des Flughafens auf.
- ... fliegen im Mittel seltener.
- ... sind zumeist älter und haben einen vergleichsweise niedrigeren Bildungsstatus.

Abhängige Variable: Akzeptanzindex	**I**	**II**	**III**	**IV**	**V**
Kriminalitätsfurcht	-0,11**				-0,11*
Bedrohungsempfinden durch Terrorismus	0,30***				0,17***
Allgemeines Sicheheitsgefühl	0,07				0,10
Sicherheitsgefühl am Flughafen	0,14***				0,09
Institutionalisiertes Vertrauen (Index)		0,11**			0,04
Generalisiertes Vertrauen (Index)		0,01			0,07
Vertrauen in Flughafenakteure (Index)		0,39***			0,18***
Flughäufigkeit (kategorial)			-0,15***		-0,11**
Diskriminierungsgefühl			-0,23***		0,08
Einstellung gegenüber CCTV (Index)				0,38***	0,23***
Sicherheit als Wert (Schwartz-Skala)				0,23***	0,11*
Bildung					0,08*
Geschlecht (Referenz: Männer)					0,00
Alter (Kategorial)					0,13**
N	820	573	708	730	375
korrigiertes	0.09	0.20	0.07	0.28	0.38

Tabelle 1: Lineares Regressionsmodell (stufenweise).

Allerdings darf bei der Interpretation der empirischen Ergebnisse nicht vergessen werden, dass die Präferenzen auf der Individualebene sehr divers und unterschiedlich gelagert sind. Was dies in Bezug auf die konkrete Ausgestaltung von Sicherheitsmaßnahmen (z.B. bei der Festlegung von bestimmten Grenzwerten) bedeutet, sollte Gegenstand von weiteren Reflexionen sein, was etwa in Form von partizipativen (etwa im Sinne einer breiten Stakeholder-Beteiligung) Verfahren genauer bestimmt werden kann. Inwieweit sicherheitstechnologische Innovationen im Kontext des Flughafens wirklich zu einer Verstärkung von Diskriminierung und Ungleichheiten beitragen, war nicht die Fragestellung des Teilvorhabens, sollte aber bei der soziologischen, ethischen und rechtlichen Betrachtung weiterhin fokussiert werden, um solche Nebenfolgen einzudämmen. Außerdem bleibt die Frage inwieweit technologische Innovationen zu einem Strukturwandel auf der kulturellen Ebene beitragen spekulativ, aber dennoch elementar für die Einordnung und Bewertung solcher Entwicklungen. Da in diesem Teilprojekt fast ausschließlich auf die Einstellungen und Wahrnehmungen der Flugpassagiere abgezielt wurde, kann dieser Aspekt zwar nicht beantwortet, aber dennoch mitgedacht werden, wenn der Vergleich von britischen und deutschen Befragten Rückschlüsse auf unterschiedlich ausgeprägte und prägende Sicherheitskulturen zulässt. Dieses empirische Ergebnis steht zudem in Übereinstimmung mit anderen ländervergleichenden Studien zu Videoüberwachung (Hempel u. Töpfer 2004).

Nutzen

In Hinblick auf den Nutzen in Form möglicher Implikationen der Teilstudie für die technischen Entwickler sei auf folgende Punkte verwiesen:

- Akzeptanz als multifaktorielles Konstrukt muss zwingend von usability (als oftmals binärer Variable) abgegrenzt werden.
- Eingriffe in die Privatsphäre sind nur einer von vielen Nebeneffekten, die von sicherheitstechnologischen Innovationen ausgehen (allerdings haben Einstellungen zum Datenschutz signifikanten Einfluss auf die Akzeptanz, was einen konstitutiven Bestandteil des SAFEST-Projekts unterstützt).
- Gute Intentionen auf Entwicklerseite müssen nicht zwangsläufig in guten Konsequenzen resultieren; aufgrund der hohen Komplexität technologischer Innovationen sind die Nebenfolgen dagegen nur schwer vor der Implementierung abschätzbar.
- Die Strategie positive und negative Nebeneffekte von technologischen Innovationen gegeneinander abzuwiegen, ignoriert die Veränderung kultureller Rahmenbedingungen, die durch solche Innovationen hervorgebracht werden (z.B. Gewöhnungseffekte im Kontext von Videoüberwachung, die nicht zwangsläufig auf eine zunehmende Akzeptanz hindeuten müssen, sondern ebenso als Indikator für Ignoranz angesehen werden können).

2.1.4 AP4 – Plattformumsetzung

AP4.4 – Individuelle Integration

AP4.4.1 – Videoüberwachung Das Ziel des Arbeitspaketes ist das Softwaremodul für videobasierte Erkennung von Menschen in das Gesamtsystem zu integrieren und zu testen. Hierfür wurde ein sogenanntes Merging-Modul entworfen, das als Schnittstelle zwischen dem Kamera-Koten und der zentralen Event-Processing-Unit dient. Weitere Details zu dem Merging-Modul sind im Arbeitspaket 5.2.1 dargestellt.

Das Zusammenspiel der Komponenten wurde erst lokal auf einem Rechner, dann global mit dem Black-Box-Ansatz überprüft: die Menschenerkennungskomponente hat aufgezeichnete Videos in Echtzeit analysiert, das Ergebnis wurde per IPv6-Verbindung an das Merging-Modul und anschließend an den im Fraunhofer FOKUS aufgesetzten Server zur finalen Auswertung übertragen. Die Event-Processing-Unit hat das im Voraus definiertes Szenario “blockierte Tür” erkannt. Das visuelle Feedback

der Alarmkomponente von Fraunhofer FOKUS wurde mit den originalen Videosequenzen verglichen. Dieses Szenario ist exemplarisch in der Live-Demo bei dem Meilensteintreffen am 17.11.2013 vorgestellt worden. Die Tests wurden mehrfach und in enger Kooperation und Anwesenheit mit den Kollegen von Fraunhofer FOKUS und der daviko GmbH durchgeführt. Dies ermöglichte eine modulübergreifende Analyse des Systems und aller Schnittstellen – die Fehler konnten nicht nur kollektiv gefunden, sondern auch erfolgreich beseitigt werden.

Die Integration der Videoüberwachung wurde zudem erfolgreich auf dem Meilensteintreffen am 17.11.2013 sowie auf dem Abschlusstreffen am 18.09.2015 demonstriert.

AP4.4.2 – Geländeüberwachung Die Geländeüberwachung basiert auf kostengünstigen, drahtlosen Knoten die über Standard Internettechnologien (IPv6) miteinander kommunizieren. Kern dieser Knoten ist das in SAFEST entwickelte Betriebssystem RIOT. Durch den für RIOT entwickelten Netzwerkstack ist es diesen Knoten möglich, eine Ende-zu-Ende Verbindung mit jedem beliebigen Server im Internet herzustellen. Dies ermöglicht eine einfache und direkte Integration der zur Geländeüberwachung genutzen Knoten in das SAFEST-Gesamtsystem.

Das Integrationskonzept der Geländeüberwachung besteht aus mehreren Ebenen, welche der Kommunikationshierarchie entsprechen. Die unterste Ebene besteht aus der Kommunikation zwischen zwei einzelnen Sensorknoten in einer "Single-Hop"-Konfiguration. Auf der nächsten Ebene wurde die Kommunikation zwischen Sensorknoten in einer "Multi-Hop"-Konfiguration verifiziert, welche neben der reinen IPv6 Kommunikation ebenfalls das auf RPL basierte Routing einschließt. Eine Ebene höher wurden die Gateways (sogenannte "Border-Router") entworfen und integriert, welche die Verbindung zwischen dem Low-Power-Funknetzwerk und dem herkömmlichen Internet herstellen. In diesem Integrationschritt wurde die IP-Kommunikation zwischen einzelnen Sensorknoten sowie den Servern der zentralen Event-Processing-Einheit verifiziert. Auf der obersten Ebene wurde schließlich der Transport der eigentlichen Event-Daten von den Sensorknoten zu dem zentralen Event-Processing nachgewiesen sowie deren korrekter Empfang gezeigt.

Neben automatisierten Tests unter Einsatz von Testbeds (FIT IoT-Lab, DES Testbed) wurde die Integration der Geländeüberwachung in das SAFEST Gesamtsystem ebenfalls erfolgreich auf den Meilenstein- und Abschlussdemonstrationen gezeigt.

AP4.4.3 – Leitsystem Es wurde eine Interaktionskomponente zwischen Leitsystem und dem Sensornetz entworfen und integriert. Dafür wurde der Lösungsraum für die Detektion der Mobiltelefone der Passagiere analysiert sowie eine Konzept erarbeitet, Inhalte (wie z.B. Fluchtwege) für geographische Cluster auszuliefern. Die Netzarchitektur sieht vor, dass die Mobiltelefone per WLAN ansprechbar sind. Jedes Telephon ist über einen Access Point angebunden, welcher wiederum per Switch in das restliche Netz eingebunden wird. Der Flughafen- bzw. Netzbetreiber kann eine explizite Zuordnung zwischen Access Point und räumlicher Umgebung vornehmen, da der Aufstellstandort fest ist. Zudem ist die Zuordnung zwischen Access Point und Switch-Port eindeutig. Über das SNMP-Protokoll und die MAC-Adressen der Telephone werden die zugehörigen Switch-Ports ermittelt. Somit lassen sich die Telephone ohne Verletzung der Privatsphäre räumlich clustern. Der Web-Server kann dann im Gefahrenfall kontextspezifische Webseiten ausliefern.

2.1.5 AP5 – Wissensfusionierung und Alarmkomponenten, Leitsystem

AP5.1 – Sensorebene

AP5.1.1 – Erkennung Menschenmengen Dieses Arbeitspaket wurde in enger Zusammenarbeit mit der daviko GmbH bearbeitet. Es wurden zwei Aufgabengruppen identifiziert: Einerseits muss das Videoverarbeitungsmodul in der Lage sein, Menschen zu erkennen, andererseits gilt es die Bewegung der Menschen von Interesse zu berücksichtigen. Aus dem im Arbeitspaket 2 ausgearbeiteten Szenarienkatalog geht hervor, dass keine rohen Daten im System übertragen werden sollen. Eine weitere Anforderung aus dem Szenarienkatalog ist der Schutz der Privatsphäre der beobachteten Personen.

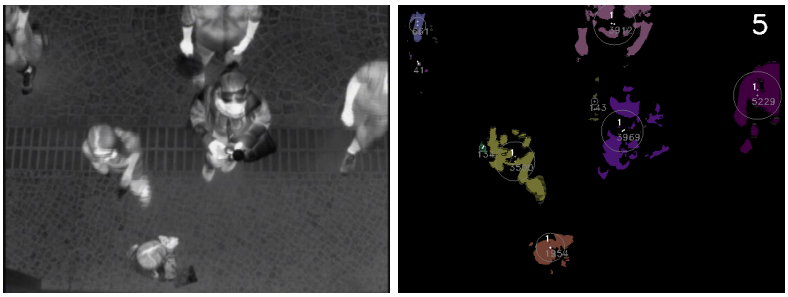


Abbildung 5: Original- und Ergebnisframe (Eingang Informatikgebäude FU).

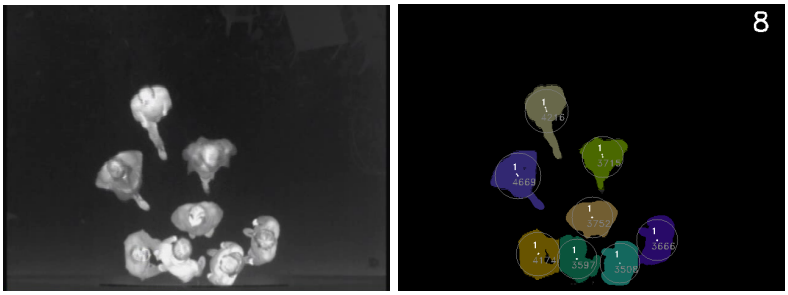


Abbildung 6: Original- und Ergebnisframe (Hinterhof Informatikgebäude FU).

Daraus folgt, dass der Kamera-Knoten zur Laufzeit jedes Frame bearbeiten soll und nur die Approximation der erkannten Personen speichert. Außerdem wird die Kamera die zu beobachtende Fläche von oben betrachten, was uns erlaubt, Menschen mit einem Kreis anzunähern. Die Aufgabe der Videoverarbeitungskomponente liegt somit darin, für jede Person einen um sie begrenzenden Kreis zu finden.

Als erstes wird der Vordergrund in jedem Frame über die Differenz zwischen dem Originalframe und dem Hintergrundmodelll gebildet. Der Hintergrund wird pixelweise modelliert: Eine adaptive Mischverteilung aus Gaußfunktionen beschreibt die Intensität für jeden Pixel. Die Modellierung einer Szene mit einer adaptiven Mischverteilung bietet die Möglichkeit nicht nur Beleuchtungen und Flächen mit mehreren Verteilungen zu beschreiben, sondern auch sich deren Veränderungen anzupassen. Die Intuition dahinter ist, dass der Hintergrund statisch ist, somit auch präsenter in einer Szene im Vergleich zu Menschen. Demnach repräsentieren kurzfristige Veränderungen in den Flächeneigenschaften Menschen. Der Algorithmus beobachtet die Szene und parameterisiert n (üblicherweise drei bis fünf) Gaußverteilungen, die sie beschreiben. Sie werden folgendermaßen gewichtet: Je kleiner die Varianz ist, desto höher ist das Gewicht der Verteilung. Die ersten k aus n repräsentieren somit statischen den Hintergrund. Bei jedem Frame wird für jeden Pixel entschieden, ob er mit den ersten k oder letzten $n - k$ Verteilungen beschrieben werden kann und entsprechend zum Hintergrund oder Vordergrund gezählt wird. Falls keine der Verteilungen in der Lage ist, den Pixel zu beschreiben, muss eine der Mischverteilungen neu parameterisiert werden.

Im zweiten Schritt werden nur die Vordergrundpixel analysiert. Das Originalbild wird nicht gespeichert. Es wird nach den zusammenhängenden Komponenten in der Vordergrundmaske gesucht. Als zusammenhängend gelten direkte Nachbarn. Die zusammenhängende Elemente des Vordergrunds bilden Teile der Personen und müssen mittels dichtebasierten Clusteringverfahrens zu einzelnen Personen zusammengefügt werden. Die gefunden Cluster bilden die sogenannten “Blobs” und repräsentieren Personen, die anschließend jeweils mit einem Kreis approximiert werden.

Die Software, die diese drei Schritte implementiert, wurde mit der von SAGEM gelieferten Kamera getestet. Dafür wurden mehrere Reihen der Aufnahmen organisiert. Daraus sind drei Typen der Videos entstanden, die sich in den Eigenschaften des Hintergrundes, der Höhe der Kamera und der Umgebung

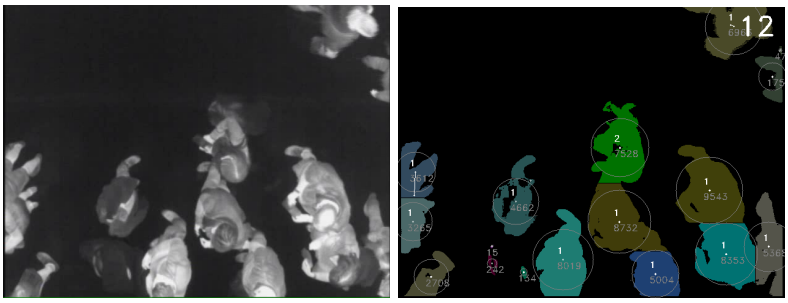


Abbildung 7: Original- und Ergebnisframe (Boarding Gate Flughafen Tegel).

unterscheiden. Die Sequenzen des ersten Typs wurden während der Langen Nacht der Wissenschaften 2013 vor dem Eingang in das Informatikgebäude der Freien Universität aufgezeichnet. Die Kamera konnte relativ niedrig angebracht werden, das aufgenommene Areal befindet sich draußen, der Boden enthällt viele Kanten. Das Originalframe aus den Aufnahmen diesen Typs ist in der Abbildung 5 auf der linken Seite zu sehen. Weitere Sequenzen wurden während der Tests zur Live-Demo aufgezeichnet. Die Szene stellt das Szenario "Blockierte Tür" dar, findet draußen im überdachten Bereich statt. Die Kamera konnte auf der Höhe von acht Metern befestigt werden. Das Szenario ist in der Abbildung 6 zu sehen. Die Abbildung 7 zeigt eine Szene aus der Sequenz, die am Flughafen Tegel aufgenommen wurde – Menschen stehen in der Schlange vor dem Boarding Gate.

Eine exakte Evaluierung des Hintergrundextraktors ist sehr herausfordernd: Um das Ergebnis mit der Wahrheit vergleichen zu können, müsste man für jeden Pixel notieren, ob es zum Hintergrund oder Vordergrund gehört. Es ist praktisch unmöglich jedes Pixel per Hand zu markieren, automatische Tools ausreichender Qualität existieren nicht. Aus diesem Grund wurde entschieden, das Endergebnis der Videoverarbeitung zu evaluieren – die Anzahl der Menschen pro Frame wurde gezählt. Das Ergebnis des Menschenerkennungsalgorithmus ist beispielhaft in den Abbildungen 5, 6 und 7 jeweils auf der rechten Seite dargestellt. Man sieht, dass es gelungen ist, bei unterschiedlichen Hintergründen einzelne Personen zu erkennen und richtig zu zählen. Die Abbildung 7 weist allerdings darauf hin, dass sehr eng aneinander stehende Personen sowie komplexe Hintergründe wie in der Abbildung 5 eine Herausforderung für den Algorithmus darstellen.

Für die exakte Evaluierung wurden drei Sequenzen per Hand annotiert und mit der Ausgabe der Software verglichen. Die mittlere Abweichung vom korrekten Ergebnis war 0.839 Personen, die Varianz der Abweichung vom korrekten Ergebnis 0.567 bei maximaler Anzahl der Menschen im Bild von zwölf Personen.

Ursprünglich wurde vorgeschlagen, die Bewegung der Menschen blockweise zu analysieren. Allerdings wäre es notwendig, eine parallele Berechnung zu Menschenerkennung durchzuführen, wobei die Bewegung der einzelnen Menschen effizient aus der Positionsdifferenz zwischen den Frames berechenbar ist. Aus diesem Grund wurde entschieden, die Bewegung in der Szene mit Hilfe von Trajektorien zu repräsentieren.

AP5.1.2 – Geländeüberwachung Die Geländeüberwachung in SAFEST basiert auf kostengünstigen, mit diversen Sensoren ausgestatteten Knoten die drahtlos miteinander kommunizieren. Die Sensorknoten bestehen hardwareseitig im Kern aus einfachen Mikrocontrollern, den Sensoren sowie entsprechenden Funkadaptern. Die Standard „Component-of-the-Shelf" (COTS) Bauteile sind einfach austauschbar.

Im Vordergrund der Geländeüberwachung steht die in SAFEST entwickele Open-Source Software-Plattform RIOT. Diese übernimmt drei Hauptaufgaben: sie (i) abstrahiert die Hardware der Sensorknoten und bietet ein einheitliches Treibermodell zur Integration diverser Sensorik, sie (ii) bietet Datenstrukturen und Algorithmen zur lokalen Fusion und Auswertung der Sensordaten und sie (iii) bietet die Kommunikationsinfrastruktur zur Vernetzung der Sensorknoten untereinander.

RIOT hat sich im Laufe von SAFEST zu einem internationalen Open-Source-Projekt mit großer Gemeinschaft und hohem Bekanntheitsgrad entwickelt.

Portierbarkeit: Hardware-Abstraktion Die Hardware-Abstraktion in RIOT basiert auf einer Reihe von low-level Treibern, die die einzelnen Funktionseinheiten moderner Microkontroller abstrahieren. Zu diesen gehören unter anderem die Ansteuerung der Pins (GPIO), Bus Systeme wie SPI, UART oder I2C, Analog-Digital Wandler (ADC) und verschiedene Timer. Abbildung 8 zeigt den grundsätzlichen Aufbau dieser Hardware-Abstraktion.

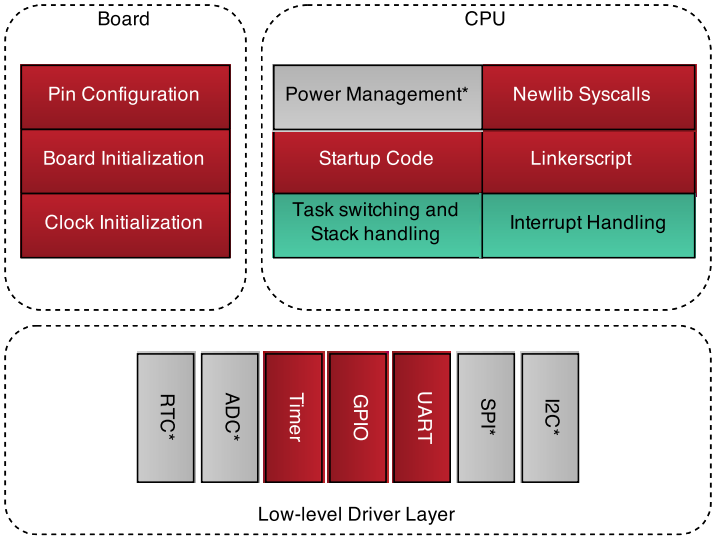


Abbildung 8: Konzept der Harware-Abstraktion in RIOT.

Auf dieser Schnittstelle setzten Gerätetreiber auf, die somit völlig entkoppelt von der eigentlich Hardware-Platform implementiert werden. Dieses Konzept ermöglicht es zum einen, Gerätetreiber auf allen unterstützten Platformen zu nutzen, und macht es zum anderen sehr einfach neue Treiber zu implementieren.

Im Projektzeitraum alleine wurde die Unterstützung für 40 neue Mikrocontroller Boards, 20 neue Mikrocontroller Typen, 19 Gerätetreibern und 5 Netzwerkgeräten zu RIOT geschaffen. Damit unterstützt RIOT heute fast alle gebräuchlichen Mikrocontroller Familien sowie IoT-typische Netzwerkadapter und Sensortypen. Damit konnte eine erhebliche Verbesserung zum aktuellen Stand der Technik (z.B. mbed oder Contiki) erreicht werden. Diese Zahlen spiegeln sich ebenfalls in der Code-Basis von RIOT wider, welche im Laufe von SAFEST von ca. 40.000 Zeilen C-code auf über 500.000 Zeilen gewachsen ist.

Kommunikation: Netzwerkstack Neben der Hardware-Abstraktion ist der in SAFEST entwickelte GNRC Netzwerk Stack eine der wichtigsten Komponenten von RIOT. Der GNRC Netzwerkstack basiert auf offenen Protokollen, die von der IETF spezifiziert wurden und somit die Basis Internet-basierter Kommunikation darstellen. Hierzu gehören neben den Kern-Internet-Protokollen wie IPv6 und UDP neue, explizit für das Internet der Dinge spezifizierte Protokolle wie 6LoWPAN und RPL.

Der Netzwerk-Stack in RIOT ist das zentrale Element der Kommunikationsplattform zur Integration von Sensorknoten in das SAFEST-Framework. Im Projektverlauf hat sich gezeigt, dass der in RIOT ursprünglich entwickelte Netzwerk-Stack die Anforderungen von SAFEST nicht vollständig erfüllt. Die Implementierung bot zum einen nicht die gewünschte Stabilität und lässt sich zum anderen durch mangelnde Modularität nicht ohne weiteres an alle im Projektverlauf entstandenen Anforderungen anpassen. Aus diesem Grund wurde ein kompletter Neuentwurf des Netzwerk-Stacks vorgenommen. Im Fokus hierbei steht eine Softwarearchitektur, die nicht nur eine zukünftige Anpassbarkeit und Erweiterbarkeit garantiert, sondern weiterhin die Implementierung automatisiert testbar macht.

Über diesen inkrementellen Entwicklungsprozess konnte eine deutlich höhere Software-Stabilität und Anwendbarkeit sichergestellt werden.

Die hoch modulare Architektur des GNRC Netzwerkstacks erlaubt eine sehr einfache and präzise Konfiguration und Erweiterbarkeit. Dies erlaubte es nicht nur auf sich ändernde Anwendungsanforderungen zu reagieren, sondern bildet eine ideale Basis für zukünftige Forschung auf allen Ebenen der Computernetzwerke (z.B. MAC layer, Routing Protokolle). Im Projektzeitraum konnte dies demonstriert werden, indem neuartige Kommunikationsprotokolle (sogenannte informationszentrische Netze) in das SAFEST-Rahmenwerk eingeführt wurden.

Nachhaltigkeit: Community Neben den technischen Errungenschaften hat der Aufbau und die Förderung der Open-Source-Gemeinschaft rund um RIOT in SAFEST eine hohe Priorität gehabt. Der Hauptgrund hierfür ist die Nachhaltigkeit des Projekts, denn durch eine aktive Gemeinschaft von freien Entwicklern wird sichergestellt, dass RIOT (als Teilergebnis von SAFEST) auch nach Ende der Projektlaufzeit gepflegt und weiterentwickelt wird.

Heute hat RIOT mehr als 100 Programmierer von fünf Kontinenten, die im Schnitt über 500 Commits pro Monat einreichen. Den RIOT Mailinglisten, die neben Github als zentrale Kommunikationsplatform etabliert worden sind, folgen über 500 Entwickler.

AP5.1.3 – Leitsystem Für die zielgerichtete Evakuierung der Passagiere über das Smartphone wurden erste Konzepte erstellt, die die adaptive Präsentation von Webinhalten auf bestimmte Nutzergruppen ermöglichen. Es wurden prinzipiell zwei Ansätze identifiziert. Einerseits können die Funkzugangspunkte als transparenter Proxy dienen und im Gefahrenfall auf gesonderte Webseiten umlenken. Andererseits kann die Zuordnung zwischen Nutzergruppe und Fluchtplan auf dem Webserver selbst erfolgen. Letzteres bietet den Vorteil, dass die Anzahl der zu konfigurierenden Netzgeräte geringer ist. Dafür benötigt der Webserver aber Zusatzinformationen, um den aktuellen Standort der ausgelösten HTTP-Anfragen zu berücksichtigen.

In SAFEST wurde ein Demonstrator, der auf einem transparenten HTTP-Proxy im Funkzugangspunkt basiert, implementiert. Dieser wurde erfolgreich auf der Abschlusspräsentation gezeigt und verifiziert.

AP5.2 – Design Wissensfusionierung

AP5.2.1 – Konzeptuelles Modell Die Erarbeitung des Konzeptes für die Wissensfusionierung wurde an das Framework ARCHITECT [1] angelehnt. Das Framework formalisiert vier Abstraktionsschichten (vgl. Abbildung 10) in die ein eventbasiertes System zerlegt werden kann und hilft auf eine strukturierte Weise ein solches System zu entwerfen.

Als erstes wurde ein Datenmodell für das videobasierte System entworfen (Language Layer). Das zentrale Konzept ist eine Dichtematrix, genannt Density-Map: Diese speichert diskretisierte Dichten des zu beobachtendes Areals. Die Density-Maps erlauben es die räumliche Komponente der Daten einfach zu speichern. Für Systemevents wurde ein Snapshot-Modell gewählt: Das System verarbeitet periodisch aufgezeichnete Snapshots der kontinuiertlichen realen Welt. Das Language Layer und das zentrale Regelwerk aus der nächsten Schicht (Execution Layer) wurde von Kollegen von Fraunhofer FOKUS bereitgestellt. Die unteren Schichten müssen die Daten aus unterschiedlichen Quellen zusammenfassend für die Weiterverarbeitung liefern. Das Merging-Modul übernimmt diese Aufgabe und bildet die Kommunikationsschicht. Das Merging-Modul schreibt Density-Maps auf den Kanal, den die zentrale Event-Processing-Unit (EPU) abonnieren kann. Das Modul selbst abonniert einen Kanal, auf den die Sensor-Knoten deren Snapshot-Events schreiben und verarbeitet diese zu den Density-Maps für das EPU.

[1] Agnès Voisard, Holger Ziekow: ARCHITECT: A layered framework for classifying technologies of event-based systems. Inf. Syst. 36(6): 937-957 (2011)

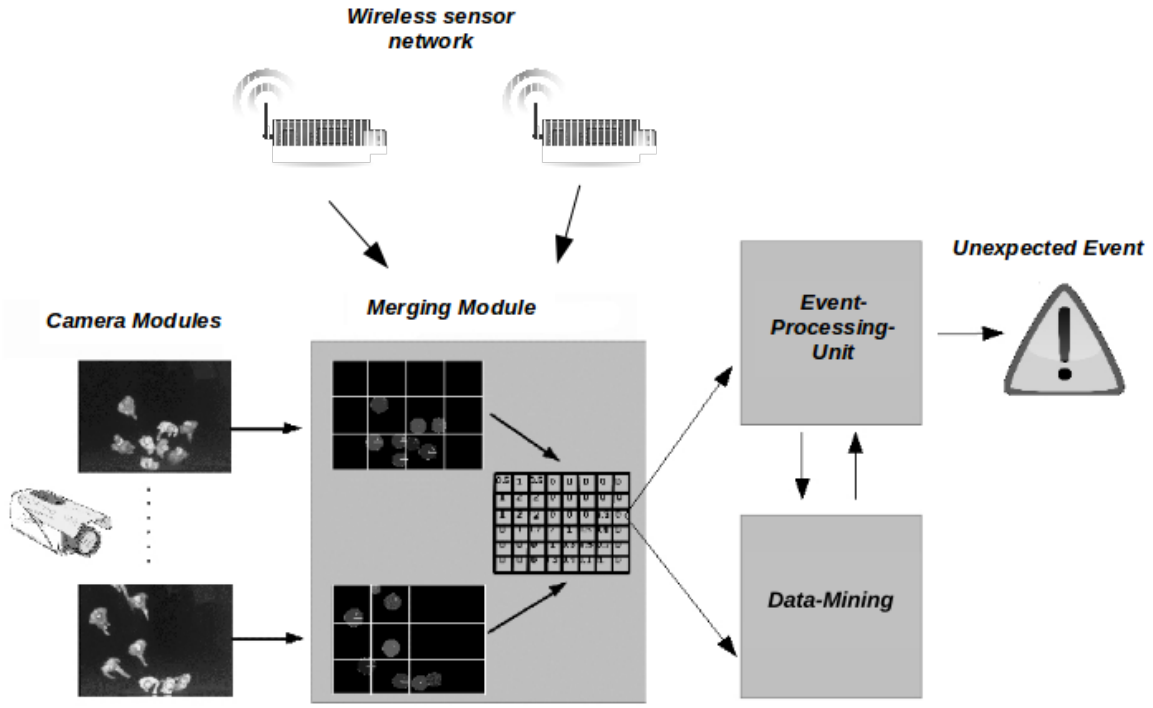


Abbildung 9: Gesamtsystem der Videoverarbeitung.

Die Abbildung 10 zeigt das Merging-Modul im Gesamtsystem. Ausgehend aus der vertikalen Position der Kamera, werden Menschen mit Kreisen approximiert. Aus diesem Grund gibt die Videoverarbeitungskomponente eine Liste der erkannten Personen, deren Position und Radien aus. Das Modul berechnet die Anzahl der Menschen pro Zelle der Dichtematrix aus dem Anteil der Fläche, die diese Personen in jeweils einem Grid verdecken, zu der Gesamtfläche der Zelle. Basierend auf den geometrischen Eigenschaften wurden analytische Formeln für diese Berechnungen entworfen.

Bisher wurden alle Tests mit einer von SAGEM gelieferten Kamera durchgeführt. Laut dem Szenarienkatalog, der im Arbeitspaket 2 zusammengestellt wurde, ist es geplant mehr als eine Kamera zu verwenden. Um eine globale Sicht auf die beobachteten Areale zu ermöglichen, wurde das Merging-Modul erweitert – es berechnet eine globale Dichtematrix aus mehreren Quellen. Da die Kamera-Knoten konfigurierbar sind und ein globales Koordinatensystem besitzen, müssen die Koordinaten der Menschen aus einzelnen Quellen nicht neu berechnet werden. Der für eine Kamera entwickelte Ansatz fürs Berechnen von diskreter Dichte aus Koordinaten und Radien der erkannten Menschen muss allerdings für die Flächen angepasst werden, da die unterschiedliche Quellen unterschiedliche Daten liefern. Wir gewichten jede Person, die in den sich überlappenden Regionen befindet abhängig von ihrer Position im Kamerabild: Je größer der Winkel zu der Person ist, desto kleiner geht sie in die Berechnung der Dichtematrix ein. Die Intuition dahinter ist die sinkende Genauigkeit von dem Menschenerkennungsalgorithmus an den Rändern des Kamerabildes.

Das Merging-Modul erlaubt es, nicht nur eine globale Sicht aus mehreren Kameras zu erstellen, sondern bietet die Möglichkeit, unterschiedliche Systemkomponenten miteinander zu verbinden, um aus der zusammengesetzten Information zusätzliches Wissen gewinnen zu können. Das Merging-Modul dient als eine Datenvorverarbeitungskomponente, sowie eine Schnittstelle zu der zentralen Event-Processing-Unit.

AP5.2.2 – Data-Mining-Strategien Das Data-Mining-Modul dient zur offline Datenanalyse und kann einerseits für die Parametrisierung der Regeln der Event-Processing-Unit und andererseits für die Erkennung von Mustern, Abhängigkeiten oder Assoziationen in aufgezeichneten Daten verwendet werden.

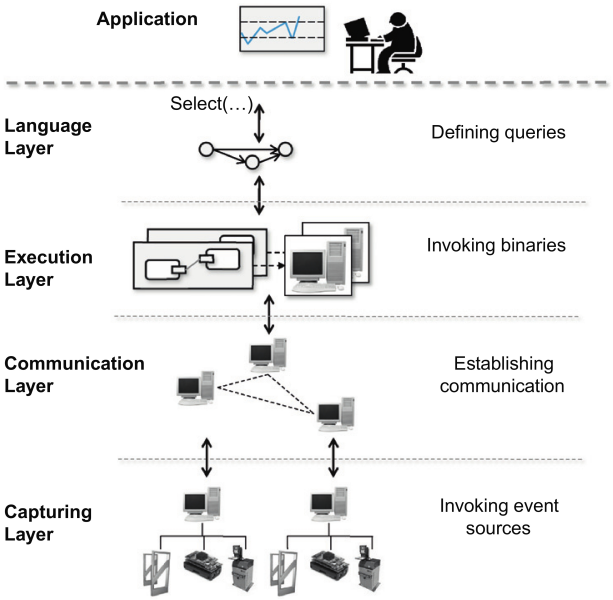


Abbildung 10: Architect Framework: Abstraktionsschichten eines eventbasierten Systems.

Die Idee hinter dem ersten Ansatz ist, die beobachteten Daten mit solchen externen Daten, wie z.B. Fluginformationen von Webseiten oder Flugplänen in Zusammenhang zu bringen. Wir schlagen mehrere Kategorien für die videobasierten und externen domainspezifischen Daten vor. Auf diesen Kategorien sollen Entscheidungsbäume gebildet werden. Der Ansatz findet anhand des Informationsgehaltes jeder Kategorie statistische Abhängigkeiten in Daten, falls solche existieren. Außerdem ist die Struktur des gefundenen Baums eine gute Visualisierung der Zusammenhänge und kann direkt in Regeln übersetzt werden.

Des Weiteren wurden Konzepte für die Vorhersage der Menschenverhaltens ausgearbeitet. Dieser Ansatz geht aus dem dynamischen Verhalten der Menschen hervor: Eine Menschenmenge wird als dynamisches System betrachtet, dessen Ausgabe (die Beobachtungen) die Bewegungen und die Form der Menge sind. Die Annahme ist, dass solch ein dynamisches System eine Reihe der Zustände besitzt und sich abhängig von diesen Zuständen verhält. Der Zustandwechsel erfolgt entsprechend den Übergangswahrscheinlichkeiten, die Zustände sind verborgen und können nicht direkt beobachtet werden. Da aber die Zustände das Verhalten des Systems bestimmen, kann man anhand der Beobachtungen des Systems die Zustandsübergenge dahinter approximieren – das System ist somit beschrieben. Sobald das Model für das System existiert, kann man ausgehend aus dem aktuellen Zustand des Systems den nächsten entsprechend den Übergangswahrscheinlichkeiten voraussagen. Die Abweichgung der Realität von der Schätzung identifiziert ungewöhnliches Verhalten.

Um die Beobachtungen des Systems als Input für eine Hidden Markov Model zu verwenden, wird ein Alphabet benötigt, die diese Beobachtungen kodiert. Es ist sinnvoll ein endliches und kompaktes Alphabet zu verwenden, um nicht durch die große Anzahl der zu approximierenden Parametern die Laufzeit der Algorithmen und die Qualität der Lösung zu beeinträchtigen. Es wurden zwei solche Alphabete entworfen: Das erste Alphabet kodiert Eigenschaften der Menschenmenge, basierend auf den Dichtematritzen, das zweite Bewegungen der Menschen. Beide Alphabete sind endlich und können direkt aus den Daten, die in der Event-Processing-Unit ankommen, berechnet werden. Das dichtebasierte Alphabet kodiert Schwankungen in der Grösse der Menschenansammlung, wobei die Ansammlung der Menschen über eine ”benachbarte“-Beziehung und Dichte derselben Ordnung gefunden wird. Das zweite Alphabet arbeitet mit Bewegungsrichtungen, die mit acht Himmelsrichtungen erst kodiert werden, dann – um die räumliche Komponente der Daten und die Abhängigkeiten zwischen den Zellen nicht

zu verlieren – mit Nachbarn verglichen werden. Die häufigsten Kombinationen bilden das Alphabet.

Das Modell kann durch zusätzliche Alphabete, die weitere Systemeigenschaften kodieren, erweitert werden.

AP5.2.3 – Ähnlichkeitsmaße Das in Zusammenarbeit mit Fraunhofer FOKUS entwickelte Datenmodell unterscheidet zwischen sogenannten People-Maps und Density-Maps. People-Maps sind für die Kameraausgabe entworfen worden und modellieren die Koordinaten und Radien gefundener Personen. Die Density-Maps sind Dichtematritzen für das Event-Processing-Unit. Die im Arbeitspaket 5.1.1. vorgestellte Methode für die Menschenerkennung verarbeitet die low-level Features und wendet Clustering schon in der niedrigen Aggregationsstufe an. Solche high-level Strukturen wie Dichtematritzen kodieren die Entfernungsinformation und können somit die Analyse der benachbarten Zellen in Kombination mit dichtebasiertem Clustering zusammenhängende Menschenmassen ähnlicher Dichte erkennen. Das Ähnlichkeitsmaß ist in dem Fall die arithmetische Differenz der Dichtewerte. Im Fall von People-Maps können daraus gewonnenen Trajektorien mit solchen Ähnlichkeitsmaßen für Kurven wie Frèchet-Distanz gruppiert werden. Infolge starker Datenaggregierung in den ersten Datenverarbeitunsstufen auf dem Sensorknoten und spezieller Datenformaten ist die Anwendung existierender Ähnlichkeitsmaße möglich.

AP5.3 – Umsetzung Wissensfusionierung

In SAFEST findet die Wissensfusionierung an mehreren Stellen statt. Wie in der Abbildung 9 dargestellt, werden voraggregierte Daten aus inhomogenen Quellen in dem sogenannten Merging-Modul zur Systemlaufzeit zusammengesetzt (AP 5.2.1). Das Data-Mining Modul aus der Abbildung 9 dient zur offline Analyse der voraggregierten Daten und wird für die Erkennung der Abhängigkeiten zur Regelherstellung und zur Parametrisierung existierender Regeln für das Event-Processing-Unit verwendet (AP 5.2.2). Konzepte für beide Module wurden in den Arbeitspaketen 5.3.1. und 5.3.2. erweitert und umgesetzt.

AP5.3.1 – Monitoring von Besucherströmen In diesem Arbeitspaket wurde das Konzept für die Fusionierung der Snapshot-Dichtematritzen, genannt Density-Maps, für die Verwendung mit mehreren Kameras erweitert und umgesetzt. Wie in AP 5.2.1. beschrieben, berechnet das Merging-Modul die Anzahl der Personen, die sich in jeweils einem Grid der globalen Dichtematrix befinden. Die Abbildung 11 visualisiert die Verarbeitungnsschritte innerhalb des Merging-Moduls als Aktivitätsdiagramm.

Das Merging-Modul empfängt von jedem Kameraknoten ein Stream von JSON-Objekten, die jeweils eine Liste der erkannten Personen und deren lokalen Positionen enthalten. Die Streams kommen asynchron bei dem Modul an und müssen, damit das globale Sicht an die überwachte Fläche korrekt berechnet wird, synchronisiert werden. Dafür verwenden wir die auf volle Sekunden gerundeten Zeitstempel eines jeden JSON-Objektes. Aus den synchronisierten Kameradaten werden lokale Dichtematritzen mit dem in dem AP 5.2.1. beschriebenen Ansatz berechnet.

Um komplexere Szenarien mit mehreren Kameras abzudecken wurde ein erweitertes Konzept implementiert. Die Herausforderung dabei ist es, das automatische Zusammenführen der Daten für alle möglichen Systemzusammensetzungen und -konfigurationen zu ermöglichen. Die Kameras können dabei in der horizontalen Ebene rotiert angebracht werden. Die Abbildung 12 veranschaulicht die Rotation der Kameras und zeigt eine 90° Drehung. Der Entwickelte Ansatz kann mit Kameradrehungen von 0°, 45°, 90° und 270° umgehen.

In dem Konfigurationsschritt aus der Abbilding 11 wird aus den Kamerapositionen, deren Höhen und Sichtwinkeln eine globale Sicht berechnet. Die globale Sicht ist eine leere Dichtematrix, in der für jede Zelle Identifikationsnummern der Kameras, die auf diese Zelle schauen, notiert sind. Ein Beispiel solcher automatisch zusammengestellten Matrix ist in der Abbildung 13 zu sehen.

Die Herausforderung dabei ist die automatische Erkennung von den Umrissen der globalen Sicht und sich überlappenden Kamerasichten. Die globale Sicht wird einmal bei der Installation des Systems berechnet und wird dann als Parameter für die Zusammensetzung der globalen Dichtematrix

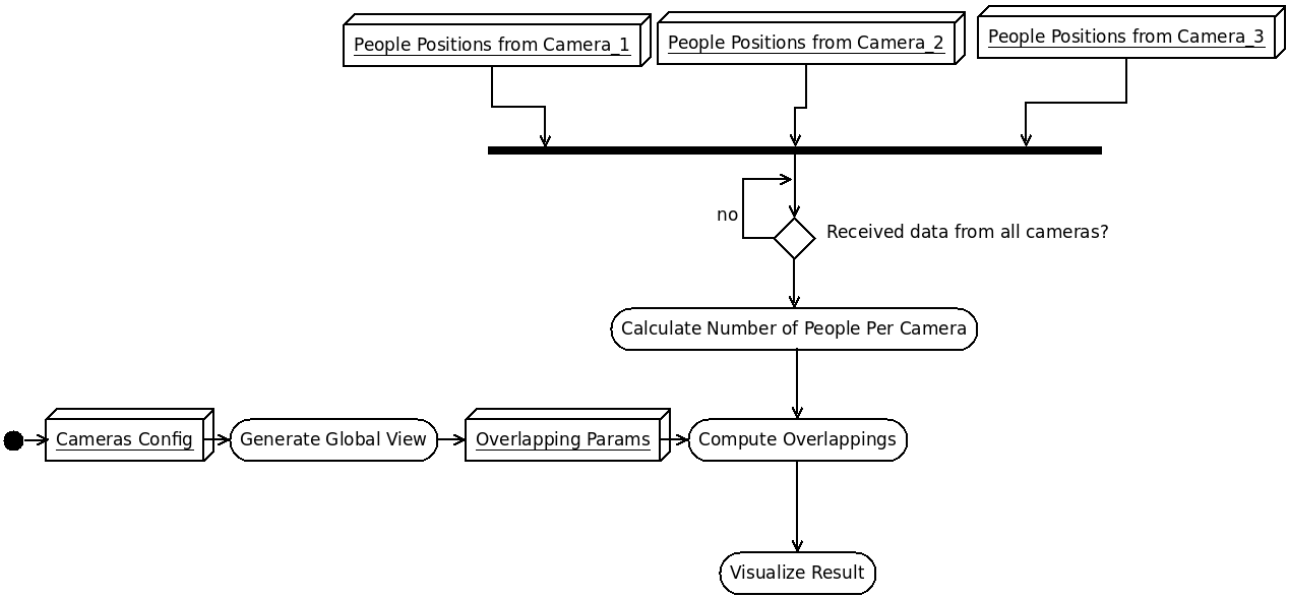


Abbildung 11: Umsetzung der Wissensfusionierung innerhalb des Merging-Moduls.

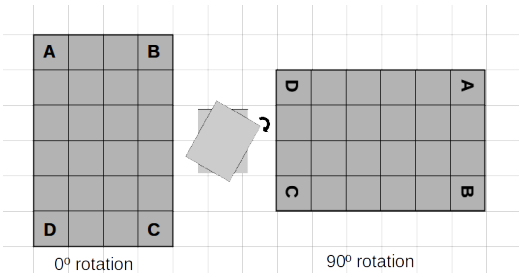


Abbildung 12: Veranschaulichung der Kamerarotationen.

verwendet. Die globale Dichtematrix wird einmal pro Sekunde aus den synchronisierten lokalen Dichtematritzen berechnet. Für die Zellen, die nur von einer Kamera gesehen werden, wird die Anzahl der gesehenen Personen direkt übernommen. Für die Zellen, für die die Sichten mehrerer Kameras sich überlappen, haben wir eine Gewichtungsfunktion implementiert. Die Funktion erlaubt es die Sichten unterschiedlicher Kameras unterschiedlich zu bewerten. Es ist möglich mehrere Konzepte für die Berechnung des Gewichtes zu verwenden. Derzeit folgt die Gewichtung der folgenden Intuition: Um die Personen nicht mehrfach zu zählen, wird die Summe der gesehen Personen durch die Anzahl der Kameras gemittelt. Eine Erweiterung der Funktion wäre die Kameras mehr zu gewichten, deren Zählergebnissen mehr getraut werden soll.

Die Implementierung erfolgte in Python und liefert eine globale Dichtematrix pro Sekunde, die als JSON-Objekt für die weitere Auswertung an die Complex-Event-Processing-Unit geschickt wird.

AP5.3.2 – Matching-Algorithmen Das Ziel des Arbeitspaketes ist die Konzepte für Data-Mining beschrieben im Dokument "Data-Mining Strategies" umzusetzen. Die Data-Mining Komponente aus der Abbildung 9 verfolgt zwei Ziele: Parametrisierung existierender Regeln für das Complex-Event-Processing-Unit und Datenanalyse für die Herstellung neuer Regeln. Beide Softwaremodule wurden in Python umgesetzt.

Zwei Datenmodelle wurden für die offline Analyse implementiert: Dichtematritzen, genannt Density-Maps und Bewegungsmatritzen, genannt Motion-Maps. Die Abbildung 14 visualisiert beide Konzepte. Die Density-Maps können direkt aus dem Merging-Modul exportiert werden. Für die Berechnung der Motion-Maps eine weitere Softwarekomponente wurde implementiert. Das Merging-Modul reicht

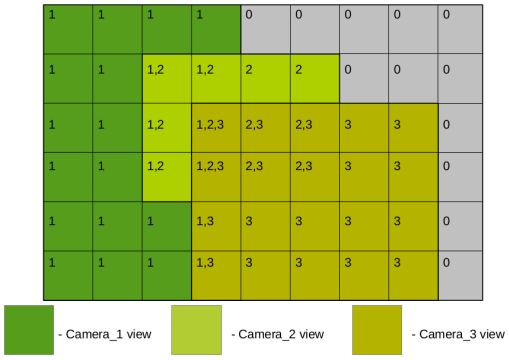


Abbildung 13: Veranschaulichung der globalen Sicht.

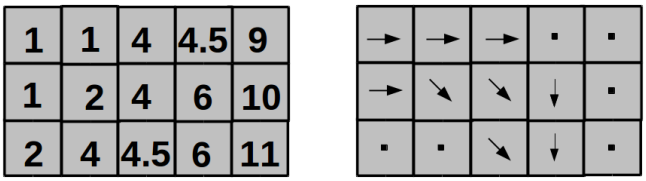


Abbildung 14: Veranschaulichung der Dichtematritzen (links) und Bewegungsmatritzen (rechts).

die Positionen der von den Kameraknoten detektierten Menschen an das Data-Mining-Modul weiter. Diese werden mittels Vektoraddition an die acht Himmelsrichtungen jeweils für eine Zelle des Grids abgebildet.

Die Dichtematritzen werden für die Parametrisierung existierender Regeln verwendet. Das Ziel ist, Datenbankabfragen an die langfristig gespeicherte Daten zu stellen, um die durchschnittliche Dichte pro ein vorgegebenes Areal innerhalb einer angefragten Zeit zu berechnen. Hierfür werden Daten in einer zellenbasierten Weise in PostgreSQL Datenbankmanagementsystem mit PostGIS Funktionalität für die Verarbeitung ortsbasierten Daten abgelegt. Zunächst werden von den Kameraknoten gelieferten JSON-Daten in die Tabelle "People Table" transformiert. Um komplizierte Joins für die Berechnung der Durchschnittsqueries zu vermeiden, wird das Raster-Template von PostGIS für die Darstellung der zellenbasierten Daten benutzt. Jeder Tabelleneintrag enthält ein Abbild von den gezählten Menschen innerhalb eines Frames in der kodierten Form: Informationen über das gesammte Gitter sind als Polygontyp (Dichte pro Zelle + Zellenindex) gespeichert. Es ist möglich mehrere Bänder (Raster in Raster) zu Speichern. Aktuell wird ein Band verwendet. Es werden solche PostGIS Funktionen wie ST_PixelAsPolygon, ST_Contains und ST_MakePolygon, die rasterbasiertde Daten als Geometrieobjekte umwandeln und verwalten, verwendet. Dadurch werden benötigte Areale in Form von Polygonen in der Datenbank gefunden. Der Durchschnittswert der Dichte wird dann in Python berechnet.

Um neue Regeln für das Complex-Event-Processing-Unit herstellen zu können, müssen zusammenhänge in den gesammelten Daten gefunden werden. Da Motion-Maps die Dynamik im Menschenverhalten beschreiben und gleichzeitig die Privatsphäre der einzelnen Menschen schützen, wuden diese für die weitere Analyse verwendet. Um das Model für das dynamische Menschenverhalten zu bilden, wurden Hidden-Markov-Modelle implementiert. Das bedeutet, dass wir nicht beobachtbare Verhalten hinter den Menschenbewegungen vermuten. Beobachtbares Verhalten wurde in Form von Sequenzen von Bewegungen abgebildet. Das gridbasierte Datenmodel erlaubt es ein Modell für ein Grid zu approximieren. Die größe des Grids is mit dem Vektoradditionsansatz skalierbar.

Ein Hidden-Markov-Modell wie es in SAFEST implementiert wurde ist in der Abbildung 15 prän-sentiert. In grün sind die Beobachtungen der Menschenbewegungen (jeweils eine der acht Himmelsrichtungen) dargestellt. Das nicht beobachtbare Verhalten ist durch die grauen Zustände des Hidden-Markov-Modells repräsentiert. Das Modell selbst besteht aus den Parametern für die Zustandsübergägne λ_i und durch die Wahrscheinlichkeiten α_j in dem aktuellen Zustand des Modells eine der Be-

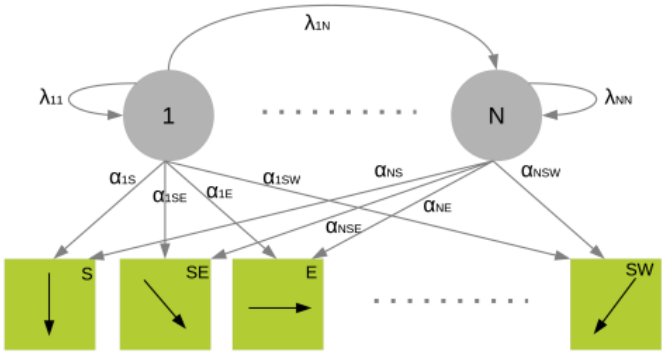


Abbildung 15: Hidden-Markov-Modell für die Bewegungsvorhersage.

wegungsrichtungen $\{S, SE, E, ..., SW\}$ zu beobachten. So ist es möglich mit dem bekannten Modell, eine Bewegungsrichtung vorherzusagen.

Um die Parameter des Modells approximieren (das Modell zu trainieren) zu können, wurde das Baum-Welch-Algorithmus implementiert. Die Validierung des Modells erfolgte mit dem Forward-Algorithmus. Es ist möglich die Anzahl der Zustände des Modells und die Länge des Beobachtungssequenz zu variieren. Das Modell wurde an den aufgezeichneten Videosequenzen für das Szenario "Blockierte Tür" trainiert. Das Modell beschreibt das normale Verhalten der Menschen, die durch eine nicht blockierte Tür durchgehen. Das Forward-Algorithmus berechnet den Schwellwert als den log-Likelihood $min(logP(O|HMM)|O^k \in \{O^0, ..., O^n\})$ für eine zu beobachtende Sequenz der Bewegungen $\{O^0, .., O^n\}$, ob das von diesem Modell produziert werden konnte. D.h. der Schwellwert als Ähnlichkeitsmaß bestimmt, ob eine Beobachtungssequenz normales Verhalten abbildet, und ist somit die Grundlage für eine neu gelernte Regel für das Complex-Event-Processing-Unit. Dieser Ansatz wurde an einem Szenario initial getestet und eignet sich somit der Herstellung neuer Regeln. Weitere Szenarien sind in Vorbereitung. Der Vorteil des implementierten Ansatzes ist, dass die verborgenen eventuell nicht intuitiven statistischen Eigenschaften zur Bildung des Schwellwertes für das abnormale Verhalten verwendet werden.

AP5.4 – Integration und Proof-of-Concept

Das Merging-Modul gilt nicht nur als eine Kameradaten fusionierende Komponente, sondern auch als eine Schnittstelle zum Alarmsystem. Es wurden zahlreiche Tests durchgeführt um das Zusammenspiel von drei Komponenten (Kamera-, Merging-, Alarm-Modul) zu testen. Es ist allerdings schwierig alle Tests zu automatisieren – der Grund ist das Fehlen des Ground Truth für die Dichtematritzen. Die Umrechnung von Menschenpositionen zu Dichtematritzen wurde daher basierend auf geometrischen Eigenschaften des Kreises geprüft: ein Mensch kann sich direkt auf der Grenze der einzelnen Blöcke befinden, d.h. ein Grid kann ein Kreis in 16 mögliche Formen teilen. Alle diese Fälle wurden rekonstruiert und überprüft.

Wie im Arbeitspaket 4.4.1 beschrieben, wurde das Zusammenspiel aller Komponenten vom Sensorknoten über das Merging-Modul zur zentralen Event-Processing- und Alarmkomponente ausführlich getestet und während der Live-Demos am 17.11.2013 sowie am 18.09.2015 erfolgreich vorgestellt.

2.1.6 AP6 – Sicherheitsmodell für Geräte von Endanwendern

AP6.5 – Sicherheitsmodell für Geräte von Endanwendern

Es wurde eine Sicherheitsanalyse bezüglich der Einbindung von externen Smartphones in das SAFEST-System durchgeführt. Der vorgeschlagene Ansatz führt zu keiner Erhöhung des Sicherheitsrisikos, da die Endanwender in den bereits existierenden Netzen integriert werden. Entsprechend greifen bestehende Sicherheitsverfahren. Weiterhin wird für die Einbindung der Endanwender kein neuer Software-Client benötigt, sondern auf bestehende Web-Clients zurückgegriffen.

2.1.7 AP7 – Demonstrator, Einsatzerprobung und Evaluation

AP7.1 – Einsatzbeschreibung

Zusammen mit den Partnern "FBS" und "SAGEM" wurde ein detaillierter Szenarienkatalog erstellt. Dieser enthält eine Auflistung von Experimenten, welche die Grundlage für spätere Feldtests gebildet haben. Die Beschreibungen der einzelnen Experimente umfassen sämtliche technischen wie nicht-technischen Parameter wie eingesetzte Hard- und Software, Szenariobeschreibung, Durchführungsort, Dauer, involvierte Partner sowie erwartete Resultate.

AP7.2 – Evaluations-Rahmenwerk

AP7.2.1 – Entwurf und Umsetzung Das Ziel des Arbeitspakets ist ein Werkzeug herzustellen, dass der Evaluierung des Gesamtsystems dient. Das Merging-Modul liegt in dem Gesamtsystem zentral und hat somit einen Überblick: Einerseits sieht es die preaggregierten Zwischenergebnisse der unterschiedlichen Sensoren, andererseits liefert es die zusammengesetzten Daten über die Gesamtsituation des zu beobachtenden Areals für die endgültige Analyse. Es wurde entschieden, dem Merging-Modul die Aufgabe der Visualisierung der Zwischenstufen der Datenaggregation zu übergeben. Das letzte Arbeitsschritt in dem Aktivitätsdiagramm in der Abbildung 11 ist die Visualisierung des Ergebnisses.

Die Abbildung 16 zeigt ein Screenshot der Visualisierung, dass von dem Merging-Modul zur Systemlaufzeit produziert wird. In den beiden unteren Bildern sind jeweils die Sicht von zwei an dem Setup beteiligten Kameraknoten zu sehen. Farbig sind die von den Knoten detektierte Personen dargestellt. Die Kameraknoten übertragen für jeweils eine Person ihre Position und die Größe and das Merging-Modul, das daraus die beiden oben dargestellten Kreise für jeweils eine Person in dem Kamerabild produziert. Außerdem wird für jede aggregierte Kamerasicht eine Griddarstellung auf die Kreisedarstellung drübergelegt. Das zusammengefügte Ergebnis von Dichteschätzung – die globale Sicht – ist in dem mittleren Bild dargestellt. Die einzelnen Personen aus den einzelnen Kamerasichten werden zu einer globalen Dichtematrix. Die grüne Linie stellt die Position und die Grenzen der rechten Kamera bezüglich der linken dar. Die Anzahl der Personen in jedem Fenster rechts zeigt die Summe der Menschen in dem Bild. Die Visualisierung wird mit synchronisierten Kamerasichten aktualisiert.

Mit dieser Visualisierungstechnik können Fehler auf jeder Datenverarbeitungsstufe ausgewertet werden. Die in der Abbidung 16 unten plazierten Bilder zeigen das Originalbild jeder Kamera. Falls die Menschen nicht erkannt wurden, werden sie nicht farbig markiert und zählen nicht in die Gesamtsumme des Zählergebnisses. Der eventuelle Unterschied zwischen der Kreisdarstellung in den oben dargestellten Fenstern der Abbildung 16 weist auf einen Fehler in der Approximation der Menschen mit Kreisen hin. Das mittlere Fenster zeigt intuitiv das Gesamtresultat.

Da die Visualisierung an das Merging-Modul gekoppelt ist, muss es nicht zusätzlich parametrisiert oder eingerichtet werden. Es ist als ein Python-Softwaremodul implementiert und kann zusammen mit dem Merging-Modul ausgeführt werden. Diese Umsetzung wurde während der ILA Airshow in Berlin Schönefeld in Mai 2014 getestet und Live debugged. Nach der Korrektur der Fehler, wurde die Software zur Live Auswertung von dem Merging-Modul selbst verwendet.

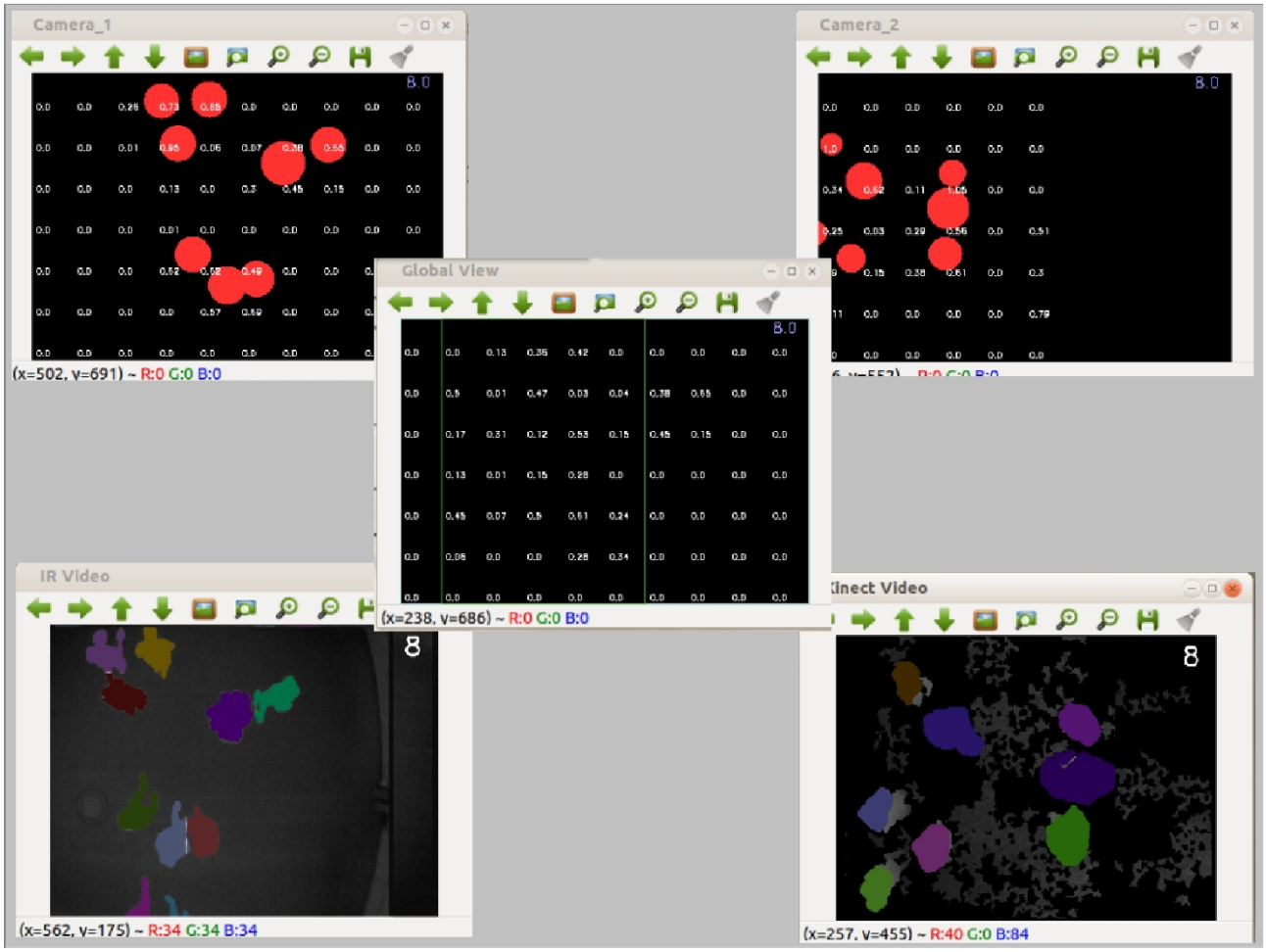


Abbildung 16: Snapshot der Visualisierungssoftware mit zwei Kameras im Set-up.

AP7.3 – Demonstrator

AP7.3.1 – Installation und Test Wissensfusionierung (Anteil Monitoring) Das Merging-Modul, das für die Wissensfusionierung und Evaluierung der Zwischenergebnisse verwendet wurde, wurde für eine leichtere Parametrisierung angepasst und mit verfügbarer Hardware vorläufig getestet und für die Integration in das Gesamtsystem vorbereitet.

AP7.3.2 – Feldtests Vier Szenarien für vier mögliche Set-ups des Demonstrators wurden im Rahmen der Vorbereitung des interen Projekttreffens, das an der Freien Universität Berlin am 26.-28. November 2014 stattgefunden hat. Zusammen mit Projektpartnern daviko GmbH, Fraunhofer FOKUS und SAGEM wurden diese Szenarien aufgebaut und getestet. Jeder Datenverarbeitungsschritt von Preprocessing auf den Knoten über die Wissensfusionierung bis Complex-Event-Processing und Alarmkomponente wurde mit echter Hardware (Smart Node, IR-Kamera, Kinect-Kamera, FIT_PC mit OLSR, Linux Laptop mit Netzwerkanalyseprogramm, MacBook mit REDIS, IPad mit Event-Monitor) ausgeführt, Schnittstellen und Datenübertragung wurden getestet. Als erstes wurde die Menschenerkennungssoftware für eine IR-Kamera auf dem Smart Node umgesetzt und die Datenübertragung über das OLSR Netzwerk überprüft. Als weiteres wurde das Merging-Modul in den Smart Node integriert und die Datenübertragung zwischen Videoverarbeitung, Datenfusionierung und REDIS umgesetzt. Im weiterem Set-up wurde zusätzlich die Videoverarbeitung für eine Kinect-Kamera in den Smart Node integriert. Die Abbildung 17 zeigt den Aufbau des Systems für dieses Beispielszenario. Als letztes wurde ein weiterer Smart Node mit jeweils einer Kamera zum Set-up hinzugefügt. Somit wurde die Funkti-

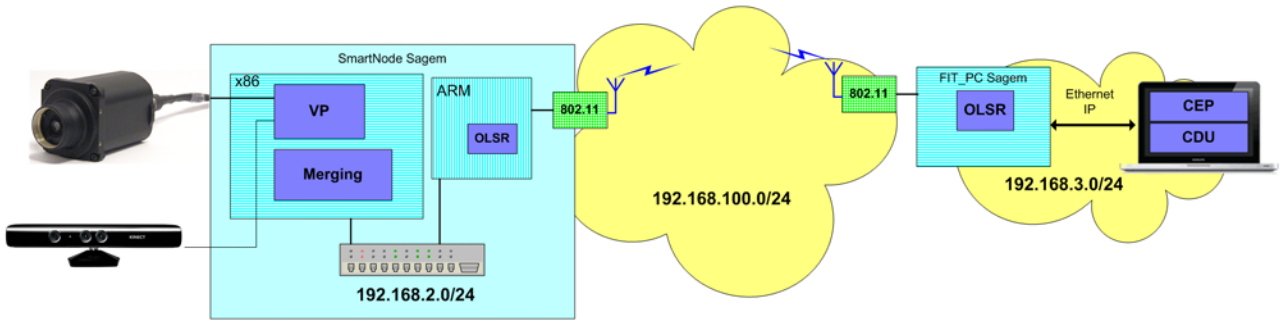


Abbildung 17: Beispielszenario für den Demonstrator.

onsfähigkeit des Gesamtsystems geprüft und bestätigt. Weitere Videoaufnahmen für die Evaluierung des Gesamtergebnisses wurden durchgeführt.

AP7.4 – Ergebnisse und Optimierung

AP7.4.1 – Auswertung und Optimierung der Wissensfusionierung (Anteil Monitoring) Während der ILA Airshow im Mai 2014 und des Integrationstreffens im November 2014 mit mehreren Kameras aufgenommene Echtdaten der Menschenströme wurden für die Evaluierung des Merging-Moduls verwendet. Die vorläufigen Ergebnisse zeigen, dass das entworfene Konzept sich für das Gesamtergebnis eignet. Wie die vorläufigen Ergebnisse des AP 7.4.2 zeigen, muss die Gewichtsfunktion aus AP 5.3.1. optimiert werden, indem die Ergebnisse einzelner Knoten abhängig von dem aktuellen Set-up unterschiedlich behandelt werden.

AP7.4.2 – Auswertung und Optimierung Menschenmengen erkennen und Geländeüberwachung Für die Auswertung der Menschenmengenerkennung wurden alle im Laufe des Projektes gesammelten Daten, das histogrammbasierte und MOG-Algorithmus für Infrarot- und histogrambasiertes Algorithmus für Kinect-Kameras verwendet. Das vorläufige Ergebnis zeigt, dass im Gegensatz zu den Infrarotkameras, die Kinectkameras sich für die Menschenerkennung nur unter bestimmten Bedingungen eignen. Bei gleichen Bedingungen weisen die Infrarotkameras mit getesteten Algorithmen für die Menschenerkennung einen relativen Fehler von 4% bis 6%, wobei der Fehler von Kinect bei rund 20% liegt. Wird die Höhenanforderung für die Platzierung der Kinect-Kamers erfüllt, sinkt der Fehler erheblich. Aktuell werden weitere Daten gesammelt, um vollständige Evaluierung zu ermöglichen.

2.1.8 AP8 – Projektkoordination, -dissemination und Berichterstattung

AP8.1 – Externe Workshops

Während der Projektlaufzeit wurden u.a. die folgenden Konferenzen und Workshops co-organisiert:

1. 1st ACM International Workshop on Sensor-Enhanced Safety and Security in Public Spaces (SESP 2012), im Zusammenhang mit der ACM MoiHoc
2. 5th International Workshop on Peer-to-peer computing and Online Social neTworking (HotPOST), im Rahmen der Konferenz IEEE ICDCS 2013
3. 6th International Workshop on OMNeT++, im Zusammenhang mit der SIMUTools 2013
4. Begleitveranstaltungen zur IETF-87
5. MANIAC Challenge 2013
6. Dagstuhl Seminar zu kritischen Infrastrukturen 2013

7. 21st IEEE International Conference on Network Protocols (ICNP), 2013
8. 6th International Workshop on Peer-to-peer computing and Online Social neTworking (HotPOST), im Rahmen der Konferenz IEEE ICDCS 2014
9. 39th IEEE Conference on Local Computer Networks (LCN)
10. 1st OMNeT++ Community Summit, 2014
11. IEEE/ACM International Symposium on Quality and Service (IWQoS), im Rahmen der ACM FCRC 2015
12. 2nd ACM Conference on Information-Centric Networking (ICN), 2015
13. Workshop „Überwachung: Technische Innovationen und ihre gesellschaftlichen Auswirkungen“

AP8.2 – Verbreitung

Das Projekt SAFEST wurde während der Projektlaufzeit auf einer Vielzahl von Messen und Konferenzen durch die Freie Universität Berlin präsentiert. Die folgende Liste zeigt eine Auswahl an Beteiligungen:

IETF 89, London Im Rahmen der IETF 89 wurde die Interoperabilität von RIOT mit diversen anderen Systemen getestet. Dies geschah im Rahmen des *IETF 6TiSCH Plugfest* sowie des *ETSI CoAP 4 Plugtest*.

CeBIT, Hannover SAFEST wurde öffentlichwirksam auf der CeBIT 2014 durch Projektmitarbeiter der FU Berlin, der HAW Hamburg sowie von INRIA auf dem Gemeinschaftsstand der Frauenhofer Gesellschaft vorgestellt. Das Expontant stand unter der Überschrift „Zivile Sicherheit mit smarten Technologien“. Die Besucher das kamerabasierte Erfassen von Menschenströmen sowie ein multi-hop Netzwerk aus Sensorknoten live demonstriert.

LinuxTag, Berlin Der LinuxTag ist europaweit die größte Messe zum Thema Open-Source-Software mit dem Fokus Linux. Wir haben das in SAFEST entwickelte Betriebssystem RIOT demonstriert. Es wurde eine erweiterte Version des auf der CeBIT präsentierten multi-hop Netzwerks aus Sensorknoten gezeigt.

ILA, Berlin Projektmitarbeiter der FU Berlin und der daviko GmbH haben auf der *ILA Berlin Air Show* am Flughafen Schönefeld im Mai 2014 die Menschenerkennungssoftware im Feldtest erprobt. Die Teilnahme wurde durch den Projektpartner FBB ermöglicht. Durch den Einsatz wurde die Implementierung getestet. Es wurden außerdem Aufnahmen von Menschenströmen unter realistischen Bedingungen für spätere Validierungen gemacht.

IoT Week, London Projektmitarbeiter der FU Berlin haben am Hackathon der IoT Week teilgenommen. Mit Software-Elementen aus SAFEST wurden dabei 2 Preise gewonnen: der erste Preis der *Connectivity Challenge* so wie der mit 1.000 EUR dotierte Gesamtpreis als *Best Solution Gold Winner*.

IETF 90, Toronto Auf dem an das IETF-Treffen angegliederten Veranstaltung Bits-N-Bytes wurden die in SAFEST entwickelten Netzwerkeigenschaften von RIOT mehr als 600 Besuchern demonstriert. Zusätzlich haben Projektmitarbeiter von der FU Berlin sowie von INRIA mit RIOT am LLN Plugfest teilgenommen.

FIT IoT-LAB Opening, Grenoble RIOT wurde sowohl Forschern als auch Industrievertretern als eines der Standardbetriebssysteme für das neu eingeweihte, international renommierte Testbed *IoT-LAB* vorgestellt.

Embedded World, Nürnberg Eine Demo aus SAFEST Software-Komponenten und RIOT wurde auf der weltgrößten Fachmesse für eingebettete Systeme präsentiert.

RIOT Hack'n'Ack Initiiert durch die HAW Hamburg und die FU Berlin existiert seit November 2014 ein monatliches sozialintegratives Arbeitstreffen, an jedem letzten Dienstag im Monat. Die beiden Standorte Hamburg/Berlin sind über eine Videokonferenz miteinander verbunden. Das *Hack'n'ACK* dient dazu, offene Fragestellungen zu erörtern, Fehler zu beheben sowie Programmcode anderer zu testen und für das Gesamtprojekt freizugeben.

Zusätzlich zu den genannten Veranstaltungen wurden Egebnisse aus dem Projekt SAFEST u.a. auf den folgenden Veranstaltungen präsentiert:

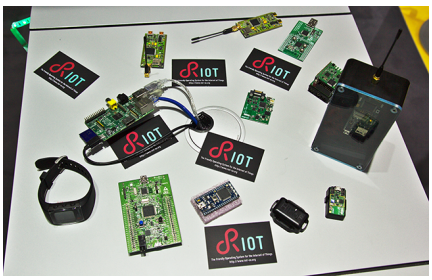
1. Lange Nacht der Wissenschaften
2. PayPal E-Commerce Meetup: „Internte of Things & Wearables“
3. GET-D Workshops in Berlin und San Francisco
4. First ACM Confernece on Information Centric Networking
5. First International Conference on Safety and Security in Internet of Things
6. Internationale Tagung „Trust in Times of (In-)Security – On the Relationship between the Phenomena of Security and Trust“, Universität Trier
7. 11th International ISCRAM Conference
8. BMBF Innovationsforum, Café Moskau
9. IETF93, Prag
10. W3C Workshop on the Web of Things, Berlin
11. ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Berlin
12. 5th Fraunhofer FOKUS Media Web Symposium, Berlin

Hervorzuheben unter den genannten Aktivitäten ist der publikumswirksame Auftritt auf der CeBIT 2014, der weltgrößten IT-Messe. Hier konnte einem breiten Fach- sowie Laufpublikum die technischen sowie soziologischem Hintergründe von SAFEST nahe gebracht werden. Aus auf der Messe konnten nachhaltige Kontakte geknüpft werden, auf welchem unter anderem der Messeauftritt von RIOT auf der Embededded World 2015 basieren wird.

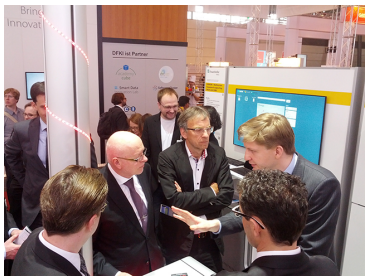
Ebenfalls ausgesprochen wichtig sind die kontinuierlichen Interoperabilitätstests im Rahmen der IETF-Treffen. Diese Veranstaltungen erlauben es den SAFEST-Projektpartnern, ihre Implementierungen der Netzwerkprotokolle mit den Implementierungen Dritter zu testen. An diesen Treffen nehmen sowohl Industrie- als auch Forschungsvertreter teil. Dies stellt sicher, dass die in SAFEST entwickelten Lösungen auch mit Lösungen Dritter kompatibel sind, wodurch die praktische Nutzbarkeit der Lösungen aus SAFEST gefördert wird.

Die technischen Innovationen von SAFEST haben zudem zu den Besuchen von Dritten an der Freien Universität Berlin geführt. In diesem Zusammenhang wurden kleinere Workshops durchgeführt:

(a) Präsentationsflächen von SAFEST

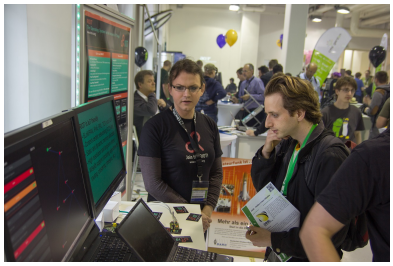


(b) Exponatstisch mit Multi-Hop-Netzwerk



(c) SAFEST-Mitarbeiter im Gespräch mit Kommunalpolitikern

Abbildung 18: Zivile Sicherheit mit smarten Technologien: SAFEST auf der CeBIT 2014



(a) Diskussionen auf dem LinuxTag

(b) Kinder experimentieren auf der Langen Nacht der Wissenschaften

(c) RIOT-Demo auf der IETF

Abbildung 19: Demonstration von SAFEST-Ergebnissen auf weiteren nationalen und internationalen Veranstaltungen im Jahr 2014

1. UDOO, Kickstarter-Projekt auf der Basis eines Microcontrollers, Mai 2014
2. ELL-i, Open-Source-Hardware für intelligentes Power-over-Ethernet, Oktober 2014
3. OneLab/Timur Friedman, Europäisches Testbed für Computernetze, Dezember 2014
4. RIOT Network Stack Task-Force workshop, February 2015

2.2 Weitere Ergebnisse

2.2.1 Auszeichnungen

1. Matthias Wählisch: Erster Preis für herausragende Leistungen zum Internet der Dinge und seiner industriellen Verwertbarkeit auf dem Forum „Junge Spitzenforscher“ Stiftung Industrieforschung
2. Cenk Gündogan und Lennart Dührsen gewinnen *Cisco Challenge: Best Use of Cisco Technology*, Internet of Things World Europe Hackathon
3. Hauke Petersen und Christian Mehlis: erster Platz *Connectivity Challenge* auf der IoT Week, London
4. Hauke Petersen und Christian Mehlis: erster Platz *Best Solution Gold Winner* auf der IoT Week, London
5. Matthias Wählisch: Reisestipendium für die für die 34th International Conference on Distributed Computing Systems (ICDCS)
6. Martine Lenders, Philipp Rosenkranz: Reisestipendium für die 13th International Conference on Mobile Systems, Applications, and Services (MobiSys)

7. Matthias Wählisch: erhielt die höchste Auszeichnung der IEEE Consumer Electronics Society für das Jahresbeste Paper „A Temporally Scalable Video Codec and its Applications to a Video Conferencing System with Dynamic Network Adaption for Mobiles“

2.2.2 Pressemitteilungen/-spiegel

Es wurden mehrere Newsletter-Beiträge und Pressemitteilungen herausgegeben.

Insbesondere die Pressemitteilung wurde von mehren Online-Portalen aufgegriffen wurde. Hervorzuheben ist das Radio-Interview *Safest – Neue Sicherheit für Menschenmengen?*, welches in der Sendung *Logo – Das Wissenschaftsmagazin* in NDR Info am 14.03.2014 ausgestrahlt wurde.

Weiterhin wurden die wissenschaftlchen Arbeiten der Projektmitarbeiter in den folgenden internationalen Nachrichtenbeiträgen diskutiert:

1. *How the Internet of Things could become a critical part of disaster response*, www.itworld.com, July 22, 2014

2. *How the Internet of Things Could Aid Disaster Response*, shlasdot.org, July 24, 2014

2.3 Voraussichtlicher Nutzen und Verwertbarkeit

Durch die Beiträge der einzelnen Arbeitsgruppen der FU Berlin wurde sowohl ein soziologischer als auch technischer Mehrgewinn erzielt. Die verschiedenen soziologischen Studien haben geholfen, die Wahrnehmung und Akzeptanz von Sicherheitslösungen erheblich besser zu beurteilen. Dabei hat sich gezeigt, dass die Akzeptanz von Fragen der Usability abgegrenzt werden müssen, da Akzeptanz ein multifaktorielles Konstrukt darstellt. Ebenfalls ist die Sorge vor dem Eingriff in die Privatsphäre nur einer von mehreren Aspekten, die die Bevölkerung skeptisch gegenüber technischen Sicherheitslösungen sieht. Insofern wurde mit den inhärenten Schutz der Privatsphäre in den von SAFEST entwickelten Lösungen, einschließlich dem expliziten Einsatz offener Lösungen der richtige Ansatzpunkt verfolgt.

Eines der Kernergebnisse von SAFEST, das offene Betriebssystem RIOT, wurde bereits innerhalb des Projektzeitraums von mehreren Dritten aufgegriffen. Berücksichtigt man den kontinuierlichen Anstieg der Entwicklergemeinschaft kann legitimerweise davon ausgegangen werden, dass auch nach Projektende eine nachhaltige Verwertung dieses Projektergebnisses sichergestellt ist. RIOT sollte dabei als eine generische Software-Plattform für zukünftige (technische) Lösungen für die zivile Sicherheit im Bereich der eingebetteten Geräte verstanden werden. Das Umfeld der eingebetteten Geräte ist von besonderer Bedeutung, da dem Internet der Dinge zukünftig eine erheblich stärkere Durchdringung prognostiziert wird.

Die initialen Ergebnisse aus SAFEST haben gezeigt, dass neuartige Netzarchitekturen notwendig sind, um sowohl den geringen Ressourcenanforderungen der Geräte als auch dem fehleranfälligen Medium Luft gerecht zu werden. Anderfalls lassen sich die im Bereich der zivilen Sicherheit hohen Anforderungen nach Robustheit und effizienter Datenverteilung nicht erfüllen. In SAFEST wurden deswegen informationszentrische Ansätze einbezogen, die ein inhärentes Zwischenspeichern (*Caching*) der Daten innerhalb des Netzes erlauben. Diese ersten Ideen sollen in dem Projekt I3 weiter ausgebaut werden.

Neben der wissenschaftlich-technischen Verwertbarkeit hatte SAFEST auch direkten Einfluss auf die Lehre. Im Rahmen des Projekts sind mehrere Abschlussarbeiten entstanden, in denen die Studenten ihr Fachwissen im Bereich der zivilen Sicherheit intensiviert haben. Darüber hinaus wurden langfristige Lehrveranstaltungen im Bereich der Software-Entwicklung und des sozio-technischen Zusammenspiels erweitert bzw. eingeführt.

2.4 Fortschritte auf dem Gebiet des Vorhabens

Nach dem Kenntnisstand zum Ende des Forschungsvorhabens SAFEST wurden anderweitig keine Ergebnisse veröffentlicht, die grundlegende Projektziele vorwegnehmen bzw. überflüssig machen. Vielmehr hat SAFEST mit seinen Leuchtturm-Ergebnissen dem IoT-Betriebssystem RIOT und dem

verteilten Programmiersystem CAF zwei deutlich über das Projekt hinausweisende Open-Source-Produkte hervorgebracht, welche inzwischen weltweite Sichtbarkeit und Anerkennung gefunden haben.

Weiterhin haben die durchgeführten soziologischen Studien den empirischen Datenbestand in der zivilen Sicherheitsforschung erheblich erweitert. Die Ergebnisse wurden sowohl national als auch international diskutiert und fanden jeweils ausgesprochen positive Resonanz.

Die grundlegende Bedeutung der von der Freien Universität Berlin erarbeiten Ergebnisse zeigt sich u.a. auch darin, dass Teile der Ergebnisse in den internationalen Standardisierungsprozess wirken. So werden Verbesserungen im klassischen IoT-Routing für das Protokoll RPL in der IETF diskutiert. Ebenfalls stellten die Arbeiten zu den informationszentrischen Netzen eine Basis für mehrere Folgearbeiten in der Fachgemeinschaft dar.

2.5 Wissenschaftliche Veröffentlichungen im Projektzeitraum

[1] P. Kietzmann, M. Landsmann, T. C. Schmidt, H. Petersen, M. Lenders, and M. Wählisch, "Leistungsmessung eines modularen Netzwerk-Stacks für das IoT-Betriebssystem RIOT," in *Proc. of the 14. GI/ITG KuVS Fachgespräch Sensornetze (FGSN2015).* Erlangen-Nürnberg, Germany: Friedrich-Alexander-Universität Erlangen-Nürnberg, Dept. of Computer Science, Sep 2015, pp. 19–22.

[2] E. Baccelli, A. Danilkina, S. Müller, A. Voisard, and M. Wählisch, "Privacy-preserving crowd incident detection: A holistic experimental approach," in *Proc. of ACM SIGSPATIAL Workshop on the Use of GIS in Emergency Management (EM-GIS-2015)*, 2015.

[3] S. Wölke, T. C. Schmidt, S. Meiling, and M. Wählisch, "Dynamic Cross-Domain Group Communication in Hybrid Multicast Networks," in *5th IEEE Int. Conf. on Consumer Electronics - Berlin (ICCE-Berlin'15).* Piscataway, NJ, USA: IEEE Press, Sep. 2015, pp. 185–189.

[4] S. Al-Sheikh, M. Wählisch, and T. C. Schmidt, "Revisiting Countermeasures Against NDN Interest Flooding," in *2nd ACM Conference on Information-Centric Networking (ICN 2015), Poster Session.* New York: ACM, Oct. 2015, pp. 195–196.

[5] T. C. Schmidt, S. Wölke, N. Berg, and M. Wählisch, "Partial Adaptive Name Information in ICN: PANINI Routing Limits FIB Table Sizes," in *2nd ACM Conference on Information-Centric Networking (ICN 2015), Poster Session.* New York: ACM, Oct. 2015, pp. 193–194.

[6] G. Pellegrino, C. Rossow, F. J. Ryba, T. C. Schmidt, and M. Wählisch, "Cashing out the Great Cannon? On Browser-Based DDoS Attacks and Economics," in *Proc. of 9th USENIX Security Workshop on Offensive Technologies (WOOT).* Berkeley, CA, USA: USENIX Assoc., 2015, pp. 1–8.

[7] H. Petersen, E. Baccelli, M. Wählisch, T. C. Schmidt, and J. Schiller, "The Role of the Internet of Things in Network Resilience," in *Internet of Things. IoT Infrastructures. First International Summit, IoT360 2014, Revised Selected Papers, Part II*, ser. LNICST, vol. 151. Berlin, Heidelberg: Springer, 2015, pp. 283–296.

[8] F. J. Ryba, M. Orlinski, M. Wählisch, C. Rossow, and T. C. Schmidt, "Amplification and DRDoS Attack Defense – A Survey and New Perspectives," Open Archive: arXiv.org, Technical Report arXiv:1505.07892, June 2015. [Online]. Available: http://arxiv.org/abs/1505.07892

[9] T. Markmann, T. C. Schmidt, and M. Wählisch, "Federated End-to-End Authentication for the Constrained Internet of Things using IBC and ECC," in *Proc. of ACM SIGCOMM, Poster Session.* New York: ACM, August 2015, pp. 603–604. [Online]. Available: http://dx.doi.org/10.1145/2785956.2790021

[10] H. Petersen, M. Lenders, M. Wählisch, O. Hahm, and E. Baccelli, "Old Wine in New Skins? Revisiting the Software Architecture for IP Network Stacks on Constrained IoT Devices," in *1st Int. Workshop on IoT Challenges in Mobile and Industrial Systems (IoT-Sys15).* Florence, Italy: ACM, May 2015.

[11] R. Hiesgen, D. Charousset, T. C. Schmidt, and M. Wählisch, "Programming Actors for the Internet of Things," *Ercim News*, vol. 101, pp. 25–26, April 2015. [Online]. Available: http://ercim-news.ercim.eu/en101/special/programming-actors-for-the-internet-of-things

[12] T. C. Schmidt, M. Wählisch, R. Koodli, G. Fairhurst, and D. Liu, "Multicast Listener Extensions for Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6) Fast Handovers," RFC Editor, RFC 7411, November 2014. [Online]. Available: http://tools.ietf.org/html/rfc7411

[13] A. Förster, C. Sommer, T. Steinbach, and M. Wählisch, Eds., *Proceedings of the 1st OMNeT++ Community Summit, Hamburg, Germany, September 2, 2014*, no. arXiv:1409.0093. Open Archive: arXiv.org, 2014. [Online]. Available: http://arxiv.org/html/1409.0093

[14] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild," in *Proc. of 1st ACM Conf. on Information-Centric Networking (ICN-2014).* New York: ACM, September 2014, pp. 77–86. [Online]. Available: http://dx.doi.org/10.1145/2660129.2660144

[15] E. Baccelli, O. Hahm, and M. Wählisch, "Spontaneous Wireless Networking to Counter Pervasive Monitoring," in *Proc. of W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)*, 2014. [Online]. Available: https://www.w3.org/2014/strint/papers/26.pdf

[16] F. Jäger, T. C. Schmidt, and M. Wählisch, "How Dia-Shows Turn Into Video Flows: Adapting Scalable Video Communication to Heterogeneous Network Conditions in Real-Time," in *Proc. of the 39th IEEE Conference on Local Computer Networks (LCN).* Piscataway, NJ, USA: IEEE Press, Sep. 2014, pp. 218–226.

[17] H. Petersen, E. Baccelli, M. Wählisch, T. C. Schmidt, and J. Schiller, "The Role of the Internet of Things in Network Resilience," Open Archive: arXiv.org, Technical Report arXiv:1406.6614, June 2014. [Online]. Available: http://arxiv.org/abs/1406.6614

[18] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild," Open Archive: arXiv.org, Technical Report arXiv:1406.6608, June 2014. [Online]. Available: http://arxiv.org/abs/1406.6608

[19] T. C. Schmidt, S. Gao, H.-K. Zhang, and M. Wählisch, "Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains," RFC Editor, RFC 7287, June 2014. [Online]. Available: http://tools.ietf.org/html/rfc7287

[20] M. Vallentin, D. Charousset, T. C. Schmidt, V. Paxson, and M. Wählisch, "Native Actors: How to Scale Network Forensics," in *Proc. of ACM SIGCOMM, Demo Session.* New York: ACM, August 2014, pp. 141–142.

[21] T. C. Schmidt, S. Wölke, and M. Wählisch, "Peer my Proxy - A Performance Study of Peering Extensions for Multicast in Proxy Mobile IP Domains," in *Proc. of 7th IFIP Wireless and Mobile Networking Conference (WMNC 2014).* Piscataway, NJ, USA: IEEE Press, May 2014, pp. 1–8.

[22] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. C. Schmidt, and M. Wählisch, "ICN Research Challenges," IRTF, IRTF Internet Draft – work in progress 06, March 2016. [Online]. Available: http://tools.ietf.org/html/draft-irtf-icnrg-challenges

[23] O. Hahm, E. Baccelli, H. Petersen, M. Wählisch, and T. C. Schmidt, "Demonstration Abstract: Simply RIOT – Teaching and Experimental Research in the Internet of Things," in *Proc. of 13th ACM/IEEE Conference on Information Processing in Sensor Networks Demo Session (IPSN)*. Piscataway, NJ, USA: IEEE Press, April 2014.

[24] E. Baccelli, G. Bartl, A. Danilkina, V. Ebner, F. Gendry, C. Guettier, O. Hahm, U. Kriegel, G. Hege, M. Palkow, H. Pertersen, T. C. Schmidt, A. Voisard, M. Wählisch, and H. Ziegler, "Area & Perimeter Surveillance in SAFEST using Sensors and the Internet of Things," in *Workshop Interdisciplinaire sur la Sécurité Globale (WISG2014)*, Troyes, France, Jan. 2014. [Online]. Available: http://hal.inria.fr/hal-00944907

[25] G. Carle, J. Schiller, S. Uhlig, W. Willinger, and M. Wählisch, Eds., *The Critical Internet Infrastructure (Dagstuhl Seminar 13322)*, vol. 3, no. 8. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2013.

[26] E. Baccelli, F. Juraschek, O. Hahm, T. C. Schmidt, H. Will, and M. Wählisch, Eds., *Proceedings of the 3rd MANIAC Challenge, Berlin, Germany, July 27 - 28, 2013*, no. arXiv:1401.1163. Open Archive: arXiv.org, 2014. [Online]. Available: http://arxiv.org/html/1401.1163

[27] M. Wählisch, T. C. Schmidt, and S. Venaas, "A Common API for Transparent Hybrid Multicast," RFC Editor, RFC 7046, December 2013. [Online]. Available: http://tools.ietf.org/html/rfc7046

[28] E. Baccelli, F. Juraschek, O. Hahm, T. C. Schmidt, H. Will, and M. Wählisch, "The MANIAC Challenge at IETF 87," *the IETF Journal*, vol. 9, no. 2, pp. 27–29, Nov. 2013.

[29] D. Charousset, T. C. Schmidt, R. Hiesgen, and M. Wählisch, "Native Actors – A Scalable Software Platform for Distributed, Heterogeneous Environments (AGERE '13 paper)," in *Proc. of the 4rd ACM SIGPLAN Conference on Systems, Programming, and Applications (SPLASH '13), Poster Session*. New York, NY, USA: ACM, Oct. 2013.

[30] ——, "Native Actors – A Scalable Software Platform for Distributed, Heterogeneous Environments," in *Proc. of the 4rd ACM SIGPLAN Conference on Systems, Programming, and Applications (SPLASH '13), Workshop AGERE!* New York, NY, USA: ACM, Oct. 2013, pp. 87–96.

[31] T. C. Schmidt, M. Wählisch, D. Charousset, and S. Meiling, "On Name-based Group Communication: Challenges, Concepts, and Transparent Deployment," *Computer Communications*, vol. 36, no. 15–16, pp. 1657–1664, Sep–Oct 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2013.08.001

[32] N. Berg, S. Meiling, T. C. Schmidt, and M. Wählisch, "Untersuchungen zur Komplexität komponierter Netzwerkarchitekturen im Future Internet," in *Report 299, 7. GI/ITG Workshop Leistungs-, Zuverlässigkeits- und Verlässlichkeitsbewertung von Kommunikationsnetzen und verteilten Systemen (MMBnet13)*. Hamburg, Germany: Universität Hamburg, Dept. Informatik, Sep 2013, pp. 73–84.

[33] M. Wählisch, E. Baccelli, J. Schiller, A. Voisard, T. C. Schmidt, S. Pfennigschmidt, M. Palkow, U. Weigmann, and U. Hanewald, "Technische Dimensionen der Flughafensicherheit," *Crisis Prevention*, no. 1, pp. 15–16, Jan. 2013.

[34] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Lessons from the Past: Why Data-driven States Harm Future Information-Centric Networking," in *Proc. of IFIP Networking*. Piscataway, NJ, USA: IEEE Press, 2013. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6663520

[35] A. Ghodsi, B. Ohlmann, J. Ott, I. Solis, and M. Wählisch, Eds., *Information-centric networking – Ready for the real world? (Dagstuhl Seminar 12361)*, vol. 2, no. 9. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2013.

[36] E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, "RIOT OS: Towards an OS for the Internet of Things," in *Proc. of the 32nd IEEE INFOCOM. Poster.* Piscataway, NJ, USA: IEEE Press, 2013.

[37] M. Landsmann, H. Perrey, O. Ugus, M. Wählisch, and T. C. Schmidt, "Topology Authentication in RPL," in *Proc. of the 32nd IEEE INFOCOM. Poster.* Piscataway, NJ, USA: IEEE Press, Apr. 2013.

[38] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Backscatter from the Data Plane – Threats to Stability and Security in Information-Centric Network Infrastructure," *Computer Networks*, vol. 57, no. 16, pp. 3192–3206, Nov. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2013.07.009

[39] M. Wählisch, A. Vorbach, C. Keil, J. Schönfelder, T. C. Schmidt, and J. H. Schiller, "Design, implementation, and operation of a mobile honeypot," Open Archive: arXiv.org, Technical Report arXiv:1205.4778, 2013. [Online]. Available: http://arxiv.org/abs/1301.7257

[40] E. Baccelli, O. Hahm, M. Wählisch, M. Günes, and T. C. Schmidt, "RIOT: One OS to Rule Them All in the IoT," INRIA, Research Report RR–8176, Dec. 2012. [Online]. Available: http://hal.inria.fr/hal-00768685

[41] E. Baccelli, T. C. Schmidt, and M. Wählisch, Eds., *Proceedings of The 1st ACM International Workshop on Sensor-Enhanced Safety and Security in Public Spaces, SESP'12 (co-located with MobiHoc'12).* New York, NY, USA: ACM, 2012.

[42] T. C. Schmidt, M. Wählisch, R. Koodli, G. Fairhurst, and D. Liu, "Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers," IETF, IETF Internet Draft – work in progress 08, September 2014. [Online]. Available: http://tools.ietf.org/html/draft-ietf-multimob-fmipv6-pfmipv6-multicast

[43] D. Charousset, T. C. Schmidt, and M. Wählisch, "Actors and Publish/Subscribe: An Efficient Approach to Scalable Distribution in Data Centers," in *Proc. of the ACM SIGCOMM CoNEXT. Student Workshop.* New York: ACM, Dec. 2012.

[44] A. Knauf, T. C. Schmidt, G. Hege, and M. Wählisch, "A RELOAD Usage for Distributed Conference Control (DisCo)," IETF, IETF Internet Draft – work in progress 02, Aug. 2013. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-disco

[45] ——, "A Usage for Shared Resources in RELOAD (ShaRe)," IETF, IETF Internet Draft – work in progress 06, June 2015. [Online]. Available: http://tools.ietf.org/html/draft-ietf-p2psip-share

[46] S. Meiling, T. C. Schmidt, and M. Wählisch, "Large-Scale Measurement and Analysis of One-Way Delay in Hybrid Multicast Networks," in *37th Annual IEEE Conf. on Local Computer Networks (LCN'12).* Piscataway, NJ, USA: IEEE Press, Oct. 2012.

[47] F. Jäger, T. C. Schmidt, and M. Wählisch, "Predictive Video Scaling - Adapting Source Coding to Early Network Congestion Indicators," in *2nd IEEE International Conference on Consumer Electronics - Berlin (ICCE-Berlin 2012).* Piscataway, NJ, USA: IEEE Press, Sep. 2012.

[48] S. Zagaria, T. C. Schmidt, S. Meiling, and M. Wählisch, "A Monitoring Framework for Hybrid Multicast Networks," in *2nd IEEE International Conference on Consumer Electronics - Berlin (ICCE-Berlin 2012).* Piscataway, NJ, USA: IEEE Press, Sep. 2012.

[49] Y. Yang, M. Wählisch, Y. Zhao, and M. Kyas, "RAID the WSN: Packet-based Reliable Cooperative Diversity," in *Proc. of the IEEE International Conference on Communications (ICC)*. Piscataway, NJ, USA: IEEE Press, 2012, pp. 371–375.

[50] G. Bartl and S. Krieg, "Flughafensicherheit aus der Sicht von Experten und Passagieren. Ergebnisse der soziologischen Begleitforschung des Projektes SAFEST," in *Ergebnisse interdisziplinr Risiko- und Sicherheitsforschung*, ser. Schriftenreihe Sicherheit, L. Gerhold, H. Jäckel, J. Schiller, and S. Steiger, Eds. Forschungsforum Öffentliche Sicherheit, 2015, no. 17, pp. 95–124. [Online]. Available: http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_17.pdf

[51] G. Bartl, L. Gerhold, and J. Schiller, "Resilienz – nationale perspektiven," in *Resilien-Tech. Resilience by Design. Strategie für die technologischen Zukunftsthemen*, ser. acatech STUDIE, K. Thomas, Ed. München: acatech, 2014, pp. 16–47.

[52] G. Bartl, L. Gerhold, and M. Wählisch, "Towards a theoretical framework of acceptance for surveillance systems at airports," in *Proc. of 11th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, S. R. Hiltz, M. S. Pfaff, L. Plotnick, and P. C. Shih, Eds. The Pennsylvania State University, USA, 2014, pp. 299–303. [Online]. Available: http://iscram2014.ist.psu.edu/sites/default/files/misc/proceedings/p180.pdf

[53] K. Steinmüller, L. Gerhold, and M.-L. Beck, Eds., *Sicherheit 2025*, ser. Schriftenreihe Forschungsforum Öffentliche Sicherheit, no. 10. Berlin: Freie Universität Berlin, Forschungsforum Öffentliche Sicherheit, September 2012.

[54] G. Bartl and L. Gerhold, "Soziale Dimensionen der Flughafensicherheit," *Crisis Prevention*, no. 1, pp. 14–15, Jan. 2013.

[55] ——, "Die Bevölkerung als Adressat der Sicherheitsforschung," in *innosecure*, K.-D. Wolf, Ed. Berlin: VDE Verlag, 2013, pp. 41–48.

[56] G. Bartl, "Subjektive Wahrnehmung und Akzeptanz von Sicherheitsmaahmen am Flughafen. Triangulation als Instrument zur Erforschung von subjektiven Wahrnehmungen," in *Berliner Methodentreffen*, 2013.

Berichtsblatt

1. ISBN oder ISSN –	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel SAFEST – Social-Area Framework for Early Security Triggers at Airports	
4. Autor(en) [Name(n), Vorname(n)] Dr. Matthias Wählisch, Hauke Petersen, Gabriel Bartl	5. Abschlussdatum des Vorhabens 30.09.2015
	6. Veröffentlichungsdatum –
	7. Form der Publikation –
8. Durchführende Institution(en) (Name, Adresse) AG CST, Inst. für Informatik, FU Berlin Takustr. 9, 14195 Berlin	9. Ber. Nr. Durchführende Institution –
	10. Förderkennzeichen*) 13N12235
	11. Seitenzahl 36
13. Fördernde Institution(en) (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben 56
	14. Tabellen 1
	15. Abbildungen 19
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum) VDI Technologiezentrum GmbH, Düsseldorf, 3. März 2016	
18. Kurzfassung Das Projekt SAFEST erforscht die Potentiale des Internet of Things (IoT) für die Erhöhung der zivilen Sicherheit. Dabei befasst es sich vornehmlich mit der frühzeitigen Erkennung von Menschenaufläufen vor Massenpaniken an Flughäfen. Hierfür liefern Sensoren verschiedene Daten, die sicher kommuniziert, analysiert und ausgewertet werden müssen, sodass auf dieser Grundlage Gegenmaßnahmen eingeleitet werden können. Das Teilvorhaben „Sensorik und Wissensfusion zum Schutz von Verkehrsinfrastrukturen unter gesellschaftlichen Randbedingungen“ hat zum Ziel, durch intelligente, verteilte Sensorik Gefahren am Flughafen rechtzeitig zu erkennen, diese mittels Wissensfusionierung auszuwerten und Passagiere in Kombination mit einem leichgewichtigen Leitsystem zu schützen. Eine soziologische Begleitstudie wird das Akzeptanzverhalten innerhalb der Bevölkerung untersuchen und Handlungsempfehlungen für Entwickler und möglichj Betreiber eines solchen Krisenmanagements ableiten. Zentrale Komponenten für die Umsetzung des Gesamtziels sind bildbasierte Erkennungsverfahren zur Identifizerung von Menschenansammlungen sowie leitsystemgesteuerte Alarmverfahren für die geordnete Auflösung gefährlicher Massensituationen. Perimetersensoren sollen sicherheitskrische Bereiche des Flughafens überwachen Alle in SAFEST entwickelte Software und Lösungen wurden als Open Source veröffentlicht. Dies ist der Abschlussbericht des Forschungsprojekts SAFEST.	
19. Schlagwörter Internet of Things, Zivile Sicherheit, Kommunikationssicherheit, verteilte Analyse	
20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN –	2. Type of document (e.g. report, publication) Final Report
3. Title SAFEST – Social-Area Framework for Early Security Triggers at Airports	
4. Autor(s) [family name, first name(s)] Dr. Matthias Wählisch, Hauke Petersen, Gabriel Bartl	5. End of project 30.09.2015
	6. Publication date –
	7. Form of publication –
8. Performing organization(s) (Name, Address) AG CST, Inst. für Informatik, FU Berlin Takustr. 9, 14195 Berlin	9. Originator's report no. –
	10. Förderkennzeichen*) 13N12235
	11. No. of pages 36
13. Sponsoring agency(ies) (Name, Adrress) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. No. of references 56
	14. No. of tables 1
	15. No. of figures 19
16. Supplementary notes	
17. Presented at (Title, place, Date) VDI Technologiezentrum GmbH, Düsseldorf, 3. März 2016	
18. Abstract The SAFEST project is dedicated to research for public safety based on the potentials of the Internet of Things. Its focus lies on an early warning system for irregular crowd detection and mass panics at airports. In this context, sensors are deployed to deliver data via secure communication to perform specialized analyses and evaluations and eventually initiate counter measures. The subproject "Sensors and knowledge fusion to protect public transport infrastructures while considering public concerns" aims at the following: Early detection of threats at airports by using interconnected sensors, analysing events by knowledge fusion, and intelligent guidance of passengers in case of incidents. A sociological study analyzes the acceptance behavior and complements the technological solution. All software and solutions developed within the project SAFEST were publically release as open source. This is the final report of the research project SAFEST.	
19. Keywords Internet of Things, Civil Security, Communication Security, Distributed Analysis	
20. Publisher	21. Price

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation ICN Research Challenges	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Dirk Kutscher, Suyong Eum, Kostas Pentikousis, Ioannis Psaras, Daniel Corujo, Damien Saucez, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum März 2016 7. Form der Publikation IRTF Internet Draft -- work in progress
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben 14. Tabellen 15. Abbildungen
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	
16. Zusätzliche Angaben http://tools.ietf.org/html/draft-irtf-icnrg-challenges	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung This memo describes research challenges for Information-Centric Networking. Information-Centric Networking is an approach to evolve the Internet infrastructure to directly support information distribution by introducing uniquely named data as a core Internet principle. Data becomes independent from location, application, storage, and means of transportation, enabling in-network caching and replication. Challenges include naming, security, routing, system scalability, mobility management, wireless networking, transport services, in-network caching, and network management.	
19. Schlagwörter Information-Centric Networking	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Flughafensicherheit aus der Sicht von Experten und Passagieren. Ergebnisse der soziologischen Begleitforschung des Projektes SAFEST	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Gabriel Bartl, Sebastian Krieg	6. Veröffentlichungsdatum 2015
	7. Form der Publikation Buchkapitel
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 95--124
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_17.pdf	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag Forschungsforum Öffentliche Sicherheit	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation A Usage for Shared Resources in RELOAD (ShaRe)	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Alexander Knauf, Thomas C. Schmidt, Gabriel Hege, Matthias Wählisch	6. Veröffentlichungsdatum Juni 2015
	7. Form der Publikation IETF Internet Draft -- work in progress
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://tools.ietf.org/html/draft-ietf-p2psip-share	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung This document defines a RELOAD Usage for managing shared write access to RELOAD Resources. Shared Resources in RELOAD (ShaRe) form a basic primitive for enabling various coordination and notification schemes among distributed peers. Access in ShaRe is controlled by a hierarchical trust delegation scheme maintained within an access list. A new USER-CHAIN-ACL access policy allows authorized peers to write a Shared Resource without owning its corresponding certificate. This specification also adds mechanisms to store Resources with a variable name which is useful whenever peer-independent rendezvous processes are required.	
19. Schlagwörter Video Conferencing over IP, Peer-to-Peer Networking	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Programming Actors for the Internet of Things	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Raphael Hiesgen, Dominik Charousset, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum April 2015
	7. Form der Publikation Journalbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 25--26
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://ercim-news.ercim.eu/en101/special/programming-actors-for-the-internet-of-things	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung The Internet of Things (IoT) enables a large number of devices to cooperate to achieve a common task. Each individual device is small and executes a confined software core. Collective intelligence is gained from distributed collaboration and Internet communication. Corresponding IoT solutions form large distributed software systems that pose professional requirements: scalability, reliability, security, portability and maintainability. The C++ Actor Framework CAF contributes such a professional open source software layer for the IoT. Based on the actor model of Hewitt et al., it aids programmers at a good level of abstraction without sacrificing performance.	
19. Schlagwörter Internet of Things	
20. Verlag ERCIM EEIG	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Old Wine in New Skins? Revisiting the Software Architecture for IP Network Stacks on Constrained IoT Devices	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum Mai 2015
4b. Autoren der Publikation (Name, Vorname(n)) Hauke Petersen, Martine Lenders, Matthias Wählisch, Oliver Hahm, Emmanuel Baccelli	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet of Things	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Federated End-to-End Authentication for the Constrained Internet of Things using IBC and ECC	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Tobias Markmann, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum August 2015
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 603--604
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://dx.doi.org/10.1145/2785956.2790021	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet of Things, Network Security	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Amplification and DRDoS Attack Defense -- A Survey and New Perspectives	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Fabrice J. Ryba, Matthew Orlinski, Matthias Wählisch, Christian Rossow, Thomas C. Schmidt	6. Veröffentlichungsdatum Juni 2015 7. Form der Publikation Technical Report
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben 14. Tabellen 15. Abbildungen
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	
16. Zusätzliche Angaben http://arxiv.org/abs/1505.07892	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security, Internet Measurement and Analysis	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation The Role of the Internet of Things in Network Resilience	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2015
4b. Autoren der Publikation (Name, Vorname(n)) Hauke Petersen, Emmanuel Baccelli, Matthias Wählisch, Thomas C. Schmidt, Jochen Schiller	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 283--296
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet of Things	
20. Verlag Springer	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Cashing out the Great Cannon? On Browser-Based DDoS Attacks and Economics	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2015
4b. Autoren der Publikation (Name, Vorname(n)) Giancarlo Pellegrino, Christian Rossow, Fabrice J. Ryba, Thomas C. Schmidt, Matthias Wählisch	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 1--8
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security, Internet Measurement and Analysis	
20. Verlag USENIX Assoc.	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Partial Adaptive Name Information in ICN: PANINI Routing Limits FIB Table Sizes	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Thomas C. Schmidt, Sebastian Wölke, Nora Berg, Matthias Wählisch	6. Veröffentlichungsdatum Oktober 2015
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 193--194
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Name-based routing as proposed in Information Centric Networking encounters the problems of (a) exploding routing tables, as the number of names largely exceeds common routing resources, and (b) limited aggregation potentials, as names are commonly independent of content locations. In this poster, we introduce PANINI, an approach to scale routing on names by adapting FIB tables simultaneously to available resources and actual traffic patterns. PANINI introduces routing hierarchies with respect to aggregation points, bimodal FIBs, and confined flooding. First evaluations show promising results in theory and experiments.	
19. Schlagwörter Network Security, Information-Centric Networking	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Revisiting Countermeasures Against NDN Interest Flooding	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Samir Al-Sheikh, Matthias Wählisch, Thomas C. Schmidt	6. Veröffentlichungsdatum Oktober 2015
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 195--196
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Interest flooding has been identified as a major threat for the NDN infrastructure. Since then several approaches have been proposed to identify and to mitigate this attack. In this paper, we (a) classify nine existing countermeasures and (b) compare them in a consistent evaluation setup. We discuss the application of pure prefix-based as well as pure interfacebased mitigation strategies in different network scenarios.	
19. Schlagwörter Network Security, Information-Centric Networking	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Dynamic Cross-Domain Group Communication in Hybrid Multicast Networks	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Sebastian Wölke, Thomas C. Schmidt, Sebastian Meiling, Matthias Wählisch	6. Veröffentlichungsdatum September 2015
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 185--189
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Group communication based on multicast enables efficient one-to-many and many-to-many distribution of real-time data. Multicast communication would therefore be beneficial to popular Internet applications such as IPTV, online multiplayer games and audio/video conferencing, and is considered as an important network service for future CCN/ICN architectures. However, multicast exists in many flavors and technologies, and on different network layers with incompatible application interfaces and divergent states of deployment. Due to these challenges of multicast plurality, there is no multicast service available on the Internet today. In this paper, we present a dynamic and technology-transparent group communication scheme by names. We extend HAMcast -- a hybrid multicast architecture -- with a mapping service between technology dependent addressing and an abstract naming. Therefore we show in detail the required components and discuss possible solutions.

19. Schlagwörter Mobile IPv6, Mobile Multicast	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für <u>Publikationen</u>

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Privacy-Preserving Crowd Incident Detection: A Holistic Experimental Approach	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2015
4b. Autoren der Publikation (Name, Vorname(n)) Baccelli, Emmanuel, Danilkina, Alexandra, Müller, Sebastian, Voisard, Agn{\`e}s, Wählisch, Matthias	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Leistungsmessung eines modularen Netzwerk-Stacks für das IoT-Betriebssystem RIOT	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum September 2015
4b. Autoren der Publikation (Name, Vorname(n)) Peter Kietzmann, Martin Landsmann, Thomas C. Schmidt, Hauke Petersen, Martine Lenders, Matthias Wählisch	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 19--22
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag Friedrich-Alexander-Universität Erlangen-Nürnberg, Dept. of Computer Science	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Towards a theoretical framework of acceptance for surveillance systems at airports	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2014
4b. Autoren der Publikation (Name, Vorname(n)) Gabriel Bartl, Lars Gerhold, Matthias Wählisch	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 299--303
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://iscram2014.ist.psu.edu/sites/default/files/misc/proceedings/p180.pdf	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag The Pennsylvania State University, USA	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Resilienz -- Nationale Perspektiven	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2014
4b. Autoren der Publikation (Name, Vorname(n)) Gabriel Bartl, Lars Gerhold, Jochen Schiller	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 16--47
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag acatech	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Thomas C. Schmidt, Matthias Wählisch, Rajeev Koodli, Godred Fairhurst, Dapeng Liu	6. Veröffentlichungsdatum September 2014 7. Form der Publikation IETF Internet Draft -- work in progress
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben 14. Tabellen 15. Abbildungen
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	
16. Zusätzliche Angaben http://tools.ietf.org/html/draft-ietf-multimob-fmipv6-pfmipv6-multicast	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Fast handover protocols for MIPv6 and PMIPv6 define mobility management procedures that support unicast communication at reduced handover latencies. Fast handover base operations do not affect multicast communication, and hence do not accelerate handover management for native multicast listeners. Many multicast applications like IPTV or conferencing, though, are comprised of delay-sensitive real-time traffic and could strongly benefit from fast handover execution. This document specifies extension of the Mobile IPv6 Fast Handovers (FMIPv6) and the Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) protocols to include multicast traffic management in fast handover operations. This multicast support is provided first at the control plane by a management of rapid context transfer between access routers, second at the data plane by an optional fast traffic forwarding that MAY include buffering.	
19. Schlagwörter Mobile IPv6, Mobile Multicast	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Proceedings of the 3rd MANIAC Challenge Berlin Germany July 27 - 28 2013	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2014
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Felix Juraschek, Oliver Hahm, Thomas C. Schmidt, Heiko Will, Matthias Wählisch	7. Form der Publikation Konferenzband
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://arxiv.org/html/1401.1163	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Peer-to-Peer Networking	
20. Verlag Open Archive: arXiv.org	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Area & Perimeter Surveillance in SAFEST using Sensors and the Internet of Things	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum Januar 2014
4b. Autoren der Publikation (Name, Vorname(n)) Baccelli, Emmanuel, Bartl, Gabriel, Danilkina, Alexandra, Ebner, Veronika, Gendry, Fran{\c c}ois, Guettier, Christophe, Hahm, Oliver, Kriegel, Ulrich, Hege, Gabriel, Palkow, Mark, Pertersen, Hauke, Thomas C. Schmidt, Voisard, Agn{\`e}s, Wählisch,	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://hal.inria.fr/hal-00944907	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung {SAFEST is a project aiming to provide a comprehensive solution to ensure the safety and security of the general public and critical infrastructures. The approach of the project is to design a lightweight, distributed system using heterogeneous, networked sensors, able to aggregate the input of a wide variety of signals (e.g. camera, PIR, radar, magnetic, seismic, acoustic). The project aims for a proof-of-concept demonstration focusing on a concrete scenario: crowd monitoring, area and perimeter surveillance in an airport, realized with a prototype of the system, which must be deployable and foldable overnight, and leverage autoconfiguration based on wireless communications and Internet of Things. This paper reviews the progress towards reaching this goal, which is planned for 2015.}	
19. Schlagwörter Internet of Things	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für <u>Publikationen</u>

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Demonstration Abstract: Simply RIOT -- Teaching and Experimental Research in the Internet of Things	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Oiver Hahm, Emmanuel Baccelli, Hauke Petersen, Matthias Wählisch, Thomas C. Schmidt	6. Veröffentlichungsdatum April 2014 7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. Tabellen 15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet of Things	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Peer my Proxy - A Performance Study of Peering Extensions for Multicast in Proxy Mobile IP Domains	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Thomas C. Schmidt, Sebastian Wölke, Matthias Wählisch	6. Veröffentlichungsdatum Mai 2014
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 1--8
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Proxy Mobile IPv6 (PMIPv6) and its multicast extensions have been designed by the IETF as a deployment friendly mobility scheme. Although easy to implement, the basic multicast proxy solution suffers from unwanted delay and jitter due to suboptimal traffic flows. In this paper, we recap recent IETF work on peering extensions for multicast proxies and make the following two contributions. First we introduce the design and implementation of a highly flexible, open proxy that allows for dynamic reconfiguration at runtime. In particular, the system can support a variety of functional extensions including peering. Second we report on extensive performance measurements of proxy peering in LTE and UMTS type networks. Our findings indicate that a transparent deployment of the peering option significantly smoothes handovers and chokes delay variations throughout the access network.

19. Schlagwörter Mobile IPv6, Mobile Multicast	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Native Actors: How to Scale Network Forensics	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Matthias Vallentin, Dominik Charousset, Thomas C. Schmidt, Vern Paxson, Matthias Wählisch	6. Veröffentlichungsdatum August 2014
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 141--142
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

When an organization detects a security breach, it undertakes a forensic analysis to figure out what happened. This investigation involves inspecting a wide range of heterogeneous data sources spanning over a long period of time. The iterative nature of the analysis procedure requires an interactive experience with the data. However, the distributed processing paradigms we find in practice today fail to provide this requirement: the batch-oriented nature of MapReduce cannot deliver sub-second round-trip times, and distributed in-memory processing cannot store the terabytes of activity logs needed to inspect during an incident. We present the design and implementation of Visibility Across Space and Time~(VAST), a distributed database to support interactive network forensics, and libcppa, its exceptionally scalable messaging core. The extended actor framework libcppa enables VAST to distribute lightweight tasks at negligible overhead. In our live demo, we showcase how VAST enables security analysts to grapple with the huge amounts of data often associated with incident investigations.

19. Schlagwörter Network Security	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Thomas C. Schmidt, Shuai Gao, Hong-Ke Zhang, Matthias Wählisch	6. Veröffentlichungsdatum Juni 2014
	7. Form der Publikation RFC
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://tools.ietf.org/html/rfc7287	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Multicast communication can be enabled in Proxy Mobile IPv6 (PMIPv6) domains via the Local Mobility Anchors by deploying Multicast Listener Discovery (MLD) proxy functions at Mobile Access Gateways, by using direct traffic distribution within an ISP's access network, or by selective route optimization schemes. This document describes a base solution and an experimental protocol to support mobile multicast senders in PMIPv6 domains for all three scenarios. Protocol optimizations for synchronizing PMIPv6 with PIM, as well as a peering function for MLD proxies are defined. Mobile sources always remain agnostic of multicast mobility operations.	
19. Schlagwörter Mobile IPv6, Mobile Multicast	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Information Centric Networking in the IoT: Experiments with NDN in the Wild	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Christian Mehlis, Oliver Hahm, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum Juni 2014
	7. Form der Publikation Technical Report
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://arxiv.org/abs/1406.6608	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Information-Centric Networking, Internet of Things	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation The Role of the Internet of Things in Network Resilience	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Hauke Petersen, Emmanuel Baccelli, Matthias Wählisch, Thomas C. Schmidt, Jochen Schiller	6. Veröffentlichungsdatum Juni 2014 7. Form der Publikation Technical Report
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben 14. Tabellen 15. Abbildungen
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	
16. Zusätzliche Angaben http://arxiv.org/abs/1406.6614	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet of Things	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation How Dia-Shows Turn Into Video Flows: Adapting Scalable Video Communication to Heterogeneous Network Conditions in Real-Time	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Fabian Jäger, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum September 2014
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 218--226
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung
Video conferencing over IP (VCoIP) is a major trend in current Internet communication and has particularly spread to the mobile realm. In this environment, users face the problem of heterogeneous and fluctuating network conditions. A promising solution to this issue is the scalable video coding (SVC). It allows an adaptation of the video stream to the available bandwidth, but requires a reliable bandwidth estimation. Adaptation times for conversational video at fluctuating network conditions are critical, and a fast strategy for bandwidth estimation is needed to avoid congestion. In this work, we analyse the capabilities of the sender and the receiver to adapt the video coding to changing network conditions. We derive an early congestion indicator at the sender side based on the jitter variation. For receivers, we use sustained goodput to extract a feasible scaling. In thorough evaluations that include real-world 3G networks, we reveal a faster congestion detection at the sender that are also more robust but less accurate than probing at the receiver.

19. Schlagwörter Video Conferencing over IP	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Spontaneous Wireless Networking to Counter Pervasive Monitoring	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2014
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Oliver Hahm, Matthias Wählisch	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben https://www.w3.org/2014/strint/papers/26.pdf	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Information Centric Networking in the IoT: Experiments with NDN in the Wild	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Christian Mehlis, Oliver Hahm, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum September 2014
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 77--86
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://dx.doi.org/10.1145/2660129.2660144	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

This paper explores the feasibility, advantages, and challenges of an ICN-based approach in the Internet of Things. We report on the first NDN experiments in a life-size IoT deployment, spread over tens of rooms on several floors of a building. Based on the insights gained with these experiments, the paper analyses the shortcomings of CCN applied to IoT. Several interoperable CCN enhancements are then proposed and evaluated. We significantly decreased control traffic (i.e., interest messages) and leverage data path and caching to match IoT requirements in terms of energy and bandwidth constraints. Our optimizations increase content availability in case of IoT nodes with intermittent activity. This paper also provides the first experimental comparison of CCN with the common IoT standards 6LoWPAN/RPL/UDP.

19. Schlagwörter Information-Centric Networking, Internet of Things	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Proceedings of the 1st OMNeT++ Community Summit Hamburg Germany September 2 2014	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2014
4b. Autoren der Publikation (Name, Vorname(n)) Anna Förster, Christoph Sommer, Till Steinbach, Matthias Wählisch	7. Form der Publikation Konferenzband
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://arxiv.org/html/1409.0093	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Peer-to-Peer Networking	
20. Verlag Open Archive: arXiv.org	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Multicast Listener Extensions for Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6) Fast Handovers	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Thomas C. Schmidt, Matthias Wählisch, Rajeev Koodli, Godred Fairhurst, Dapeng Liu	6. Veröffentlichungsdatum November 2014 7. Form der Publikation RFC
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben 14. Tabellen 15. Abbildungen
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	
16. Zusätzliche Angaben http://tools.ietf.org/html/rfc7411	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Fast handover protocols for Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6) define mobility management procedures that support unicast communication at reduced handover latency. Fast handover base operations do not affect multicast communication and, hence, do not accelerate handover management for native multicast listeners. Many multicast applications like IPTV or conferencing, though, comprise delay-sensitive, real-time traffic and will benefit from fast handover completion. This document specifies extension of the Mobile IPv6 Fast Handovers (FMIPv6) and the Fast Handovers for Proxy Mobile IPv6 (PFMIPv6) protocols to include multicast traffic management in fast handover operations. This multicast support is provided first at the control plane by management of rapid context transfer between access routers and second at the data plane by optional fast traffic forwarding that may include buffering. An FMIPv6 access router indicates support for multicast using an updated Proxy Router Advertisements message format. This document updates RFC 5568, Mobile IPv6 Fast Handovers.	
19. Schlagwörter Mobile IPv6, Mobile Multicast	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Subjektive Wahrnehmung und Akzeptanz von Sicherheitsmaßnahmen am Flughafen. Triangulation als Instrument zur Erforschung von subjektiven Wahrnehmungen	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2013
4b. Autoren der Publikation (Name, Vorname(n)) Gabriel Bartl	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Die Bevölkerung als Adressat der Sicherheitsforschung	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2013
4b. Autoren der Publikation (Name, Vorname(n)) Gabriel Bartl, Lars Gerhold	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 41-48
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag VDE Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Soziale Dimensionen der Flughafensicherheit	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Gabriel Bartl, Lars Gerhold	6. Veröffentlichungsdatum Januar 2013
	7. Form der Publikation Journalbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 14--15
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation A RELOAD Usage for Distributed Conference Control (DisCo)	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum August 2013
4b. Autoren der Publikation (Name, Vorname(n)) Alexander Knauf, Thomas C. Schmidt, Gabriel Hege, Matthias Wählisch	7. Form der Publikation IETF Internet Draft -- work in progress
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://tools.ietf.org/html/draft-ietf-p2psip-disco	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung This document defines a RELOAD Usage for Distributed Conference Control (DisCo) with SIP. DisCo preserves conference addressing through a single SIP URI by splitting its semantic of identifier and locator using a new Kind data structure. Conference members are enabled to select conference controllers based on proximity awareness and to recover from failures of individual resource instances. DisCo proposes call delegation to balance the load at focus peers.	
19. Schlagwörter Video Conferencing over IP, Peer-to-Peer Networking, Mobile Multicast	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Design Implementation and Operation of a Mobile Honeypot	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2013
4b. Autoren der Publikation (Name, Vorname(n)) Matthias Wählisch, Andr{e} Vorbach, Christian Keil, Jochen Schönfelder, Thomas C. Schmidt, Jochen H. Schiller	7. Form der Publikation Technical Report
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://arxiv.org/abs/1301.7257	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Backscatter from the Data Plane -- Threats to Stability and Security in Information-Centric Network Infrastructure	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Matthias Wählisch, Thomas C. Schmidt, Markus Vahlenkamp	6. Veröffentlichungsdatum November 2013
	7. Form der Publikation Journalbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 3192--3206
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://dx.doi.org/10.1016/j.comnet.2013.07.009	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Information-centric networking (ICN) raises data objects to first class routable entities in the network and changes the Internet paradigm from host-centric connectivity to data-oriented delivery. However, current approaches to content routing heavily rely on data-driven protocol events and thereby introduce a strong coupling of the control to the data plane in the underlying routing infrastructure. In this paper, threats to the stability and security of the content distribution system are analyzed in theory, simulations, and practical experiments. We derive relations between state resources and the performance of routers, and demonstrate how this coupling can be misused in practice. We further show how state-based forwarding tends to degrade by decorrelating resources. We identify intrinsic attack vectors present in current content-centric routing, as well as possibilities and limitations to mitigate them. Our overall findings suggest that major architectural refinements are required prior to global ICN deployment in the real world.

19. Schlagwörter Network Security, Information-Centric Networking	
20. Verlag Elsevier	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Topology Authentication in RPL	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum April 2013
4b. Autoren der Publikation (Name, Vorname(n)) Martin Landsmann, Heiner Perrey, Osman Ugus, Matthias Wählisch, Thomas C. Schmidt	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
	12. Literaturangaben
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security, Internet of Things	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation RIOT OS: Towards an OS for the Internet of Things	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Oliver Hahm, Mesut Günes, Matthias Wählisch, Thomas C. Schmidt	6. Veröffentlichungsdatum 2013
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Mobile IPv6, Internet of Things	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Information-centric networking -- Ready for the real world? (Dagstuhl Seminar 12361)	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2013
4b. Autoren der Publikation (Name, Vorname(n)) Ali Ghodsi, Börje Ohlmann, Jörg Ott, Ignacio Solis, Matthias Wählisch	7. Form der Publikation Konferenzband
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Information-Centric Networking	
20. Verlag Schloss Dagstuhl--Leibniz-Zentrum fuer Informatik	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Lessons from the Past: Why Data-driven States Harm Future Information-Centric Networking	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Matthias Wählisch, Thomas C. Schmidt, Markus Vahlenkamp	6. Veröffentlichungsdatum 2013
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6663520	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Information-centric networking (ICN) raises data objects to first class routable entities in the network and changes the Internet paradigm from host-centric connectivity to data-oriented publish/subscribe. We revisit the data-centric paradigm from the perspective of security and resilience and question its applicability in an open, widely distributed routing and forwarding service. Current concepts of content routing are built on data-driven protocol events and thereby introduce a strong coupling of the control to the data plane in the underlying routing infrastructure. In this paper, we explore the vulnerability of the distribution backbone. Based on a straight-forward analytical model we show that local systems cannot be protected from the threats of data-driven state management on an Internet scale. By practical evaluations using the example of the CCNx implementation, we further analyze threats to stability and performance of a data-driven infrastructure that refrains from separating the control from the data plane. We identify intrinsic attack vectors, as well as possibilities and limitations to mitigate them. Our overall findings suggest that major architectural refinements are required prior to global ICN deployment in the real world.

19. Schlagwörter Network Security, Information-Centric Networking	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Technische Dimensionen der Flughafensicherheit	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum Januar 2013
4b. Autoren der Publikation (Name, Vorname(n)) Matthias Wählisch, Emmanuel Baccelli, Jochen Schiller, Agn{\`e}nes Voisard, Thomas C. Schmidt, Stefan Pfennigschmidt, Mark Palkow, Uwe Weigmann, Uwe Hanewald	7. Form der Publikation Journalbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 15--16
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Network Security	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Untersuchungen zur Komplexität komponierter Netzwerkarchitekturen im Future Internet	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Nora Berg, Sebastian Meiling, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum September 2013
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 73--84
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Mobile Multicast	
20. Verlag Universität Hamburg, Dept. Informatik	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation On Name-based Group Communication: Challenges Concepts and Transparent Deployment	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Thomas C. Schmidt, Matthias Wählisch, Dominik Charousset, Sebastian Meiling	6. Veröffentlichungsdatum September 2013
	7. Form der Publikation Journalbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 1657--1664
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://dx.doi.org/10.1016/j.comcom.2013.08.001	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Human-centric naming will largely facilitate access and deployment of network services in a future Internet. Information-centric networking (ICN) introduces such vision of a name-oriented, secure, globally available publish-subscribe infrastructure. Current approaches concentrate on unicast-like pull mechanisms and thereby fall short of naming and automatically updating content at groups of receivers. In this paper, we adopt the information-centric paradigm, but argue that an inclusion of multicast will grant additional benefits to the network layer. Our contribution bridges the gap between requesting content by name and applying requests to a scalable distribution infrastructure in a many-to-many communication model. We introduce a group-oriented naming concept that integrates the various available group schemes, simplifies rendezvous processes, and introduces new use cases. We present an open-source prototype of this name-oriented multicast access implemented in the HAMcast middleware.

19. Schlagwörter Mobile Multicast, Network Security, Information-Centric Networking	
20. Verlag Elsevier	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Native Actors -- A Scalable Software Platform for Distributed Heterogeneous Environments	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Dominik Charousset, Thomas C. Schmidt, Raphael Hiesgen, Matthias Wählisch	6. Veröffentlichungsdatum Oktober 2013
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 87--96
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Writing concurrent software is challenging, especially with low-level synchronization primitives such as threads or locks in shared memory environments. The actor model replaces implicit communication by an explicit message passing in a ``shared-nothing'' paradigm. It applies to concurrency as well as distribution, but has not yet entered the native programming domain. This paper contributes the design of a native actor extension for C++, and the report on a software platform that implements our design for (a) concurrent, (b) distributed, and (c) heterogeneous hardware environments. GPGPU and embedded hardware components are integrated in a transparent way. Our software plattform supports the development of scalable and efficient parallel software. It includes a lock-free mailbox algorithm with pattern matching facility for message processing. Thorough performance evaluations reveal an extraordinary small memory footprint in realistic application scenarios, while runtime performance not only outperforms existing mature actor implementations, but exceeds the scaling behavior of low-level message passing libraries such as OpenMPI.

19. Schlagwörter	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Native Actors -- A Scalable Software Platform for Distributed Heterogeneous Environments (AGERE '13 paper)	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Dominik Charousset, Thomas C. Schmidt, Raphael Hiesgen, Matthias Wählisch	6. Veröffentlichungsdatum Oktober 2013
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation The MANIAC Challenge at IETF 87	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum November 2013
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Felix Juraschek, Oliver Hahm, Thomas C. Schmidt, Heiko Will, Matthias Wählisch	7. Form der Publikation Journalbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 27--29
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Peer-to-Peer Networking	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation A Common API for Transparent Hybrid Multicast	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum Dezember 2013
4b. Autoren der Publikation (Name, Vorname(n)) Matthias Wählisch, Thomas C. Schmidt, Stig Venaas	7. Form der Publikation RFC
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben http://tools.ietf.org/html/rfc7046	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Group communication services exist in a large variety of flavors and technical implementations at different protocol layers. Multicast data distribution is most efficiently performed on the lowest available layer, but a heterogeneous deployment status of multicast technologies throughout the Internet requires an adaptive service binding at runtime. Today, it is difficult to write an application that runs everywhere and at the same time makes use of the most efficient multicast service available in the network. Facing robustness requirements, developers are frequently forced to use a stable upper-layer protocol provided by the application itself. This document describes a common multicast API that is suitable for transparent communication in underlay and overlay and that grants access to the different flavors of multicast. It proposes an abstract naming scheme that uses multicast URIs, and it discusses mapping mechanisms between different namespaces and distribution technologies. Additionally, this document describes the application of this API for building gateways that interconnect current Multicast Domains throughout the Internet. It reports on an implementation of the programming Interface, including service middleware. This document is a product of the Scalable Adaptive Multicast (SAM) Research Group.

19. Schlagwörter Peer-to-Peer Networking, Mobile Multicast	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation The Critical Internet Infrastructure (Dagstuhl Seminar 13322)	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2013
4b. Autoren der Publikation (Name, Vorname(n)) Georg Carle, Jochen Schiller, Steve Uhlig, Walter Willinger, Matthias Wählisch	7. Form der Publikation Konferenzband
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet Measurement and Analysis	
20. Verlag Schloss Dagstuhl--Leibniz-Zentrum fuer Informatik	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Sicherheit 2025	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Karlheinz Steinmüller, Lars Gerhold, Marie-Luise Beck	6. Veröffentlichungsdatum September 2012
	7. Form der Publikation Konferenzband
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag Freie Universität Berlin, Forschungsforum Öffentliche Sicherheit	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation RAID the WSN: Packet-based Reliable Cooperative Diversity	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
	6. Veröffentlichungsdatum 2012
4b. Autoren der Publikation (Name, Vorname(n)) Yuan Yang, Matthias Wählisch, Yubin Zhao, Marcel Kyas	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation 371--375
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation A Monitoring Framework for Hybrid Multicast Networks	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Sebastian Zagaria, Thomas C. Schmidt, Sebastian Meiling, Matthias Wählisch	6. Veröffentlichungsdatum September 2012
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Many popular Internet applications like IPTV, video or voice chat, social networks and massive multiplayer online games communicate in groups. While IP layer multicast remains hesitant in global deployment, applications implement their own group distribution techniques at the price of higher complexity and lower efficiency. Emerging hybrid multicast approaches become a promising alternative to fill that gap. Hybrid multicast networks bridge between application and IP-layer multicast and gain multicast deployment at a system level throughout the Internet. In this paper, we present a monitoring framework for such hybrid multicast networks based on a common API in the process of standardization. Monitoring tools are useful to identify network failures and to improve the performance. The target of our monitoring framework is to collect, analyze and visualize node and routing information, thereby making the complexity of hybrid networks accessible to network administrators for the first time.

19. Schlagwörter Peer-to-Peer Networking, Mobile Multicast	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Predictive Video Scaling - Adapting Source Coding to Early Network Congestion Indicators	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Fabian Jäger, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum September 2012
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung A major trend in current Internet communication augments voice conversation with video. Video conferencing over IP (VCoIP) has rapidly spread in the mobile realm, where it faces the problem of heterogeneous, fluctuating network conditions. Scalable video coding enables bandwidth adaptation, but requires guidance by appropriate resource estimators. This work focuses on the analysis and design of an adaptive, bandwidth-aware transmission strategy for real-time multimedia applications like video conferencing. We present an early indicator of network congestion based on jitter variation along with our implementation of a new lightweight sender-based approach to adapt the video codec.	
19. Schlagwörter Video Conferencing over IP	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Large-Scale Measurement and Analysis of One-Way Delay in Hybrid Multicast Networks	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Sebastian Meiling, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum Oktober 2012
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Group communication plays an important role in the distribution of real-time data for IPTV, multimedia conferencing, or online multiplayer games, but IP multicast remains unsupported in today's global Internet. Hybrid solutions that bridge between overlay and underlay multicast are a promising escape from the deployment dilemma of multicast. In this paper, we examine the real-time capabilities of hybrid multicast in a globally distributed environment based on our adaptive architecture HAMcast within the Planet-Lab testbed. We present a large-scale measurement study and analysis of one-way packet delay distributions in several realistic group scenarios. The unique results in global traces of hybrid multicast data have been achieved by carefully tracking packets and continuously correcting clock offsets. Companion measurements of unicast-based distribution are part of our analysis, as well as the comparative discussion of our results with previous findings from theory and simulation. Our measurements reveal that about 50% of global group members experience a real-time compliant service within the conversational time bounds of 150ms.

19. Schlagwörter Peer-to-Peer Networking, Mobile Multicast, Internet Measurement and Analysis	
20. Verlag IEEE Press	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Actors and Publish/Subscribe: An Efficient Approach to Scalable Distribution in Data Centers	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Dominik Charousset, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum Dezember 2012
	7. Form der Publikation Konferenzbeitrag
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Data center applications are required to be fault-tolerant and self-healing, and at the same time to scale dynamically with the number of available hardware resources. Highly efficient task distribution is crucial for such services that require low latency and high availability. This paper introduces pub/sub actors as a paradigm to build distributed data center applications without a single point of failure. Our approach does not actively distribute tasks, but uses group communication and an orchestration protocol. Requests are received by a group of potential servers, but only processed by one of them. We present a key-value store using LIBCPPA as a case study of promising performance.	
19. Schlagwörter Mobile Multicast	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation Proceedings of The 1st ACM International Workshop on Sensor-Enhanced Safety and Security in Public Spaces SESP'12 (co-located with MobiHoc'12)	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Thomas C. Schmidt, Matthias Wählisch	6. Veröffentlichungsdatum 2012
	7. Form der Publikation Konferenzband
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution
	10. Förderkennzeichen *) 13N12235
	11a. Seitenzahl Bericht
	11b. Seitenzahl Publikation
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	12. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter	
20. Verlag ACM	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.

Anlage 4 zum Schlussbericht: Berichtsblatt für Publikationen

1. ISBN oder ISSN	2. Berichtsart Veröffentlichung
3a. Titel des Berichts	
3b. Titel der Publikation RIOT: One OS to Rule Them All in the IoT	
4a. Autoren des Berichts (Name, Vorname(n))	5. Abschlußdatum des Vorhabens
4b. Autoren der Publikation (Name, Vorname(n)) Emmanuel Baccelli, Oliver Hahm, Matthias Wählisch, Mesut Günes, Thomas C. Schmidt	6. Veröffentlichungsdatum Dezember 2012 7. Form der Publikation Research Report
8. Durchführende Institution(en) (Name, Adresse) Freie Universität Berlin, Inst. für Informatik, AG CST, Prof. Dr.-Ing. Jochen Schiller, Takustr. 9, 14195 Berlin	9. Ber.Nr. Durchführende Insitution 10. Förderkennzeichen *) 13N12235 11a. Seitenzahl Bericht 11b. Seitenzahl Publikation 12. Literaturangaben
13. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. Tabellen 15. Abbildungen
16. Zusätzliche Angaben http://hal.inria.fr/hal-00768685	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung	
19. Schlagwörter Internet of Things	
20. Verlag	21. Preis

*) Auf das Förderkennzeichen und die Förderung durch das BMBF soll auch in der Veröffentlichung hingewiesen werden.