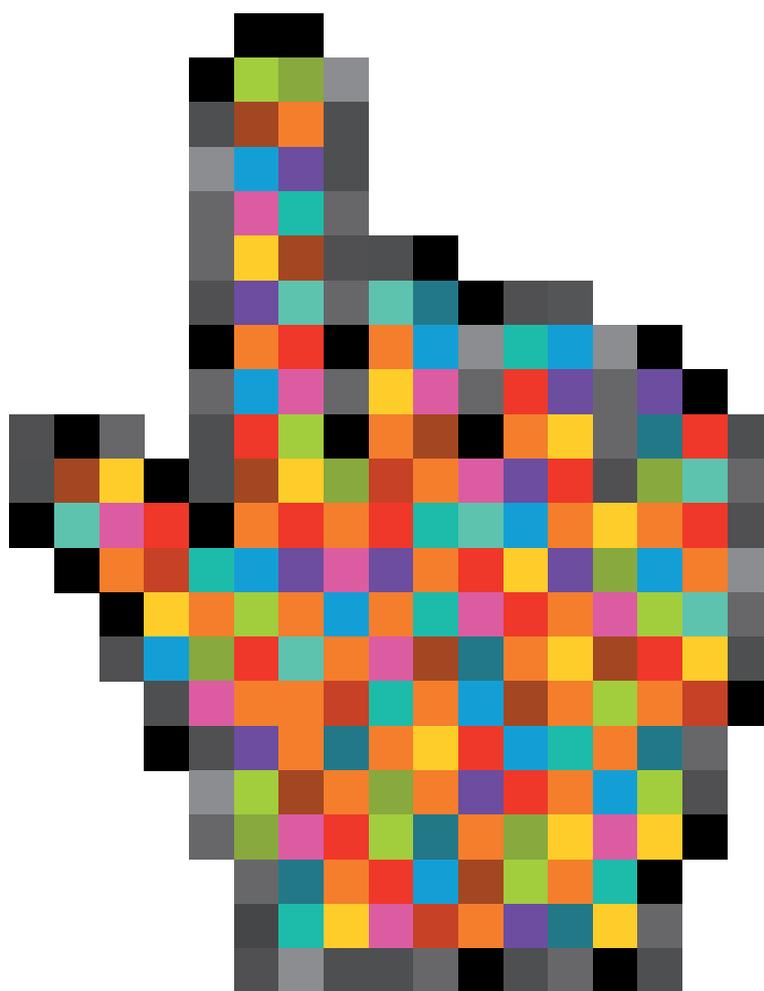


Max Planck FORSCHUNG

Das Wissenschaftsmagazin der Max-Planck-Gesellschaft 2014



Digitale Welten

ECHTZEITSYSTEME

Mit Sicherheit
pünktlich

MASCHINELLES LERNEN

Ein Weg aus dem
inneren Gefängnis

SZENENANALYSE

Bilder nehmen
Formen an

SPEZIAL

Forschung leicht gemacht.

Schafft die Papierstapel ab!

Das Magazin der Max-Planck-Gesellschaft
jetzt als ePaper: www.mpg.de/mpf-mobil

Internet: www.mpg.de/mpforschung

Kostenlos
downloaden!

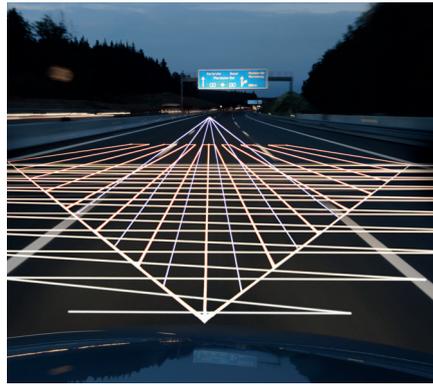


MAX-PLANCK-GESELLSCHAFT

Inhalt



04 Im Netz: Menschen hinterlassen beim Surfen mannigfaltige Abdrücke. Was machen Rechner damit?



52 Im Blickfeld: Vorausschauende Computerprogramme helfen, Verkehrsunfälle zu vermeiden.



58 Im Teleskop: Mit dem Fernrohr entschlüsselt Michael Backes den Inhalt von Monitoren in gespiegelten Bildern.

04 Der digitale Zauberlehrling
Vor zwei Jahren ging eine Meldung durch die Medien: Ein Rechner hatte das knifflige Wissensquiz *Jeopardy* im US-amerikanischen Fernsehen gewonnen. Das wirft Fragen auf wie: Was können Computer wissen? Was lässt sich dagegen tun, wenn Maschinen Fakten nicht zum Besten eines Nutzers sammeln? Der Essay gibt Antworten.

10 Das Echo des digitalen Gezwitzers
Twitter, Facebook & Co. – soziale Medien beherrschen zunehmend das Internet. Wie aber breiten sich Nachrichten über diese neuen Plattformen aus? Welche Rolle spielt dabei eine kleine Clique von Super-Einflussreichen?

18 Der Daten-Schutzmantel
Unsere Informationsgesellschaft lebt von Daten. Oft genug aber geraten Unternehmen, die nicht auf die Analyse dieses digitalen Rohstoffs verzichten wollen, in Konflikt mit dem Datenschutz. Wissenschaftler entwickeln daher Konzepte, um aussagekräftige statistische Informationen zu liefern und dabei persönliche Daten vor Missbrauch zu schützen.

24 Mit Sicherheit pünktlich
Wenn die Elektronik im Auto oder in Flugzeugen nicht absolut pünktlich Befehle verarbeitet, dann kann das lebensgefährlich werden – etwa, wenn sich der Airbag bei einem Unfall nicht oder zu spät öffnet. Forscher untersuchen, unter welchen Bedingungen solche Echtzeitsysteme zuverlässig funktionieren.

30 Ein Weg aus dem inneren Gefängnis
Computer, die Gedanken lesen? Was sich wie Science-Fiction anhört, könnte schon bald Realität werden. Für Menschen, die an amyotropher Lateralsklerose leiden, keinen Muskel mehr bewegen und auch nicht mehr mit ihrer Außenwelt kommunizieren können, wäre das ein Weg aus ihrer Isolation. Wissenschaftler wollen diesen Patienten eines Tages ermöglichen, sich kraft ihrer Gedanken mitzuteilen.

36 Dialog der Maschinen
Damit etwa Strom aus regenerativen Quellen optimal genutzt werden kann, sind cyber-physikalische Systeme gefragt. Sie vernetzen Sensoren und Aktoren wie zum Beispiel Kraftwerke mit einer Regelung. Informatiker entwickeln mathematische Methoden, um die Zuverlässigkeit der Systeme zu garantieren.

44 Bilder nehmen Formen an
Menschen reicht ein zweidimensionales Foto oder ein Film, um ein Gesicht oder einen Körper auch in 3-D zu erfassen. Diese Fähigkeit bringen Forscher jetzt Computern bei – und schaffen so neue Möglichkeiten, Bilder und Filme zu bearbeiten.

52 Bordcomputer mit 7. Sinn
Künftig sollen elektronische Assistenten Unfälle nicht nur im letzten Moment mit einer Notbremse verhindern, sondern den Verkehr vorausschauend verfolgen.

58 Spione im Dienst der Sicherheit
Die elektronischen Medien unseres Alltags stecken voller Fallen. Eine Gruppe von Informatikern deckt diese Sicherheitslücken mit unkonventionellen Methoden auf.

63 Standorte
63 Impressum

Der digitale Zauberlehrling

Vor zwei Jahren ging eine Meldung durch die Medien: Ein Rechner hatte das knifflige Wissensquiz *Jeopardy* im US-amerikanischen Fernsehen gewonnen. Das wirft Fragen auf: Was können Computer wissen? Wie setzen sie dieses Wissen für Sprachverstehen und Dialoge mit Menschen ein? Und: Was lässt sich dagegen tun, wenn Maschinen über einen Nutzer Fakten sammeln, die nicht zu dessen Bestem sind?

TEXT GERHARD WEIKUM

Haben Computer das Potenzial, dem Menschen intellektuell ebenbürtig oder gar überlegen zu sein? Die Informatik und ihr Teilgebiet, die künstliche Intelligenz, verfolgen diese Frage, seit Alan Turing vor mehr als fünfzig Jahren einen Test vorgeschlagen hat: Kann ein Computer, der mit einem menschlichen Dialogpartner über eine Textschnittstelle kommuniziert, sich so verhalten, dass der Mensch selbst nach längerer Zeit nicht festzustellen vermag, ob hinter dem Gesprächspartner ein Mensch oder eine Maschine steckt?

.....

**Unser Wissen ist nahezu
lückenlos digitalisiert
und systematisch organisiert.**

Menschliches Wissen – in Büchern, Aufsätzen, Nachrichten und anderen Texten – ist heute nahezu lückenlos digitalisiert und systematisch organisiert. Das prominenteste Beispiel digitaler Wissenssammlungen ist die Online-Enzyklopädie *Wikipedia*. Für Computer ist *Wikipedia* allerdings zunächst nicht verständlich, da die Textinhalte für Menschen geschrieben sind.

Das hat sich in den vergangenen Jahren geändert: Umfassende maschinenlesbare Wissensbasen wie der von Google genutzte *Knowledge Graph* ermöglichen Computern ein Textverständnis, das darüber hinaus geht, nur die Begriffe etwa einer Suchanfrage in einem Text zu erkennen. Sie stellen vielmehr zwischen den Begriffen einen Bedeutungszusammenhang her und erlauben somit semantisches Suchen. Sie können also auch Fragen mit mehrdeutigen Begriffen richtig beantworten. Und dank des semantischen Verständnisses kennen Computer auch die Bedeutung von Texten, welche sich, wie die Artikel der *Wikipedia*, an Menschen richten.

Die Wissensbasen, die das tiefere Sprachverständnis ermöglichen, wurden weitgehend automatisch erstellt und werden ständig aktualisiert und erweitert. Der *Knowledge Graph* kennt mehr als zwanzig Millionen Personen, Orte, Filme, Arzneimittel, Sportereignisse und vieles mehr, dazu mehr als eine Milliarde Fakten über diese Einheiten und ihre Beziehungen untereinander. Google nutzt das gewaltige Wissen, um Suchanfragen besser zu verstehen, Suchresultate besser in Ranglisten zu ordnen, bessere Empfehlungen für Nutzer von Youtube und anderen Webportalen zu geben sowie für intelligente Vorschläge zu Restaurants, Konzerten und anderem.

Vor allem drei Projekte haben die Methoden zur automatischen Konstruktion derartig umfassender Wissensbasen entscheidend vorangebracht: *DBpedia*



an der FU Berlin und Uni Leipzig; *Freebase*, das von Google aufgekauft wurde und heute den Kern des *Knowledge Graph* bildet; und *Yago*, das wir seit dem Jahr 2005 am Max-Planck-Institut für Informatik entwickelt haben.

Eine wichtige erste Dimension digitalen Wissens besteht darin, Einheiten – Entitäten genannt – zu sammeln, eindeutig zu benennen und in semantische Klassen wie Personen, Orte, Organisationen oder Ereignisse einzuordnen. Das macht im großen Stil vor allem *Yago*, indem es mit cleveren Algorithmen Kategorienamen aus *Wikipedia* mit dem manuell erstellten Thesaurus *WordNet* verknüpft. Die resultierende Wissensbasis enthält nahezu zehn Millionen Entitäten und mehr als 300 000 feinkörnige und hierarchisch organisierte Klassen wie Politiker, Musiker, Bassisten, Rockballaden, Heavy-Metal-Songs, Benefizkonzerte oder Freiluftopern.

Die zweite Dimension einer Wissensbasis sind Fakten über Entitäten. Das sind zum einen Merkmale wie die Größe eines Fußballtorhüters oder die Anzahl seiner Länderspiele; zum anderen Beziehungen zwischen Entitäten, etwa der Geburtsort eines Torwarts, die Vereine, für die er gespielt hat, seine Ehefrau, die Hauptstadt eines Landes oder die Vorstandsmitglieder eines Unternehmens.

Sprache ist oft mehrdeutig. So lassen Namen und Phrasen mehrere Interpretationen zu.

Die dritte Dimension schließlich sind Regeln, die generelle Zusammenhänge ausdrücken – unabhängig von konkreten Entitäten. Dazu gehören Gesetzmäßigkeiten wie etwa die, dass jede Person genau einen Geburtsort hat und dass Hauptstädte von Ländern im jeweiligen Land liegen müssen. Solche Regeln können allerdings auch mit Unsicherheiten behaftet sein, müssen also nicht immer hundertprozentig zutreffen. Eine Person wohnt wahrscheinlich in derselben Stadt wie der Ehepartner oder in der Stadt, in der sie arbeitet.

Solches Allgemeinwissen brauchen Maschinen, um mehrere Fakten logisch zu verknüpfen. Hat man zum Beispiel keine Anhaltspunkte über den Wohnort von Angela Merkel, weiß man aber, dass ihr Ehemann an der Humboldt-Universität Berlin arbeitet, kann der Computer daraus schließen, dass die Kanzlerin in Berlin wohnt.

Sprache ist oft mehrdeutig. Das mag an der Satzstruktur liegen, viel häufiger aber lassen Namen und Phrasen mehrere Interpretationen zu. Um dies zu illustrieren, betrachten wir den Satz: „Page played Kashmir on his Gibson.“ Handelt es sich hier um den Google-Gründer Larry Page, der sich mit dem Schauspieler und Regisseur Mel Gibson am Rande des Himalaja trifft? Das macht offensichtlich keinen Sinn! Menschen erkennen dies aufgrund ihres Erfahrungsschatzes sofort, die Maschine jedoch muss das systematisch und algorithmisch analysieren. Tatsächlich ist hier die Rede von dem Led-Zeppelin-Gitarristen Jimmy Page, der den Song *Kashmir* auf einer Les-Paul-Gitarre der Firma Gibson spielt.

Um einen Satz aber wirklich zu verstehen, muss die Maschine auch die Beziehungen zwischen den beteiligten Entitäten erkennen und semantisch interpretieren. So kann sich das Verb „play“ auf Spiele, Sport, Musik, Trickserei und vieles mehr beziehen. Die Wahrscheinlichkeit, dass „play“ im Sinne der Relation *MusicianPerformsSong* verwendet wurde, ist eben sehr hoch, wenn die mehrdeutigen Namen „Page“ und „Kashmir“ auf einen Musiker und ein Musikstück hinweisen.

Umgekehrt spricht in einem Satz, der „play“ mit der genannten Bedeutung von *MusicianPerformsSong* verwendet, vieles dafür, dass der Satz auch einen Musiker und einen Song erwähnt. Diese wechselseitigen Abhängigkeiten in der Interpretation der Verbal- und Nominalphrasen werden mithilfe von Optimierungsalgorithmen gelöst.

Digitales Wissen in Kombination mit reichhaltiger Statistik und schlaun Algorithmen ermöglicht der Maschine also ein verblüffend tiefes Sprachverstehen. Und natürlich bleibt man nicht bei einzelnen Sätzen in Aussageform stehen, sondern betrachtet außerdem Fragen, ganze Absätze, lange Essays oder wissenschaftliche Publikationen und auch Dialoge mit dem Menschen.



Ein schwieriges Beispiel für einen Fragesatz ist etwa: „Who did scores for westerns?“ Da muss man analysieren, dass sich „scores“ auf Filmmusik bezieht, mit „westerns“ Westernfilme gemeint sind und die saloppe Formulierung „did“ im Sinne der Relation *ComposedMusic* zu interpretieren ist. Mit diesem Sprachverständnis kann der Computer direkt eine Antwort aus seiner Wissensbasis liefern – etwa Ennio Morricone, der zum Beispiel die Musik zum Film *Spiel mir das Lied vom Tod* komponiert hat.

Die Wissens- und Sprachtechnologie von Computern unterliegt heute noch massiven Grenzen. Oft steht und fällt alles mit dem Reichtum der zugrunde liegenden Statistiken oder dem Ausmaß an Training für Lernverfahren. Auch gibt es Sprachen wie Mandarin, die einer Syntaxanalyse schwer zugänglich sind und ein viel komplexeres Maß an Mehrdeutigkeit aufweisen als das Englische oder Deutsche. Bei manchen Sprachen wie Bambara oder Urdu existiert kein großer Korpus an digitalen Texten und damit auch keine umfassende Statistik.

Wenn wir jedoch den Fortschritt des vergangenen Jahrzehnts extrapolieren, kann man womöglich schon im Jahr 2020 mit Leistungen rechnen, die dem Bestehen des anfangs erwähnten Turing-Tests nahe kommen. Wir könnten dem Computer ein Schullehrbuch über Biologie „zum Lesen“ geben – und der Rechner würde anschließend Fragen auf dem Niveau einer mündlichen Abiturprüfung beantworten. Oder man denke an ein Spiel, in dem man gemeinsam mit anderen Onlinenutzern mit einer virtuellen Version des britischen Kochs Jamie Oliver Speisen zubereitet. Damit Jamie auf die Fehler seiner Lehrlinge bei der Zubereitung von Tiramisu richtig reagieren kann, muss der Computer die Gespräche und Gesten, die Mimik und visuellen Eindrücke analysieren und mit seinem Kochkunstwissen kombinieren.

Im Bereich der medizinischen Diagnose gab es vor dreißig Jahren den heute belächelten Versuch automatischer Expertensysteme. Dieses damals gescheiterte Unterfangen rückt heute in variiertem Form in Reichweite. Man stelle sich einen Arzt vor, der mit einem Patienten dessen Symptome und die Ergebnisse der ersten Labortests bespricht. Dabei hört der Computer zu und übernimmt die Rolle des beratenden Assistenten.

Mit seinem enzyklopädischen Fachwissen kann dieser digitale Assistent entscheidende Hinweise liefern auf Diagnosehypothesen, die sich ausschließen lassen, oder zusätzliche Untersuchungen empfehlen, die unterschiedliche Hypothesen spezifisch diskriminieren. Der Computer kann sich auch als Gesprächspartner einschalten, mit Fragen an den Arzt oder den Patienten. In diesem Zukunftsszenario hat die Maschine eine sehr wesentliche Rolle, überlässt aber Entscheidungen und Verantwortung dem menschlichen Experten.

**Wir werden potenziell zum
Spielball von Effekten, um die
wir nicht gebeten haben.**

Digitales Wissen und intelligentes Sprachverstehen machen nicht bei Nachrichten, prominenten Personen und Allgemeinwissen halt, sondern sind auch methodische Bausteine, um Wissen über uns alle und unsere Vorlieben zu sammeln und für smarte Empfehlungen und Mensch-Maschine-Interaktionen zu nutzen. Die Quelle dafür sind unsere vielfältigen Interaktionen mit dem Internet – sei es über unsere Mitgliedschaften in sozialen Netzen oder über unser Smartphone und alles, was wir mit ihm machen.

Damit werden wir potenziell auch zum Spielball von Benutzertracking, Werbung und anderen Effekten, um die wir nicht unbedingt gebeten haben. Im Jahr eins nach dem NSA-Skandal ist offensichtlich, wie stark unser aller Privatsphäre dadurch beeinträchtigt werden kann. Dabei spielt digitales Hintergrundwissen eine wesentliche Rolle, wie das folgende fiktive Szenario vor Augen führt.

Zoe, eine junge Frau aus Namibia, die in Europa studiert, stellt Fotos und anderes Material auf ihre Seite in einem sozialen Netzwerk. Dort empfiehlt sie ihren Freunden außerdem Filme und Musik, unter anderem die grönländische Indie-Rock-Sängerin Nive Nielsen. Zoe ist im Netzwerk unter ihrem richtigen Namen bekannt und verfügt über ein öffentliches Kurzprofil. >



Zoe hat Probleme mit ihrer Schilddrüse, nimmt das Medikament Synthroid und leidet unter Nebenwirkungen. Sie findet ein Onlineforum zu Gesundheitsthemen, wird unter einem Pseudonym Mitglied und beteiligt sich an Diskussionen. Zu guter Letzt benutzt Zoe auch Suchmaschinen, um nach alternativen Medikamenten zu recherchieren, etwa Levothroid, aber auch nach Filmen über Apartheid oder nach ihrer Lieblingsängerin Nive Nielsen. Die Suchmaschinen

Der Privacy Advisor verfügt über sehr persönliche Kenntnisse von Zoe.

erkennen Zoe nur als anonymen Nutzer, aber ein Internetbeobachter der Tracking- und Targeting-Branche kann ihre Such- und Clickhistorie über einen längeren Zeitraum sammeln.

Dieses vermeintlich harmlose Szenario hat es in sich. Ein Algorithmus mit Hintergrundwissen könnte Verknüpfungen zwischen Zoes drei Identitäten in der digitalen Welt herstellen. Der Angreifer könnte mithilfe einer Wissensbasis ermitteln, dass Synthroid und Levothroid Arzneien für dieselbe Art von Unterfunktion der Schilddrüse sind. Zusammen mit weiteren Hinweisen könnte er dann schließen, dass es sich im Gesundheitsforum und in der Suchhistorie um ein und dieselbe Person handelt.

Zudem gibt es eine extrem geringe statistische Wahrscheinlichkeit, dass sich zwei verschiedene junge Frauen aus Afrika für dieselbe grönländische Sängerin und andere Nicht-Mainstream-Themen interessieren. Der Angreifer kann somit die Suchhistorie mit Zoes Identität im sozialen Netzwerk verknüpfen. Schließlich folgt, dass Zoe dieselbe Person sein muss, die über ihre Schilddrüsenprobleme im Gesundheitsforum diskutiert. Das öffnet die Tür für unerwünschte Werbemails, mögliche Probleme mit der Krankenversicherung und andere – mehr als nur unangenehme – Konsequenzen.

Was wir hier skizziert haben, ist eine automatisierte Attacke auf Zoes Privatsphäre. Sie lebt von genau jener Wissens- und Sprachtechnologie des Computers, die wir zuvor als Segen und Hilfe für den Men-

schen angesehen haben. Eine systematische, nachhaltig wirkende Gegenmaßnahme könnte selbst auf digitalem Wissen und Sprachverstehen beruhen: ein persönliches Softwarewerkzeug, genannt Privacy Advisor. Es beobachtet kontinuierlich Zoes Verhalten im Internet, kennt ihre Aktivitäten und Vorlieben. Und es analysiert permanent das Risiko, inwieweit Zoe kritische Dinge von sich preisgibt, die ein mächtiger Angreifer ausnutzen könnte. Wenn das Werkzeug Alarm schlägt, sollte es Zoe die Lage erklären und vorschlagen, wie sie sich alternativ zu verhalten hat, um das Risiko zu verringern.

Der Privacy Advisor ist ein Konzept, das tatsächlich in hohem Maße auf maschinellem Wissen und Sprachverstehen basiert. Gegenüber potenziellen Angreifern besitzt es jedoch einen Vorteil: Es verfügt nicht nur über Welt- und Allgemeinwissen, sondern darüber hinaus auch über sehr persönliche Kenntnisse von Zoe. Damit Zoe dem Werkzeug vertrauen kann, muss es selbst als Open-Source-Software konzipiert und durch zahlreiche Programmierer überprüft sein. Seine Leistungsfähigkeit erhält es durch die an Zoe angepasste Konfiguration und die persönliche Wissensbasis.

An der Realisierung dieser Vision arbeiten Michael Backes (Universität des Saarlandes), Peter Druschel und Rupak Majumdar (Max-Planck-Institut für Softwaresysteme) sowie der Autor im Rahmen des durch einen ERC Synergy Grant geförderten Projekts IMPACT. Das Projekt zielt auf ein wissenschaftlich fundiertes Verständnis aller relevanten Dimensionen des sozialen Basars, zu dem sich das Internet entwickelt hat, und ihrer potenziellen Spannungen: Zusätzlich zur Privatsphäre (*Privacy*) sind die Verantwortlichkeit der Nutzer (*Accountability*), die Spezifikations-treue von Diensten (*Compliance*) und das Vertrauen in Information und Wissen (*Trust*) fundamentale Pfeiler, die ein künftiges Internet haben sollte.

Dieser Artikel hat beleuchtet, inwieweit der Computer Wissen und Sprache – intellektuelle Fähigkeiten, die dem Menschen vorbehalten zu sein scheinen – zu erwerben vermag. Dabei haben wir gesehen, dass Maschinen heute digitales Wissen in großem Umfang automatisch sammeln und organisieren und für ein immer besser werdendes Sprachverständnis nutzen. Die folgenden Thesen mögen zum weiteren Nachdenken und Diskutieren anregen:

Maschinen werden dem Menschen in nicht zu ferner Zukunft in vielen Anwendungssituationen haushoch überlegen sein, wie etwa beim Beantworten wissensintensiver Fragen oder der automatischen Zusammenfassung langer Texte oder ganzer Korpora und deren Aufbereitung für Analysen. Maschinen werden auch in der Lage sein, Abiturprüfungen zu bestehen. Dem Bestehen des Turing-Tests werden Maschinen damit sehr nahe kommen. Man kann dies als Simulation intelligenten Verhaltens ansehen, die auf Wissen, Statistik und Algorithmen beruht. Für den Effekt in Anwendungen ist es irrelevant, ob wir es mit „künstlicher“ oder „echter“ Intelligenz zu tun haben.

In Situationen, die Einfühlungsvermögen und kognitive Flexibilität erfordern, wird die Maschine dem Menschen nicht wirklich überlegen sein, sich aber als unverzichtbarer Assistent erweisen. Ein Beispiel dafür ist die Hilfe bei medizinischen Diagnosen, wo der Computer als nahezu vollwertiger Gesprächspartner für Arzt und Patient fungieren kann. Es wird aber auch immer Situationen geben, in denen uns die Maschine nicht zu imitieren vermag: Humor, Ironie, Flirten und andere Emotionen bleiben sicher noch lange dem Menschen vorbehalten.

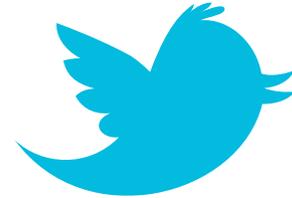
**Wir können Computern beibringen,
uns zu warnen, wenn wir im Internet
zu viel preisgeben.**

Da Computer zunehmend die Bedeutung von Texten in sozialen Medien analysieren und Zusammenhänge zwischen Begriffen herstellen, eröffnen sich ihnen völlig neue Anwendungsmöglichkeiten – aber nicht nur zum Besten der Nutzer: Das semantische Verständnis befähigt die Maschinen auch, uns Menschen umfassender zu analysieren. Doch wir müssen uns dem nicht ausliefern: Schließlich können wir Computern beibringen, uns mit ihrem Sinn für Bedeutungen und Zusammenhänge zu warnen, wenn wir im Internet zu viele Informationen preisgeben, die Algorithmen zu detaillierten Persönlichkeitsprofilen verknüpfen könnten. ◀

DER AUTOR



Prof. Dr. Gerhard Weikum, Jahrgang 1957, studierte Informatik und promovierte an der TU Darmstadt. An dieser Hochschule arbeitete er 1987 als wissenschaftlicher Assistent. Weitere Stationen als Postdoc waren das MCC in Austin sowie die ETH Zürich, wo er zwischen 1990 und 1994 auch eine Professur innehatte. In dieser Funktion ging er danach an die Universität des Saarlandes in Saarbrücken. Seit 2003 ist er Direktor und wissenschaftliches Mitglied am Max-Planck-Institut für Informatik.



Das Echo des digitalen Gezwitschers

Twitter, Facebook & Co. – soziale Medien beherrschen zunehmend das Internet. Wie aber breiten sich Nachrichten über diese neuen Plattformen aus? Welche Rolle spielt dabei eine kleine Clique von Super-Einflussreichen? Und inwiefern sind die alten Massenmedien auch online ganz vorn mit dabei? Diese Fragen beschäftigen **Krishna Gummadi** am **Max-Planck-Institut für Softwaresysteme** in Saarbrücken.

TEXT **RALF GRÖTKER**

Krishna Gummadi besitzt nicht weniger als 1,75 Milliarden Tweets – Textnachrichten des Social-Media-Dienstes Twitter. Das Unternehmen bietet Nutzern die kostenlose Möglichkeit, über einen Computer oder ein internetfähiges Mobiltelefon Nachrichten an andere Teilnehmer, die sich zu Anhängern des Absenders erklärt haben, zu twittern (engl. für zwitschern). Jeder Beitrag besteht aus maximal 140 Zeichen (was der Länge dieses Satzes entspricht), meist inklusive eines Hinweises auf eine Webadresse. „Eine Goldgrube“, sagt der 31-jährige Inder. Der Schatz liegt sicher verwahrt auf 58 Computerservern in der „Wartburg“ – einem trutzigen, in den 1920er-Jahren erbauten Gemeindehaus in der Saarbrücker Innenstadt.

Hier, in direkter Nachbarschaft zur Sparkasse und zu einer Kreditkarten-Firma, ist das Max-Planck-Institut für Softwaresysteme untergebracht, jedenfalls bis der Neubau des expandierenden Instituts auf dem Universitätscampus fer-

tig ist. Gummadi leitet seit 2005 die Forschungsgruppe „Networked Systems Research“. Um seine Leidenschaft für die 1,75 Milliarden Tweets zu verstehen, muss man etwas weiter ausholen.

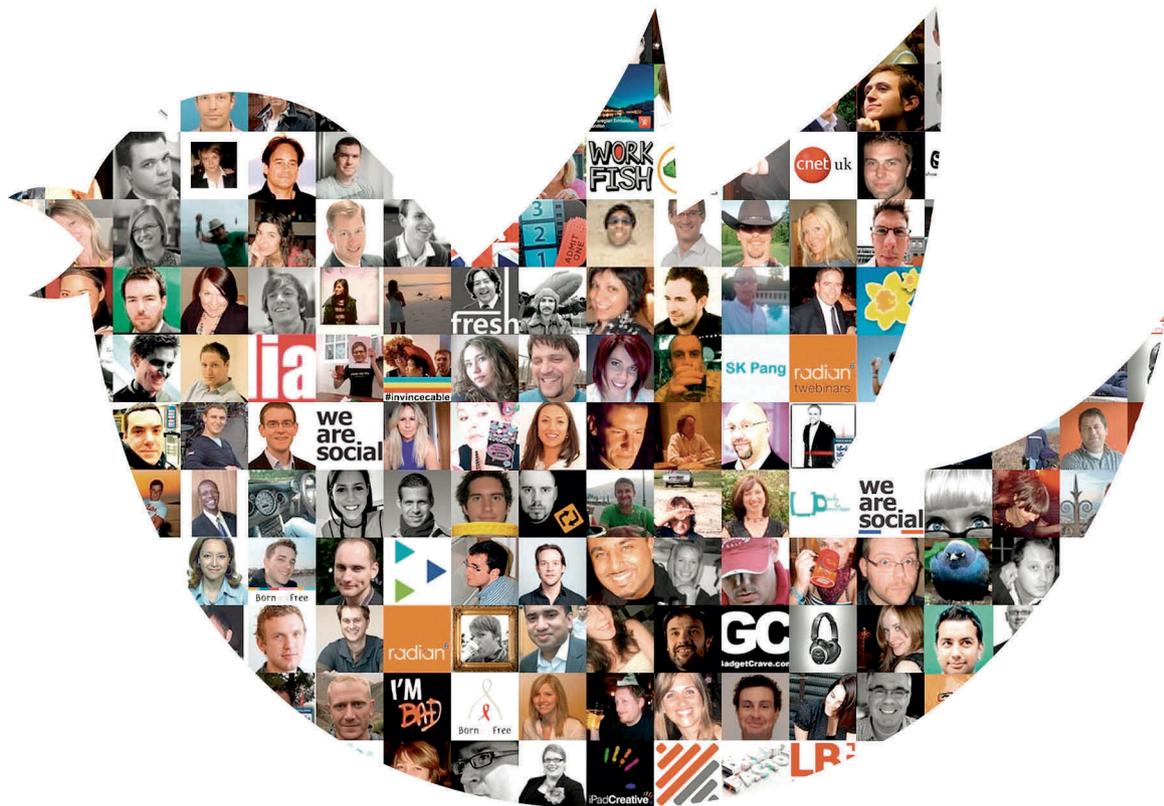
Anfang 2003 brach im Prince of Wales-Krankenhaus in Hongkong die SARS-Epidemie aus. Untersuchungen zeigten später: Ein einziger Patient hatte 50 Mitpatienten auf direktem Weg infiziert, was schlussendlich zu 156 SARS-Fällen allein in besagtem Krankenhaus führte – und dann zum Ausbruch der Epidemie weit über die Stadt hinaus.

VERBREITEN VIREN SICH WIE MODESTRÖMUNGEN?

Ganz ähnlich wie mit Krankheiten scheint es sich mit Ideen und Moden zu verhalten. Der plötzliche Erfolg der Schuhmarke Hush Puppies ist dafür ein Beispiel. Mitte der 1990er-Jahre war der Absatz für die bequemen Kreppsohlentreter auf einem Tiefpunkt angelangt. Dann, plötzlich, geschah das

Unerwartete: Der New Yorker Modedesigner John Bartlett bestellte eine Serie Hush Puppies für die Präsentation seiner Frühjahrskollektion. Er war auf die Schuhe aufmerksam geworden, weil einige Leute in der New Yorker Clubszene sie zu tragen begonnen hatten. Eine Hush-Puppies-Epidemie brach aus. 1995 verkaufte die Firma 430 000 Paar Schuhe – 400 000 mehr als im Vorjahr; im Jahr darauf gingen sogar knapp zwei Millionen Paar über die Ladentheken.

Der amerikanische Wissenschaftsautor Malcolm Gladwell, der die Geschichte in seinem Buch *The Tipping Point* beschreibt, hat für derartige Vorkommnisse eine einfache, aber plausible Erklärung. Epidemien werden von *Influentials* losgetreten – Leuten in einer besonderen beruflichen und sozialen Position, aber auch mit einer bestimmten Begabung und Lebenseinstellung, die es ihnen ermöglicht, mit einer ungeheuer großen Anzahl von Menschen in persönlichen Kontakt zu treten.



Collage: designergold nach einer Vorlage von fotolia

Die schon seit den 1950er-Jahren vor allem in der Marketingwelt als Standardwissen zirkulierende Theorie der sozialen Epidemie wurde in der jüngeren Vergangenheit immer wieder stark kritisiert. Ein Einwand: Die Verbreitung von Viren und von Moden sei nicht vergleichbar, weil das Infektionsrisiko bei wiederholtem Kontakt mit dem Erreger im Falle eines Virus jedes Mal gleich hoch ist, bei einer Mode jedoch sowohl Mitzieh- wie Abstumpfungseffekte entstehen können. Ein anderer Vorwurf: Leute wie Gladwell würden sich die Anekdoten so auswählen, wie sie ihnen ins Konzept passten.

Oft zeigt tatsächlich schon ein näherer Blick auf die Ereignisse, dass vermeintliche Schlüsselpersonen lediglich ein Produkt der Umstände sind. Gerade der oben erwähnte SARS-Ausbruch in Hongkong ist dafür exemplarisch. Im Prince of Wales-Krankenhaus begann alles damit, dass bei dem besagten Patienten fälschlicherweise eine Lungenent-

zündung diagnostiziert wurde. Statt ihn zu isolieren, wurde er in einem offenen, überfüllten Saal mit schlechter Luftzirkulation untergebracht. Man schloss einen Bronchien-Ventilator an seine Lungen an – der die SARS-Viren in der Umgebung verteilte. Als Beleg für die *Influentials*-Theorie ist der Fall daher ein denkbar schlechtes Beispiel.

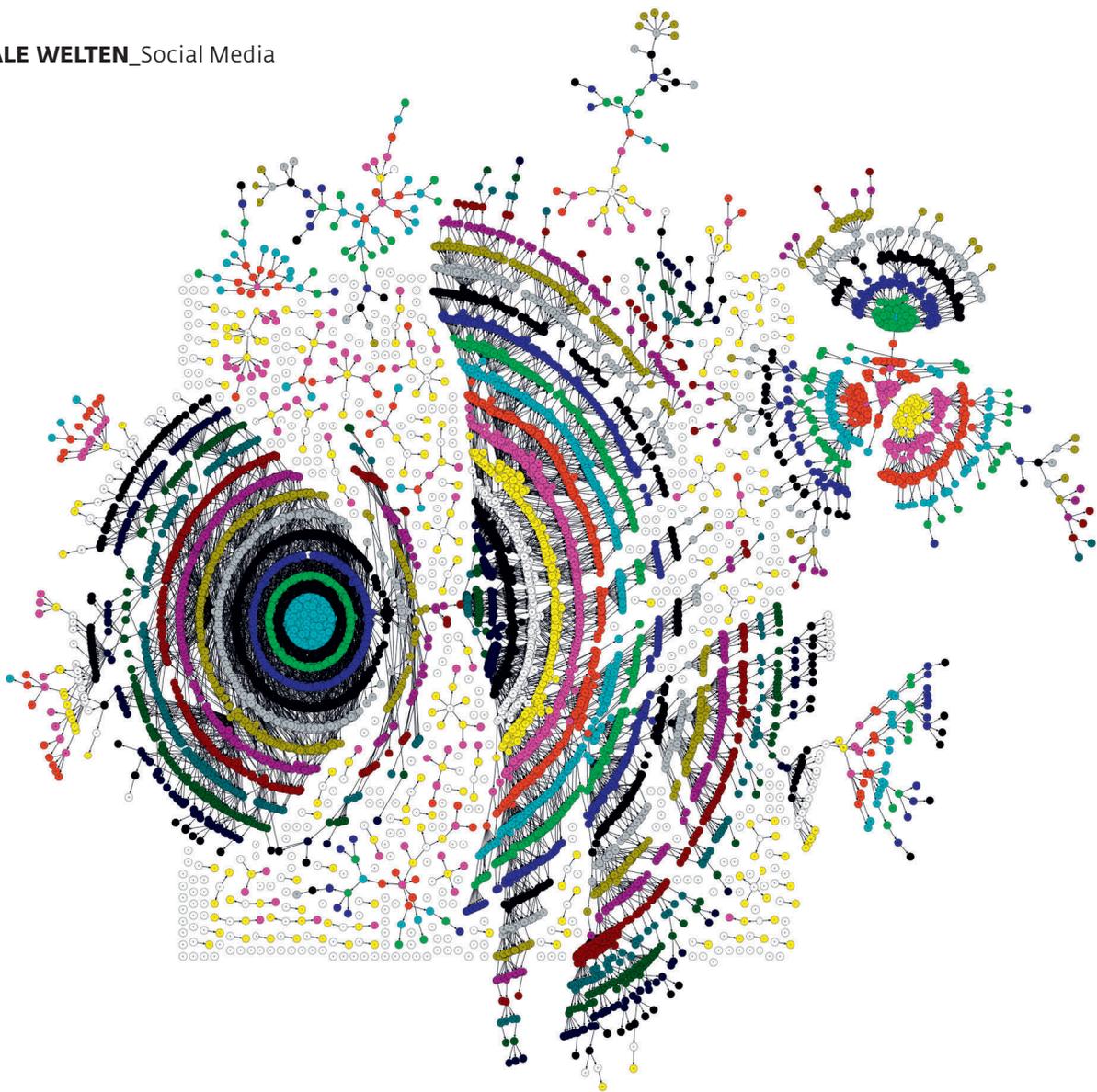
DIE ERSTE EMPIRISCHE STUDIE SOZIALER NETZWERKE

Hier kommt nun Krishna Gummadi ins Spiel. Die Forschungen, an denen er vor allem mit seiner mittlerweile als Assistent Professor am Korean Institute of Science and Technology tätigen Mitarbeiterin Meeyoung Cha gearbeitet hat, versprechen nämlich den Streit um die *Influentials* zu klären. Gummadi untersucht seit mehreren Jahren die Informationsflüsse sozialer Netzwerke in Internet-Communitys wie Facebook, LiveJournal, LinkedIn (dem amerikanischen Pendant zu Xing) und Twitter.

Der Vogel, der die neuesten Nachrichten vom Dach pfeift, ist blau und dient Twitter als Logo (links). Die Nutzer verwenden Fotos oder Symbole als Erkennungsmarken (rechts).

Was sich innerhalb dieser Online-Netzwerke tut, wie sich etwa Moden verbreiten, gibt wichtige Aufschlüsse auch über die Verbreitung von Viren und sozialen Epidemien in der physischen Welt. Denn hier wie dort sind die grundlegenden Strukturen Netzwerke – mit durchaus vergleichbaren Eigenschaften.

Einige der ersten Arbeiten überhaupt, welche die Entwicklung von Online-Netzwerken in großem Stil nachzeichnen, sind 2007 von Gummadis Gruppe veröffentlicht worden. Seit Neuestem untersucht er in einer groß angelegten Reihe von Studien das Nutzungsverhalten des Online-Dienstes Twitter. In der zweiten Hälfte des Jahres 2009 haben die Forscher Informationen – mit spezieller Erlaubnis von Twitter und unter Berücksichtigung



Eine Meldung schlägt Wellen: Die Grafik zeigt, wie eine Web-Adresse über Twitter verbreitet wird. Jeder der mehr als 14 000 Knoten, die in den großen Verbreitungsbäumen auch in mehreren Ebenen übereinanderliegen, repräsentiert einen Nutzer. Die Farben geben die Stufen der Verbreitung wieder (weiß, gelb und so weiter – nach der 15. Verbreitungsstufe wiederholt sich die Farbcodierung). Der Ausgangspunkt und die ersten weiterführenden Knoten des prominenten Baums in der linken Bildhälfte liegen unter dem türkisen Punkt verborgen.

der üblichen Richtlinien des Datenschutzes – von knapp 55 Millionen Twitter-Konten „gecrawlt“: Im Prinzip öffentliche, aber eben nicht in gesammelter Form vorliegende Informationen wurden durch wiederholte Datenabfragen an die Twitter-Webseite gesammelt. Aus diesen 55 Millionen wurden wiederum sechs Millionen aktive Nutzer herausgefiltert. Diese Nutzer hatten einander wiederum die erwähnten 1,75 Milliarden Tweets gesendet.

Auf der Grundlage der neuen Daten ist es erstmals möglich, empirisch zu untersuchen, wie sich Ideen und Moden in sozialen Netzwerken verbreiten – und damit gängigen Theorien der Mundpropaganda oder der Innovationsverbreitung auf den Zahn zu fühlen.

Eine Studie, an der das Max-Planck-Team derzeit arbeitet, soll zeigen, ob es verschiedene Nutzer sind oder immer wieder dieselben, die mit Erfolg ihre Twitter-Kollegen auf eine bestimmte Webseite hinweisen. Bis vor Kurzem war es lediglich möglich, solche Fragen mithilfe von Computersimulationen oder anderen Modellen zu untersuchen.

RANGFOLGE EINFLUSSREICHER TWITTER-NUTZER

Duncan Watts, ehemals Soziologe an der New Yorker Columbia-Universität und heute in der Forschungsabteilung bei Yahoo, kam bei einem Test verschiedener Modellierungsverfahren zu dem Ergebnis, dass die *Influentials* zwar un-

ter bestimmten Umständen eine Rolle spielen könnten – aber dass diese Umstände eng definiert sind und vermutlich relativ selten eintreten. *Influentials*, so das Resümee seiner Studie, sind weniger Leute mit bestimmten Eigenschaften als vielmehr solche, die einfach Glück gehabt haben.

Genau hieran knüpft die neue Twitter-Studie an. Bei der Formulierung von Hypothesen und dem Design von Versuchen greift die Studie auf die im Feld der Netzwerk-Analyse etablierten Methoden zurück. Das Vorgehen ist allerdings empirisch. In den Daten suchten die Forscher gezielt danach, welche Webseiten die Twitter-Nutzer einander empfohlen hatten. Dann legten sie eine Rangliste an, die zeigen soll, welche

» Ohne die Massenmedien geht gar nichts. Dennoch wirkt die große Mehrheit aus weniger gut verlinkten Twitter-Nutzern wie ein Verstärker für Nachrichten von den Massenmedien.

Nutzer zur Verbreitung einer bestimmten Webseite am meisten beigetragen hatten. Zu diesem Zweck durchforsteten die Wissenschaftler Millionen von Twitter-Nachrichten nach darin genannten Webseiten-Adressen und diese wiederum nach Korrelationen und Mustern. „Eine ziemlich haarige Angelegenheit“, sagt Gummadi. Selbst große Rechneranlagen stoßen bei derartigen Aufgaben an die Grenzen ihrer Kapazitäten.

Nun liegt der Einwand nahe, dass man genauso wenig vom Verhalten in Online-Netzwerken wie Twitter auf andere soziale Phänomene schließen kann wie von der Verbreitung von Viren auf soziale Epidemien. Strikt betrachtet stimmt das. Andererseits helfen gerade die Analysen von sozialen Medien, ein Gespür dafür zu entwickeln, welche Feinheiten entscheidende Unterschiede machen können – sowohl online als auch auf der Straße.

So etwa hat die Studie eines Teams um Jure Leskovec von der Carnegie Mellon University ergeben, dass auf der in den USA populären Produkt-Empfehlungsseite Epinion die meisten Empfehlungsketten nach wenigen Schritten im Nichts enden – was per se erst einmal eine schlechte Voraussetzung für die Verbreitung von sozialen Epidemien ist. Anders verhält es sich bei der Fotoseite Flickr, mit der sich eine Vorgängerstudie von Gummadis Twitter-Analyse befasst. „Die meisten Bilder finden hier keine große Verbreitung“, fasst Krishna Gummadi das Ergebnis zusammen. „Einige wenige Superstars unter den Fotos machen einen Großteil der Empfehlungen aus.“ Hier liegen die Voraussetzungen für Epidemien also günstiger.

Eine neulich veröffentlichte Studie, die auf dem Twitter-Datensatz basiert, untersucht detailliert, wie sich die verschiedenen Kommunikationswege innerhalb von Twitter unterscheiden. Auf Twitter ist es möglich, jemandem einfach nur zu „folgen“, also dessen Nachrichten zu beziehen – ohne dass diese Gefolgschaft, so wie die „Freundschaft“ auf Facebook, der Bestätigung des Ge-

genübers bedarf. Man kann, zweitens, Nachrichten weiterleiten – an die Personen, die einem selbst „folgen“. Drittens: Man kann auf Nachrichten antworten.

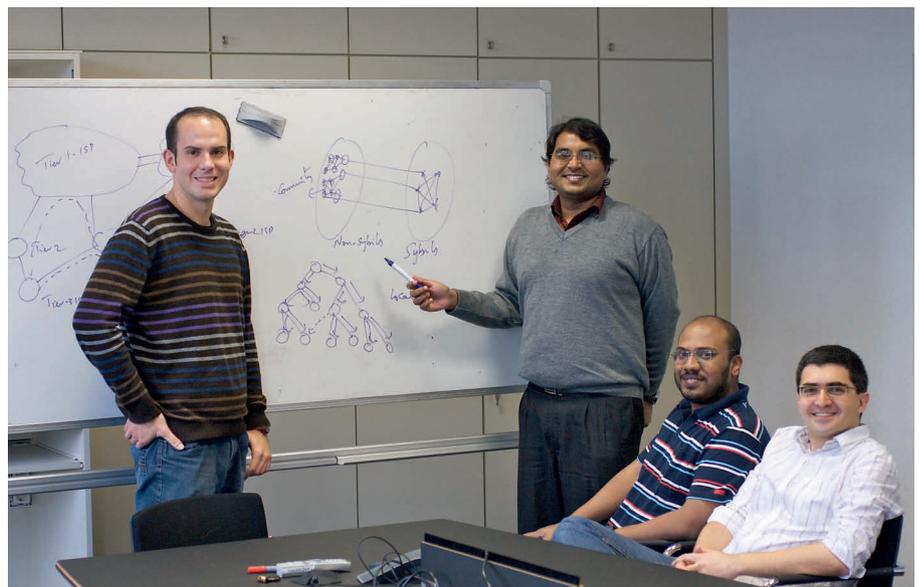
DIE STARS ERHALTEN DIE MEISTEN ANTWORTEN

Wenn man diese drei Aktionsformen jeweils für sich untersucht, hat man nicht mehr ein, sondern quasi drei Twitter-Netzwerke vor sich. Das Resultat: In der Kategorie „Nutzer mit den meisten Followern“ waren Nachrichtenmagazine sowie Stars und Politiker die einflussreichsten Akteure. In der Kategorie „Weitergeleitet“ hatten ebenfalls die News-Anbieter die Nase vorn, aber auch prominente Business-Ratgeber. Die meisten „Antworten“ schließlich erhielten die Stars. Was heißt: Tausende von Followern zu haben, macht einen Twitter-Nutzer nicht notwendig zum *Influential* – jedenfalls ist es kein Indiz dafür, dass die Botschaft, die man verbreiten will, auch aufgenommen und weiter verbreitet wird.

Daneben zeigte die Studie: Einflussreiche Twitter-Nutzer sind meist nicht nur auf einem einzigen Gebiet, sondern in verschiedenen Themenfeldern erfolgreich (dies im Gegensatz etwa zu den Communitys auf der Plattform Epinion, die sich meist um ein spezielles Produkt drehen). Und: Die Einflussreichen sind keine Eintagsfliegen. Sie bleiben über einen längeren Zeitraum erfolgreich. „Einfluss ist hier kein Zufallsprodukt, sondern das Ergebnis konzertierter Bemühungen“, hält Gummadis Studie in Entgegnung auf den *Influentials*-Skeptiker Watts fest.

Noch etwas fällt ins Auge: die hervorgehobene Rolle, welche die Massenmedien oder deren Repräsentanten in den sozialen Online-Netzen spielen. Diese Rolle entspricht nicht unbedingt dem, was man sich unter Mundpropaganda vorstellt. Krishna Gummadis Team hat diese Beobachtung gleich zum Anlass einer neuen Studie genommen. „Wir wollten wissen: Was passiert, wenn wir hoch verlinkte Akteure wie die Seiten von Nachrichtensen-

Einer Nachricht auf der Spur: Massimiliano Marcon, Krishna Gummadi, Bimal Viswanath und Nuno Santos (von links) diskutieren, wie sich Information in sozialen Gruppen ausbreitet.



dern und Zeitungen einfach aus dem Spiel entfernen?“), sagt der Netzwerkforscher.

NÜTZLICHE ANALYSEN FÜR MARKETING-EXPERTEN

Man wählte das Auftauchen der britischen Amateur-Schlagersängerin Susan Boyd in den Twitter-Nachrichten von 2009 als Testereignis. Das Resultat: 60 Prozent aller Twitter-Nutzer erfuhren durch Tweets, die von den Nachrichtenseiten kamen, zuerst von Boyd. Was bedeutet: Ohne die Massenmedien geht gar nichts. Dennoch wirkt die große Mehrheit aus weniger gut verlinkten Twitter-Nutzern wie ein Verstärker für von den Massenmedien kommende Nachrichten. Diese Mehrheit hatte an der Verbreitung der Nachricht von Susan Boyd einen Anteil von immerhin fünf Prozent.

Noch vieles mehr ließe sich mittels der Twitter-Daten untersuchen. „Mich würde interessieren, ob Dienste, die für Empfehlungen genutzt werden, dazu führen, dass die Spannweite der individuell konsumierten Medien zunimmt – ob ich also Dinge lese, von denen ich auf dem Wege der herkömmlichen Massenmedien gar keine Kenntnis hätte“, sagt Gummadi. Ein anderes Vorhaben: „Wir könnten herausfinden, wie sich Moden und Gepflogenheiten verbreiten.“ So wurde es in letzter Zeit auf Twitter üblich, anstelle ellenlanger www-Adressen Kürzel einzusetzen, sogenannte Tiny-URLs. In dem Datensatz ließe sich

genauestens verfolgen, wer wann welche Form von Tiny-URLs ins Spiel gebracht hat. „So etwas wäre nützlich als Anhaltspunkt dafür, wie sich Innovationen verbreiten.“

Für Marketingexperten könnten die Resultate solcher Analysen durchaus nützlich sein. Auch hier ist man mittlerweile von dem Glauben an die Macht der *Influentials* abgerückt. „Das Web hat sich verändert. Heute ist nahezu jeder bei Xing oder Facebook angemeldet – da können wir gar nicht mehr sagen, wer der Relevanteste ist“, meint Christian Wilfer, Geschäftsführer der auf virales Marketing spezialisierten Agentur Dialog-Solutions. Und: „Es kommt immer auf das Produkt an“, ergänzt Mundpropaganda-Experte Martin Oetting von trnd. „Wenn ich einen Weichspüler bewerbe, dann gibt es dafür kaum eine Gruppe von besonders einflussreichen Vermittlern. Viel wichtiger sind hoch involvierte Normalverbraucher.“

Dementsprechend verhält es sich auch mit der Strategie der Marketing-Community trnd: Statt einiger weniger werden viele tausend Konsumenten, die sich als Produkttester auf der Online-Plattform von trnd registriert haben, mit Neuigkeiten sozusagenimpft. Anders als bei Dialog Solutions, die mit ihrer Plattform Shareifyoulike einen ähnlichen Plan verfolgen, konzentriert sich trnd jedoch auf die Offline-Kommunikation – weil Leute ihren Freunden doch anders zuhören als den „Friends“ auf Facebook.

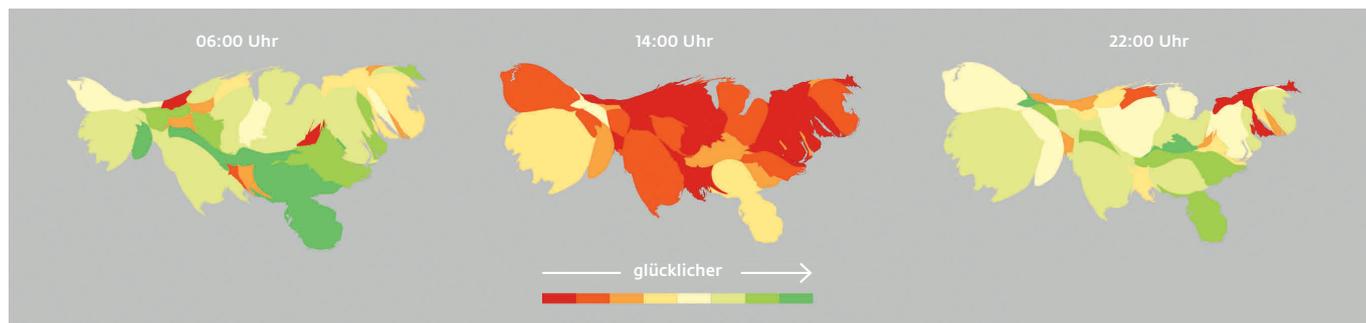
Relevant für praktische Anwendungen ist die Analyse von Netzwerken in sozialen Medien, wie sie Krishna Gummadi und seine Kollegen in Saarbrücken betreiben, aber nicht nur für die Marketing- und Innovationsforschung. Die genaue Kenntnis von Netzwerkstrukturen ist auch die Voraussetzung von Algorithmen zur Spam-Bekämpfung. Spammer steigern ihre Online-Reputation, indem sie ihre Seiten und Benutzerkonten so häufig wie möglich verlinken. Oft entstehen so aber lediglich in sich geschlossene Verlinkungs-Universen – ohne Verbindung zu den Clustern der ehrbaren Netzbürger. Mithilfe von Algorithmen lassen sich solche Spam-Cluster identifizieren und lahmlegen.

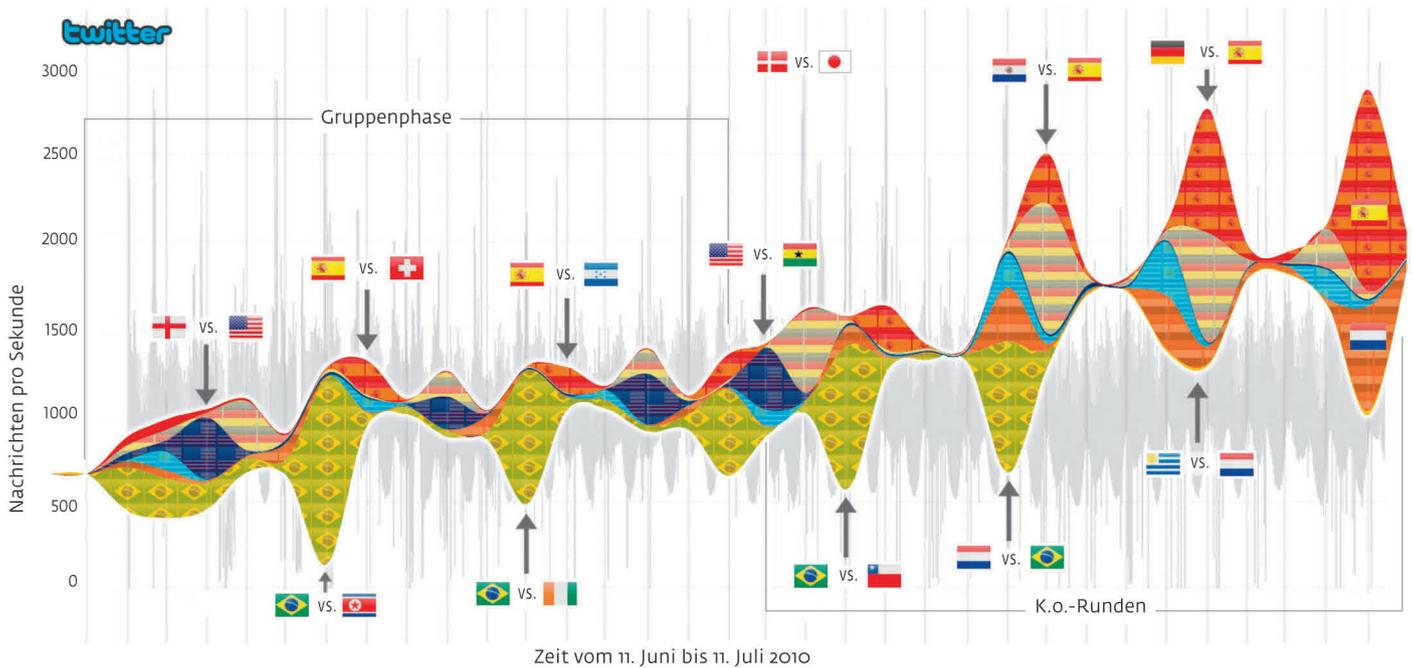
SUCHE IM SOZIALEM UMFELD MACHT GOOGLE KONKURRENZ

Ein weiteres Anwendungsgebiet ist *social search*: die Suche nicht im World Wide Web, sondern innerhalb der Gemeinschaft Gleichgesinnter. Ein Prototyp eines solchen Suchverfahrens wurde vor einigen Jahren unter der Leitung von Gummadis damaligem Studenten Alan Mislove entwickelt, der heute als Assistant Professor an der Northeastern University in Boston lehrt. „Wir wollten wissen, wie stark man bei der Suche von der sozialen Umgebung profitieren kann“, sagt Mislove.

Wann immer einer der zehn am Projekt beteiligten Forscher eine Webseite aufrief, wurden deren Bezeich-

Die USA im täglichen Wechselbad der Gefühle: Anhand der in Twitter-Nachrichten verwendeten Wörter, denen Punktzahlen für Stimmungen zugeordnet sind, lässt sich zu verschiedenen Tageszeiten die Stimmungslage der Twitter-Nutzer in den einzelnen US-Bundesstaaten abschätzen. Rot steht für eher schlechte Laune, Grün für bessere. Demnach sind die Menschen in den westlichen und südöstlichen Staaten generell fröhlicher, am frühen Nachmittag erreicht die Stimmung jedoch überall einen Tiefpunkt. Die Verzerrungen der Staaten ergeben sich, weil ihre Flächen widerspiegeln, wie hoch der Anteil der dort abgesetzten Nachrichten an allen Tweets in den USA liegt.





Twittern zu Zeiten der Fußballweltmeisterschaft 2010: Die Grafik gibt für den Zeitraum vom 11. Juni bis 11. Juli wieder, wie viele Twitter-Nachrichten pro Sekunde den Namen des Landes als markierten Schlüsselbegriff enthielten, dessen Flagge den Peaks unterlegt ist. Um die Nachrichtendichte zu den ausgewählten Ländern besser auseinanderhalten zu können, weisen die Peaks mal nach oben und mal nach unten. Insgesamt stieg die Zahl der Tweets mit Ländernamen gegen Ende der WM. Grau im Hintergrund erkennt man die Gesamtzahl der Tweets pro Sekunde.

nung und Inhalt im institutseigenen Netzwerk gespeichert. Startete einer der Wissenschaftler dann eine Internetsuche, wurde ihm als Ergebnis neben der Google-Liste eine Liste aus den vom Team besuchten Webseiten präsentiert. Der Vorteil: „PeerSpective“, so der Name des Projekts, zeigte auch Ein-

träge in Online-Bibliothekskatalogen an, die auf Google gar nicht verzeichnet sind.

Knapp acht Prozent aller tatsächlich angezeigten Suchergebnisse, so das Resultat der Pilotstudie, konnten ausschließlich mit PeerSpective gefunden werden. So gut schafft es selten

jemand, sich neben Google zu behaupten. Mislove ist dies mit Software gelungen, die er innerhalb von nur einer Woche im Alleingang zusammengebastelt hat.

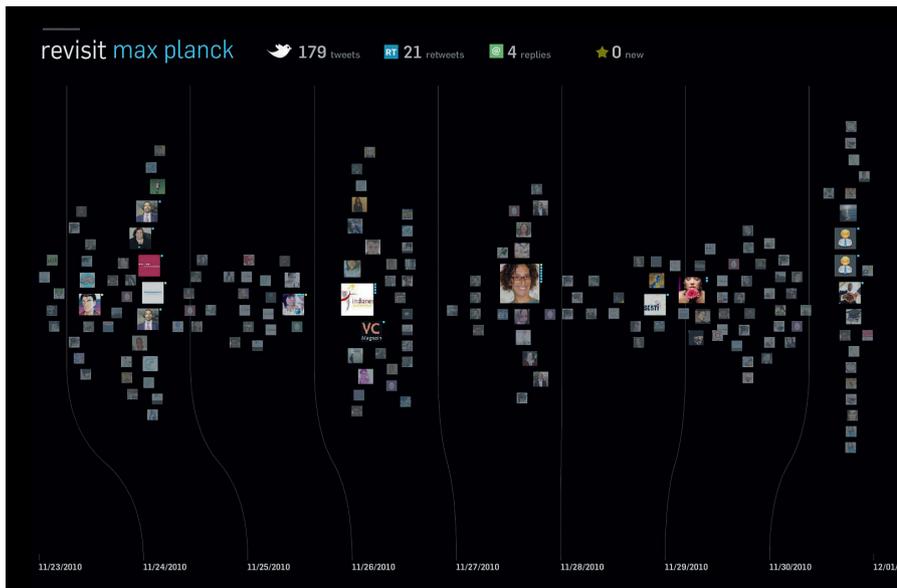
Erste Suchmaschinen, die sich des Prinzips von PeerSpective bedienen, gibt es bereits auch auf dem Markt. So etwa das von der kalifornischen Firma Eurekster angebotene Swicki. Auch in den Forschungsabteilungen von Yahoo, Google und Microsoft existieren Pläne für *social search*. Durchgesetzt haben sich statt neuartiger Suchmaschinen jedoch bislang eher integrierte Lösungen wie „See what your friends are sharing on facebook“ und „E-mailed – Blogged – Viewed most“ auf den Seiten der NEW YORK TIMES oder der Integration von „Buzz“ in Googles „gmail“.

Aber einerlei wie *social search* angegangen wird: Damit der Ansatz funktioniert, kommt es zunächst darauf an, für eine bestimmte Suchanfrage erst einmal die passende Community zu finden. Dieses Vorhaben gingen Gummadi und seine Leute vor Kurzem an. Sie versuchten, mit einem der üblichen Algorithmen Gruppen innerhalb eines Netzwerks aufzuspüren, um so Menschen

FISCHEN NACH INFORMATIONEN

Ein Großteil der Inhalte von Social-Media-Plattformen ist öffentlich zugänglich, weil die Nutzer dieser Veröffentlichung zugestimmt haben. Im Normalfall kann jedoch nur das Unternehmen, welches eine Social-Media-Plattform betreibt, auf die Gesamtheit dieser Daten zugreifen, um diese etwa statistisch auszuwerten. Allerdings ist es auch von außen möglich, durch automatisierte Suchanfragen Informationen, die innerhalb der sozialen Netzwerke in verstreuter Form vorliegen, zu sammeln und zusammenzuführen. Diese Suchanfragen erfolgen mit der Hilfe eines digitalen Suchroboters – „Web-Crawler“ genannt. Auch Internet-Such-

maschinen verwenden Crawler, um einen Index der im World Wide Web vorhandenen Seiten zu erstellen. Auf diesen Index wird dann bei der aktuellen Suchanfrage zurückgegriffen. Die meisten Social-Media-Seiten limitieren die Anzahl von Suchanfragen, die ein bestimmter Internet-Nutzer tätigen darf, damit nicht Dritte einen wirtschaftlichen Vorteil aus der Analyse der Datenbanken ziehen. Forscher, die mittels „Crawling“ Aufschluss über die Beschaffenheit von Netzwerkstrukturen in Social Media erzielen wollen, müssen deshalb meist zuvor eine Genehmigung des jeweiligen Social-Media-Dienstes einholen.



Wer twittert wann über die Max-Planck-Gesellschaft? Für die Zeit vom 23. November bis 1. Dezember 2010 gibt die Grafik wieder, wann Nachrichten mit den Wörtern „Max Planck“ versendet wurden. Vertikal übereinanderstehende Symbole symbolisieren Tweets, die zur selben Zeit abgesetzt wurden. Dabei sind die Tweets desto weiter in der Mitte dargestellt je mehr Antworten es auf sie gab oder je häufiger sie weitergezwitschert wurden. Groß dargestellt werden entweder neue Nachrichten oder – wie hier im Fall einer rückblickenden Analyse – zufällig ausgewählte Nachrichten. Die Max-Planck-Gesellschaft ist seit Oktober 2010 auf Twitter aktiv.

mit ähnlichen Interessen herauszufiltern. Erstaunlicherweise konnte aber der Algorithmus einige Gruppen, von denen man wusste, dass sie existierten, nicht detektieren.

TWITTER-NACHRICHTEN ALS STIMMUNGSBAROMETER

Hier musste erst ein wenig Soziologie ins Spiel kommen. Gruppen nämlich sind nicht gleich Gruppen. Einige Gruppen (in der Soziologie „Gemeinschaften“ genannt) werden durch persönliche Verbindungen zusammengehalten: „So wie einige von uns hier am Institut sich jede Woche treffen, um Poker zu spielen – weil wir einfach gern zusammensitzen“, wie Krishna Gummadi lächelnd sagt. Andere Gruppen (die „Gesellschaften“) sind themenbezogen – „so wie Greenpeace“. In themenbezogenen Gruppen kennen die meisten Teilnehmer einander gar nicht. Gummadi: „Auf diesen Unterschied mussten wir erst mal kommen. Der von uns zuerst eingesetzte Algorithmus, der lediglich Teilnehmer herausfilterte, die durch besonders wenige Zwischenschritte miteinander verbunden waren, konnte diese Cluster deshalb gar nicht finden.“

Wenn man Krishna Gummadi zuhört, scheint die Spanne der praktischen Belange, in denen die Ergebnisse der Analyse von Netzwerken in den

sozialen Medien zum Tragen kommen könnten, schier unendlich zu sein. Eine der neuesten Arbeiten ist ein nationales Stimmungsbarometer. Alan Mislove hat Twitter-Nachrichten in den USA daraufhin ausgewertet, welche emotionale Befindlichkeit sich in ihnen widerspiegelt. Das Ergebnis ist in einer animierten Landkarte wiedergegeben, in der die einzelnen Bundesstaaten auf einer Farbskala von grün (*happy*) über gelb (*neutral*) bis rot (*not happy*) rangieren – und im Verlauf des Tages die Farbe wechseln.

Für sich genommen, ist das Stimmungsbarometer nur eine Spielerei. Aber es demonstriert, welche Informa-

tionen in den sozialen Medien schlummern. Die Betreiber von Twitter wissen buchstäblich, wie die Welt tickt. Sie können beobachten, worüber die Leute reden und was sie mit ihrem Geld machen. Daraus kann man Prognosen ableiten – ob Aktien von Automobilkonzernen sinken oder fallen, oder welchen Erlös ein soeben gestarteter Kinofilm am Ende der ersten Woche einspielen wird. Das ist schon faszinierend. Andererseits: „Es ist wirklich verrückt, welche Macht diese Unternehmen haben“, so Gummadi. Von daher kann man schon verstehen, warum einem 1,75 Milliarden Tweets als Goldgrube erscheinen. ◀

GLOSSAR

Social Media: Online-Plattformen für den Austausch von Meinungen, Nachrichten und medialen Inhalten wie Fotos innerhalb von sozialen Netzwerken. Zu den in Deutschland verbreiteten Social Media gehören die Business-Community Xing, die auf Studenten ausgerichtete Plattform StudiVZ, Facebook, der Fotodienst Flickr sowie Twitter.

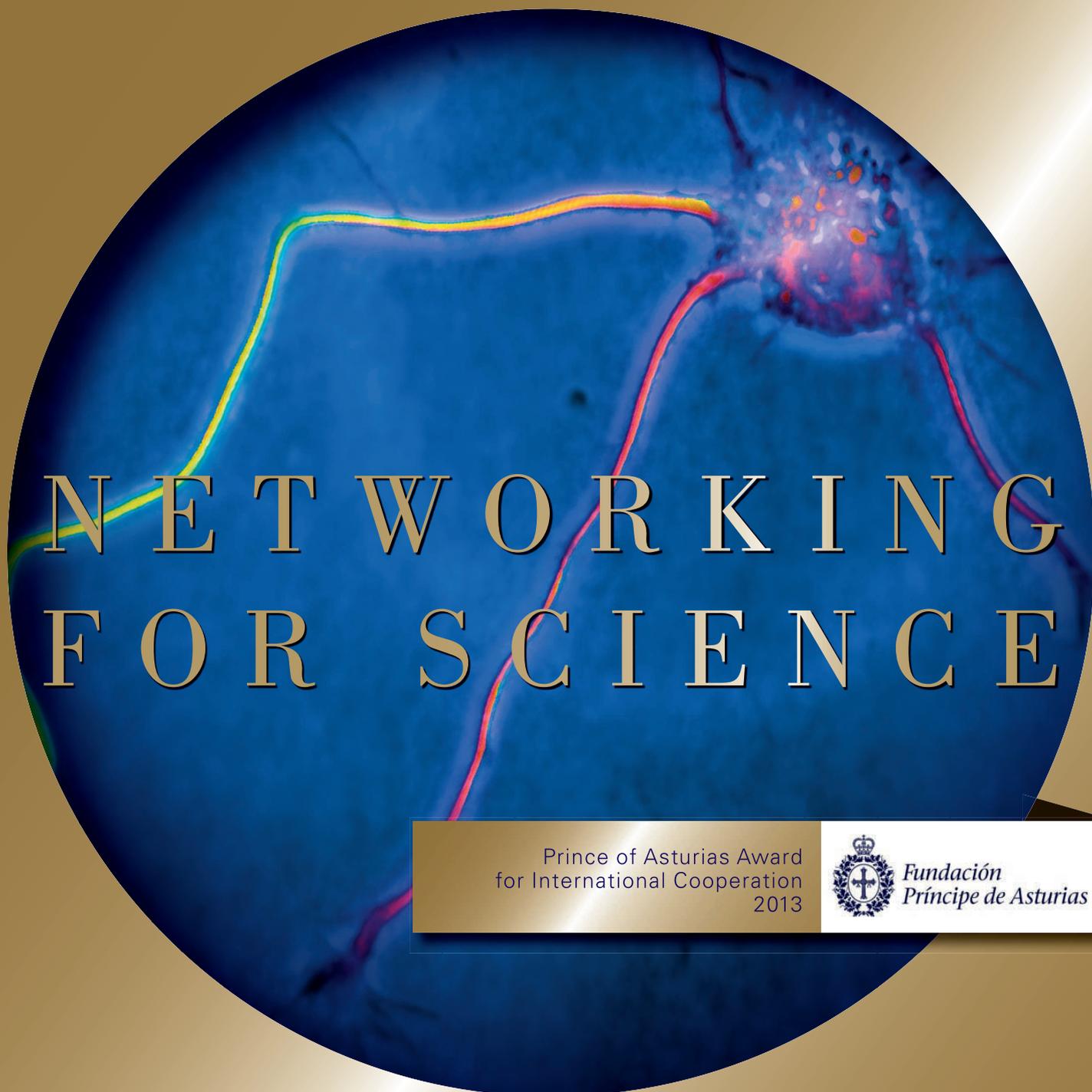
Word of Mouth Marketing: Verbreitung von Empfehlungen oder Informationen durch die Weitergabe in der persönlichen Kommunikation. Netzwerkstrukturen, in denen ähnlich wie im Liniennetz des internationalen Flugverkehrs einige *Hubs* die Aufgabe eines Verteilers übernehmen, begünstigen die schnelle Verbreitung von Werbebotschaften. Eine besondere Form des „WoMa“ sind Verfahren des *collective filtering*, wie sie etwa bei den persönlichen Buch- und Medienempfehlungen bei Amazon zum Einsatz kommen.

Theorie der sozialen Epidemie: Nach dem in neuerer Zeit vor allem durch den amerikanischen Wissenschaftspublizisten Michael Gladwell vertretenen Erklärungsmodell verbreiten sich Meinungen oder Werbebotschaften in ähnlicher Weise wie Krankheitserreger. Eine zentrale Rolle in diesem Modell spielt die *Influentials*-Theorie. Nach dieser Theorie werden Entwicklung und Ausmaß einer Epidemie vor allem durch die Existenz einer kleinen Gruppe von Menschen gesteuert, die über eine besonders hohe Anzahl sozialer Kontakte verfügen.



THE MAX PLANCK SOCIETY

www.mpg.de/en



NETWORKING
FOR SCIENCE

Prince of Asturias Award
for International Cooperation
2013



Fundación
Príncipe de Asturias

Der Daten-Schutzmantel

Daten sind der Rohstoff der Informationsgesellschaft. Oft genug aber geraten Unternehmen, die nicht auf umfassende Datenanalysen verzichten wollen, in Konflikt mit dem Datenschutz.

Paul Francis, Direktor am **Max-Planck-Institut für Softwaresysteme** in Kaiserslautern, sucht einen Ausgleich zwischen den gegenläufigen Interessen. Sein Unternehmen Aircloak spielt dabei eine wichtige Rolle.

TEXT **CHRISTIAN J. MEIER**

Der Blick hinter die Kulissen des Internets ist ernüchternd. Ein kostenloses Programm namens Ghostery zeigt an, wer mein Surfverhalten verfolgt. Paul Francis vom Max-Planck-Institut für Softwaresysteme in Kaiserslautern hat es mir empfohlen, als wir uns ein paar Tage zuvor in einem Café nahe dem Institut gegenüberßen.

Mit seinem verschlissenen Ampelmännchen-T-Shirt und einem karierten Hemd wirkt Francis wie ein legerer, etwas in die Jahre gekommener Computersonnyboy aus dem Silicon Valley. Es verwundert daher nicht, dass der Wissenschaftler nicht nur forscht, sondern gleichzeitig ein Start-up in Kaiserslautern betreibt. Sowohl seine Forschung als auch sein Unternehmen widmet er einem besseren Schutz der Privatsphäre von Internetnutzern.

Dabei betrachtet Paul Francis sein Start-up namens Aircloak als ein Forschungsinstrument. Den kommerziellen Erfolg der Firma sieht er als Gradmesser für die Fortschritte seiner Forschung. Was Francis mit seinem Start-up macht, ist eine Art Expedition in die reale Welt des Internets. Und die ist ein Dschungel, in dem Hunderte von Firmen eifrig Daten über Surfer sammeln. Diese Dienst-

leister haben sich darauf spezialisiert, die Onlinewege der Internetnutzer zu verfolgen. Die Daten verkaufen sie an Unternehmen, die damit etwa ihre Werbung optimieren können.

Davon bekomme ich, wieder zu Hause am Schreibtisch, schnell einen Eindruck: Sechs „Tracker“ zeigt Ghostery nach dem Klicken auf einen Onlineartikel eines Nachrichtenmagazins. Nach den Besuchen von ein paar weiteren Seiten, etwa einer Suchmaschine für Flüge oder von Facebook, habe ich schon etwa zwanzig verschiedene solcher Tracker identifiziert.

DAS FALSCHES VERSPRECHEN DER NUTZER-ANONYMITÄT

Die Tracker liefern den Datensammlern die Information, wer welche Seite besucht. Zwar bleibt der Nutzer dabei eine Nummer, aber immer die gleiche Nummer: Es lässt sich verfolgen, welche Websites der Nutzer mit der Nummer X besucht. „Die Firmen legen bei jedem Besuch einen Datensatz an“, erklärt Francis. Anhand der so entstehenden Datenbank lässt sich das Surfverhalten von Nutzer X untersuchen. Das ist für gezielte Werbung nutzbar, die X bestmöglich bei seinen Vorlieben packt.

„Es ist unglaublich“, sagt der aus den USA stammende Informatiker und schüttelt den Kopf, bevor er erklärt, wie die gezielte Werbung funktioniert. „Nehmen wir an, Sie kommen auf eine Website, die Platz für eine Anzeige hat, und mehrere Firmen wollen Ihnen ihre Werbung zeigen“, sagt er. „All diese Firmen machen dann bei Google ein Angebot. Der Meistbietende kommt zum Zug.“

Wo ist das Problem?, möchte man einwenden. Die Daten sind ja anonymisiert. Niemand weiß, dass es, sagen wir, Paul Francis oder Christian J. Meier sind, die diese oder jene Websites gern besuchen. Es sind Hausnummer eins oder Hausnummer zwei. Die Privatsphäre bleibt gewahrt.

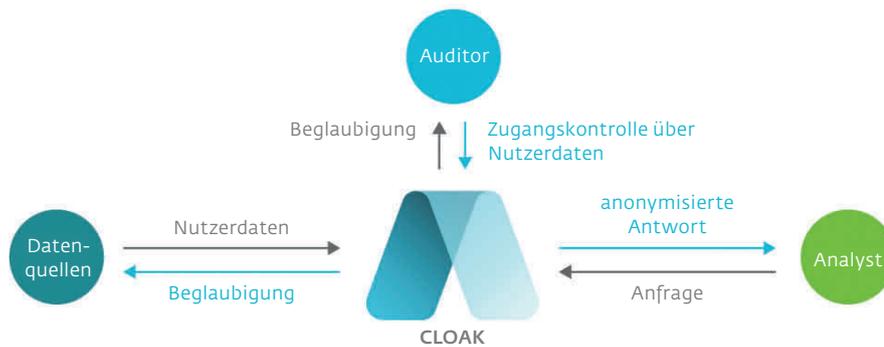
Doch so einfach sieht Francis die Sache nicht. Er spricht von einem falschen Versprechen der Nutzeranonymisierung, das da lautet: Wenn Daten erst einmal anonymisiert sind, kann niemand etwas über ein bestimmtes Individuum herausfinden. >

Lückenhafter Persönlichkeitsschutz: Durch die geschickte Kombination von Daten aus verschiedenen Quellen kann sich wie in unserem fiktiven Beispiel ein umfassendes individuelles Profil ergeben. Forscher des Max-Planck-Instituts für Softwaresysteme wollen das verhindern.



▷
NAME: MAX MUSTERMANN
ALTER: 58 JAHRE
WOHNORT: OBERPFAFFENHOFEN

▷
BERUF:
ENTWICKLUNGSCHEF EINES
MITTELSTÄNDISCHEN UNTERNEHMENS
▷
JAHRESGEHALT: 110000 EURO
▷
FAMILIENSTAND:
VERHEIRATET, DREI KINDER
▷
HOBBYS:
GLEITSCHIRMFLIEGEN, BIERDECKEL-SAMMELN
▷
HÄUFIGSTE SUCHANFRAGEN IM INTERNET:
GLEITSCHIRMFLIEGEN STARTRAMPE, MIGRÄNE,
SEXTIPPS, BIERDECKELBÖRSE, BRAUEREI,
DESSOUS, KRAMPFADERN
▷
KRANKHEITEN:
MIGRÄNE, KRAMPFADERN



Der Weg in die Anonymität: Die Cloak garantiert, dass Analysten aus Datensätzen keine Individuen herausfiltern können. Hinter der Cloak, einem undurchdringlichen Schutzmantel für Informationen, werden Nutzerdaten aus einer oder mehreren Quellen verwaltet. Ehe sie dorthinfließen, erhält die Datenquelle eine Beglaubigung, dass die Informationen tatsächlich in die Cloak fließen und nicht zu einem Ort, der lediglich vorgibt, eine solche zu sein. Der Analyst erhält auf seine Anfragen anonymisierte Antworten, die hinter der Cloak ermittelt werden. Dabei wehrt das Unternehmen Aircloak, das die Cloak betreibt, auf Individuen zielende Anfragen ab. Ausschließlich seine Auditoren kontrollieren den Zugang zu den Daten.

Die Brisanz steigt außerdem dadurch, dass es neben den Firmen, die das Surfverhalten einer Person X kennen, andere Unternehmen gibt, die weitere Informationen über die Person besitzen: Die Bank kennt ihre finanzielle Situation, der Energieversorger ihren Energieverbrauch, die Kreditkartenfirma erfährt einiges über das Konsumverhalten von X. Der Mobilfunkanbieter weiß, wann sich X wo aufgehalten hat. „Oft verkaufen die Firmen Daten über ihre Kundschaft“, erklärt Francis. Er wisse von Fällen aus den USA, in denen Banken anonymisierte Kundendaten an andere Organisationen gaben. Prinzipiell ist es also möglich, dass ein Käufer all diese Daten in einen Topf wirft und so ein umfassendes Bild über X gewinnen kann. Der Verbraucher wird gläsern. „Die Daten werden zwar zu harmlosen Zwecken gesammelt, aber je nach Käufer kann die Sache schwerwiegend werden“, warnt Francis.

Ein Datenschutz-Guerillero ist der Informatiker trotz solcher Szenarien nicht. An sich verteidigt er die Analyse anonymisierter Nutzerdaten. Sie könne sehr nützlich sein, meint er und nennt ein Beispiel: „Im medizinischen Bereich verursacht Betrug Milliarden Schäden“, sagt Francis. In medizinischen Datenbanken könnte man Betrugsfällen auf die Spur kommen, zum Beispiel indem man die Verschreibungen untersucht. Gibt es Ärzte, die besonders viel verschreiben? Oder die Medikamente verschreiben, die sie nicht verschreiben sollten?

Doch Anonymisierung allein helfe nicht, die Privatheit des unbescholtenen Gros der Ärzte zu schützen. „Es ist

schwierig, alle medizinischen Daten in eine große Datenbank zu packen, ohne die Privatheit zu gefährden“, sagt Francis. Daher werde dieses Potenzial nicht genutzt.

Zwei spektakuläre Fälle aus der Vergangenheit zeigen, was Francis meint. Sie demonstrieren, dass mitunter sogar Institutionen, denen man fundiertes Know-how im Datenschutz zutraut, leicht zu überlisten sind.

KOMBINIERTEN DATEN IDENTIFIZIEREN INDIVIDUEN

Ende der 1990er-Jahre veröffentlichte eine staatliche Agentur im US-Staat Massachusetts, welche die Krankenversicherungen staatlicher Angestellter verwaltete, Daten über die Versicherten, damit Forscher diese nutzen konnten. Die Agentur glaubte die Privatheit der Staatsbediensteten zu schützen, indem sie den Namen, die Sozialversicherungsnummer und andere „ausdrückliche Bezeichner“ jeder Person aus den Daten entfernte. Auch der damalige Gouverneur von Massachusetts, William Weld, garantierte der Öffentlichkeit, dass die Privatheit der Versicherten damit geschützt sei.

Er hatte nicht mit der pfiffigen Informatikstudentin Latanya Sweeney gerechnet. Für zwanzig Dollar kaufte sie sich das Wählerverzeichnis der Stadt Cambridge bei Boston, wo Weld wohnte. Darin standen Namen, Adressen, Postleitzahl, Geburtsdatum und Geschlecht jedes Wählers. Mit Leichtigkeit konnte sie so den Gouverneur in den

von der Agentur herausgegebenen Versichertendaten finden: Nur sechs Einwohner von Cambridge in den vermeintlich anonymisierten Krankenversicherungsdaten teilten seinen Geburtstag, drei davon waren Männer, von denen nur einer seine Postleitzahl hatte – der Gouverneur selbst. Öffentlichkeitswirksam sandte Sweeney dem Gouverneur seine Akte, samt der darin enthaltenen Diagnosen und Verschreibungen.

Ein paar Jahre später, 2006, veröffentlichte der Onlinedienst AOL zwei Millionen Suchanfragen von 650 000 Nutzern. Forscher freuten sich über diese Möglichkeit, das Internetverhalten sehr vieler Nutzer anhand einer so riesigen Datenmenge untersuchen zu können. AOL anonymisierte die Daten: Das Unternehmen entfernte Nutzernamen, IP-Adressen, die den Computern zugeordnet sind, und andere Informationen, die eine direkte Identifizierung von Nutzern ermöglichten. Jeder Nutzer wurde allerdings mit einer eindeutigen Nummer versehen, damit die Daten für die Forschung wertvoll blieben.

Diesmal waren es zwei Journalisten der NEW YORK TIMES, die AOL zeigten, dass diese Anonymisierung keinen perfekten Schutz der Privatheit bot. In Anfragen des Nutzers 4417749 fanden sie Hinweise auf dessen Identität. Es gibt nämlich nicht viele Nutzer, die gleichzeitig einen Landschaftsgärtner in „Lilburn, GA“, und nach einem zum Verkauf stehenden Haus in „Shadow Lake, Georgia“, suchten. Die Journalisten identifizierten eine gewisse Thelma Arnold hinter den Anfragen. Arnold bestätigte, die Suchphrasen eingegeben zu haben, darunter auch Peinliches wie „Hund, der auf alles uriniert“.

Die Moral dieser Geschichten: Ein listiger, vielleicht sogar böswilliger Analyst kann verschiedene Informationen über Personen kombinieren. Indem er verschiedene Datensätze wie Filter nutzt, kann er wie bei der Rasterfahndung Individuen identifizieren und aussagekräftige Profile von ihnen anlegen.

Paul Francis verweist anhand der Beispiele auf einen Zielkonflikt beim Umgang mit den Daten: Für Analysten sind Daten umso interessanter, je mehr sie über das Individuum aussagen. Für Werbeleute zum Beispiel ist nicht nur

Vermittler im Datenkonflikt: Paul Francis (rechts) und Sebastian Probst Eide entwickeln Konzepte, um Unternehmen aussagekräftige statistische Informationen zu liefern und dabei persönliche Daten vor Missbrauch zu schützen.

das Geschlecht einer Person wichtig, sondern auch Fragen wie: Lebt sie in einem Double-income-no-kids-Haushalt? Gehört sie einer bestimmten Szene an? In welcher Wohngegend lebt sie?

Doch die Präzision kostet etwas: Das Risiko steigt, dass sich ein Leck in der Privatsphäre auftut. Um die Privatsphäre zu schützen, sollten Daten also möglichst wenig über eine Einzelperson verraten. „Je besser jedoch die Privatheit geschützt ist, desto weniger nützlich sind die Daten“, erklärt der Forscher.

Paul Francis möchte das gebrochene Versprechen der Nutzeranonymisierung wiederherstellen und den Unternehmen gleichzeitig aussagekräftige Daten zur Verfügung stellen. Doch er sagt auch: „Das Problem lässt sich nicht wirklich lösen, man kann es nur Schritt für Schritt entschärfen.“ Zwischen Analysten und Datenschützern finde ein ähnlicher Wettlauf statt wie zwischen Programmierern von Computerviren und Virenschützern. Letztere hängen immer einen Schritt hinterher. Wie Virenschützer müssen auch Datenschützer die konkreten Tricks der Gegenseite analysieren, um dafür konkrete Gegenmaßnahmen zu finden.

Um praxistaugliche Mittel zu entwickeln, die zwischen den gegenläufigen Interessen von Datenschutz und Datennutzung ausgleichen, verfolgt Paul Francis einen Ansatz, der sich von den Lösungsvorschlägen vieler Informatiker grundlegend unterscheidet.

Bisher behandelten Informatiker das Problem allein als ein informationstechnisches oder informationstheoretisches. „Auf diese Weise vernachlässigt man aber viele Aspekte des Problems, das neben technischen auch rechtliche, wirtschaftliche und psychologische Seiten hat“, kritisiert Francis. „Es wurden Hunderte von akademischen Publikationen geschrieben, aber kaum eine dieser Lösungen wird in der Praxis benutzt“, sagt er. Der Grund: Die Industrie akzeptiere keine Lösung, die eine Datenanalyse wesentlich teurer oder weniger präzise mache. >



Prüfstand für den Datenschutz: Felix Bauer präsentiert das Konzept von Aircloak auf der CeBIT in Hannover. Dass es für Unternehmen, die Informationen etwa über ihre Kunden nutzen wollen, attraktiv ist, haben die Max-Planck-Wissenschaftler zu einem ihrer Forschungsziele erklärt.

Auch Francis hat bis vor wenigen Jahren auf rein akademische Weise Techniken entwickelt, die Lecks in der Privatsphäre stopfen sollten. „Dann hatte ich das Gefühl, dass die Technik reif genug war, um ein Start-up zu gründen“, sagt er. Das Unternehmen sollte den Praxistest für die Forschungserkenntnisse bringen. Inzwischen gibt es Aircloak seit eineinhalb Jahren. Neben Francis besteht das Team aus fünf jungen Computerspezialisten, die alle praktische Erfahrung mitbringen, etwa aus dem Team von Google+ oder aus dem Kampf gegen Malware und Hacker.

Aircloak will eine Privatsphäre ohne Leck schaffen und dabei alle Aspekte des Datenschutzes berücksichtigen, neben den technischen also auch die juristischen, ökonomischen und psychologischen.

Francis spricht daher mit Datenschutzexperten ebenso wie mit Unternehmen. Erfahrungen darüber, wie Firmen ticken, hat er als Forschungsleiter bei zwei Start-ups im Silicon Valley gesammelt. So kann der Forscher etwa die Sorgen einer Firma verstehen, die Finanzsoftware für die PCs und Mobilgeräte von Verbrauchern herstellt und wissen möchte, warum die Software auf Mobilgeräten wenig genutzt wird. Dazu würde sie gern Nutzerdaten sammeln und auswerten. Doch wegen der sensiblen Natur der Daten – sie beinhalten den Aufenthaltsort, die Finanzen und die Einkäufe eines Nutzers – macht sich die Firma Sorgen um technische und rechtliche Probleme sowie um die mögliche Wirkung des Vorhabens auf die Öffentlichkeit. Daher lässt sie diese Form der Marktforschung lieber bleiben.

Diese Sorgen will Aircloak seinen Kunden durch das Cloaked Computing nehmen. Die Erfindung des Unternehmens erklärt Felix Bauer, Forscher des Max-Planck-Instituts für Softwaresysteme und Mitgründer von Aircloak: „Die Daten werden noch auf dem Computer



oder dem Mobilgerät des Nutzers verschlüsselt“, sagt der Physiker. „Dann werden sie in unser zentrales System geschickt.“ Dieses System, eine sogenannte Cloak, was zu Deutsch Umhang oder Deckmantel heißt, ist nach außen hin abgesichert, sodass niemand darauf zugreifen kann. „Nur innerhalb dieses Systems können die Daten entschlüsselt und analysiert werden“, erklärt Bauer.

Die Cloak ist mehr als eine Firewall, mit der sich etwa Unternehmen gegen Onlineattacken von außen schützen. „Es ist eine Art Blackbox“, erklärt Francis. Es gebe keine Nutzernamen und Passwörter, keinen Weg, von außen einzudringen. Ein Chip garantiere diese Sicherheit ähnlich wie ein Trusted Platform Modul, das an einen bestimmten PC gebunden ist und diesen umfassend gegen äußere Angriffe schützt. Manipulationen sind praktisch unmöglich: „Jede Änderung der Software, die wir vornehmen, muss von einer dritten Partei genehmigt werden.“

Wenn ein Unternehmen etwas über seine Nutzer wissen möchte, dann stellt es eine Anfrage an die Cloak, zum Beispiel: Wie viele meiner Nutzer sind weiblich? Die Cloak verarbeitet die Daten entsprechend und schickt die anonymisierten Daten zurück.

Cloaked Computing unterscheidet sich vom derzeit üblichen Umgang mit Daten, erklärt Francis. Bislang werden die Daten meist schon in anonymisierter Form in die Datenbank der Unternehmen gelegt, die das Surfverhalten analysieren oder sonstige Daten sammeln. Bei Aircloak hingegen gelangen die verschlüsselten, aber noch nicht anonymisierten Informationen in die Datenbank. So verlieren sie nicht an Qualität für den

Kunden. Wegen der Cloak sind sie dennoch sicher. Die Anfrage des Kunden wird mithilfe der Rohdaten beantwortet, enthält also das Maximum an Information. Erst die Antwort wird anonymisiert und an den Kunden weitergegeben.

Wenn die Datenbank nicht von den Unternehmen betrieben wird, die an den Daten interessiert sind, und wenn sie gleichzeitig durch eine Cloak geschützt ist, könne weniger private Information in unbefugte Hände gelangen als aus Datenbanken der einschlägigen Unternehmen, in denen die Information bereits anonymisiert liegt. Allerdings garantiert auch das Cloaked Computing keine absolute Sicherheit. Denn listige Analysten können durch die geschickte Kombination von Anfragen Informationen über Einzelpersonen herausfinden.

ZUFÄLLIGE SCHWANKUNGEN IN DEN ANTWORTEN

Um das zu verhindern, beobachtet Aircloak die Anfragen von Analysten und sucht nach Hinweisen auf einen solchen Angriff. Angenommen, eine Datenbank enthält Angaben zum Einkommen von Personen, gibt auf Anfragen aber nur das gesamte Einkommen einer ganzen Gruppe von Nutzern oder andere statistische Antworten zur Gehaltsverteilung heraus.

Ein seriöser Analyst stellt vielleicht folgende Anfrage: Gib mir die Altersverteilung der Nutzer, die ein bestimmtes Einkommen haben. Das Ergebnis wäre ein Diagramm, das jeweils die Anzahl der Nutzer mit einem Monatseinkommen von, sagen wir, über 4000 Euro in den Altersgruppen von 20 bis 30, 30 bis 40 und so fort angibt.

Ein unseriöser Analyst will aber das Gehalt einer Person X herausfinden. Vorausgesetzt, der Angreifer kann die Person X anhand von Postleitzahl, Geburtsdatum und Geschlecht identifizieren, so könnte er zuerst nach dem Gesamteinkommen aller Personen mit der gleichen Postleitzahl fragen. Er stellt dann eine zweite Anfrage: Gib mir das Gesamteinkommen aller Personen mit dieser Postleitzahl außer X. Um das Gehalt von X zu ermitteln, muss er dann nur noch beide Antworten voneinander subtrahieren.

Um solch einen Bruch des Datenschutzes zu verhindern, fügen Aircloak und andere einschlägige Unternehmen, die derlei Analysen betreiben, den Antworten eine leichte zufällige Schwankung hinzu. Dann weicht die Differenz der beiden Gesamteinkommen deutlich von der tatsächlichen Differenz ab. Der Angreifer erhält keine wertvolle Information.

Für einen seriösen Analysten, der nach der Altersverteilung in einer Gehaltsklasse fragt, bliebe die Antwort dagegen wertvoll, obwohl die Antwort auf seine Frage leicht von den tatsächlichen Zahlen abweicht. Wenn es statt 203 Personen in einer Altersgruppe 206 oder 202 sind, kann er immer noch erkennen, welche Altersgruppe in einer Gehaltsklasse wie vertreten ist.

Ein Angreifer könnte seine Anfrage durch zusätzliche Kriterien auch auf bestimmte Individuen eingrenzen. Um derlei Trickserei zu erschweren, hat Francis' Team ein einfaches Mittel ersonnen. „Es gibt eine untere Schwelle“, erklärt der Informatiker. Die Antwort wird mit der zufälligen Schwankung versehen, und wenn das Ergebnis unterhalb dieser Schwelle liegt, gibt das System keine Antwort, es sagt zum Beispiel: Sorry, der Wert ist zu klein. Das System verwehrt dem Anfragenden somit die Methode der Rasterfahndung, bei der ein Datensatz nach dem Ausschlussverfahren immer weiter eingegrenzt wird.

„Sie mögen einwenden, dass die Idee, eine untere Schwelle für herausgegebene Antworten einzuführen, nicht sonderlich originell ist“, gibt der Forscher zu. „Das stimmt. Aber niemand hat diese

Idee zuvor analysiert. Sogar diese simple Idee ist zu schwierig, um sie theoretisch zu analysieren. Natürlich löst unser Ansatz das Problem nicht perfekt. Aber es ist etwas, was man tun kann.“

DIE SYSTEMFORSCHUNG ÄHNELT EINER ENTDECKUNGSFAHRT

Allerdings werden Hacker jedem Stein, den man ihnen in den Weg wirft, auszuweichen suchen und neue Angriffsmöglichkeiten aushecken. „Um den Einfluss der künstlich hinzugefügten zufälligen Schwankungen zu eliminieren, könnte der Analyst etwa die gleiche Anfrage immer und immer wieder stellen. Der Mittelwert der Zahlen, die er dabei herausbekommt, wird nahe am wahren Wert liegen“, sagt Francis. Freilich könne man verhindern, dass dieselbe Anfrage mehrmals gestellt werde.

Doch die Anfragen lassen sich auch unterschiedlich formulieren. Statt der Postleitzahl kann der Analyst beispielsweise die geografischen Koordinaten Länge und Breite verwenden. Das wäre die gleiche Anfrage. Auch zur Abwehr

solcher Versuche haben die Forscher kürzlich eine Methode entwickelt, die aus patentrechtlichen Gründen jedoch noch nicht publik werden soll.

Bei aller Praxisnähe stellt die Forschung von Francis' Team Grundlagenforschung der Informatik dar. „Das sehr komplexe System, mit dem wir es zu tun haben, erfordert einen hohen Aufwand an ingenieurwissenschaftlichem Know-how und informeller Analyse.“ Informatiker sprechen hierbei von Systemforschung. „Wir beziehen ja auch noch Wirtschaft, Politik und Soziologie in unser Denken ein, sodass das System sogar noch komplexer wird als bisher“, sagt Francis.

Ein wesentlicher Teil der Systemforschung ähnelt einer abenteuerlichen Entdeckungsfahrt. Das Team von Paul Francis gleicht der Crew eines Schiffes, das durch ein Seegebiet voller Riffe schippert. Kaum hat es am Bug ein Leck geflickt, kracht es am Heck, und sie müssen dort ein neues Loch stopfen. Doch der Kaiserslauterer hat sichtlich Spaß an diesem Wettstreit. Er wird es den Angreifern alles andere als leicht machen. ◀

AUF DEN PUNKT GEBRACHT

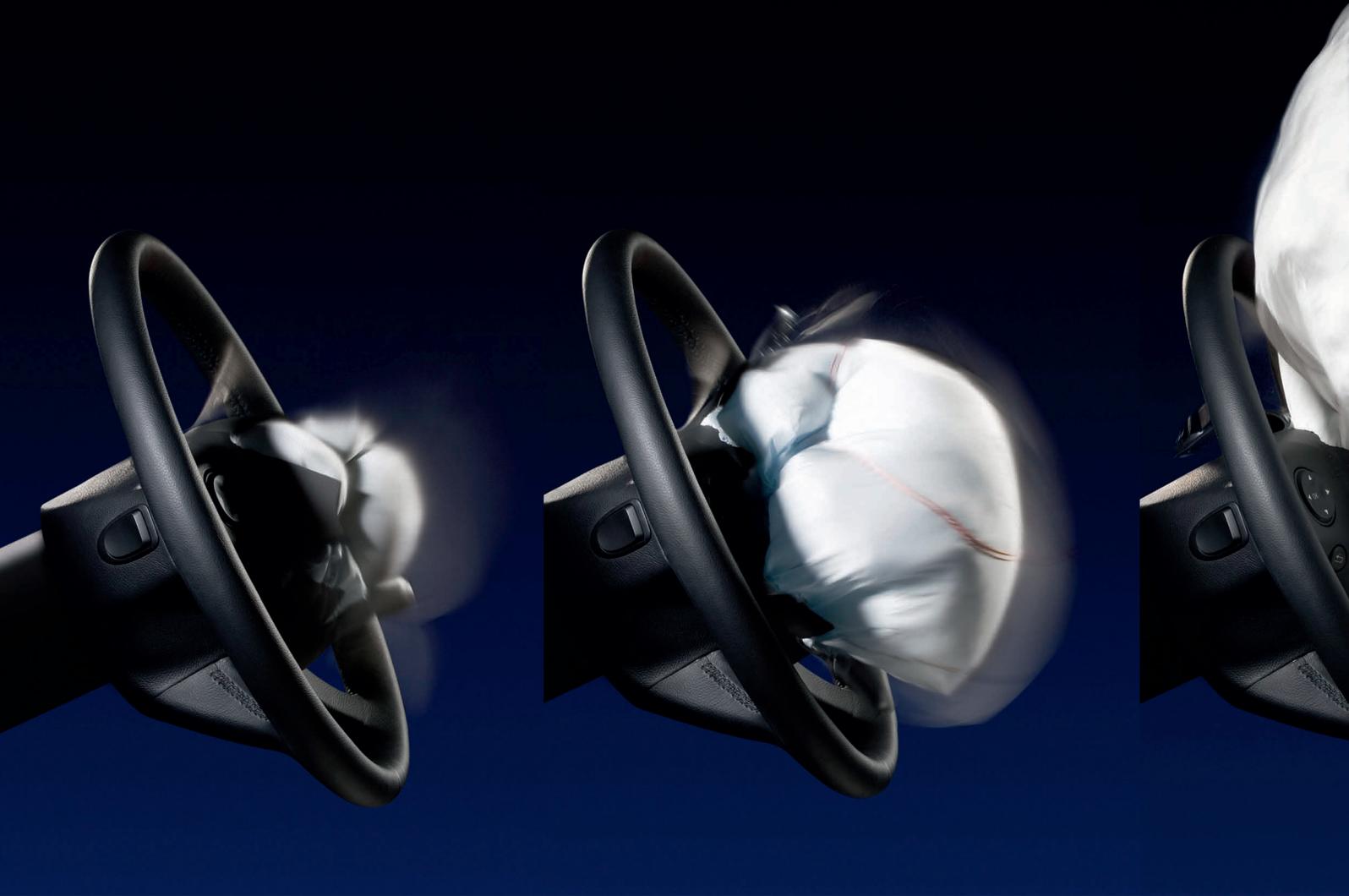
- **Spezialisierte Unternehmen analysieren das Surfverhalten von Internetnutzern. Andere Firmen verfügen über vielfältige weitere Daten von Personen. Wer die Daten zusammenführt, erhält oft umfassende Profile mit teilweise sehr privaten Details von Einzelpersonen.**
- **Analysten, die möglichst viel Information aus Daten gewinnen wollen, und Datenschützer befinden sich in einem ständigen Wettlauf.**
- **Das Start-up-Unternehmen Aircloak will, basierend auf Erkenntnissen von Max-Planck-Forschern, eine Privatsphäre ohne Leck schaffen und berücksichtigt dabei die technischen, juristischen, ökonomischen und psychologischen Aspekte des Datenschutzes.**

GLOSSAR

Cloak: Dieser Schutzmantel sichert nicht-anonymisierte Daten hermetisch vor unerlaubten Zugriffen von außen.

Cloaked Computing: Hinter der Cloak werden Daten in nicht-anonymisierter Form analysiert, um statistische Fragen mit größtmöglichem Informationsgehalt zu beantworten. Das Ergebnis wird anonymisiert und an den Fragenden geschickt.

Tracker: Mit dieser Software verfolgen einschlägige Unternehmen das Surfverhalten von Internetnutzern. Ein Tracker registriert, welche Webseiten von einem bestimmten Computer besucht werden.



Mit Sicherheit pünktlich

Wenn ein Computer eine Webseite extrem langsam aufbaut, ist das vielleicht ärgerlich, aber nicht mehr. Wenn jedoch die Elektronik im Auto oder in Flugzeugen nicht absolut pünktlich Befehle verarbeitet, dann kann das lebensgefährlich werden. Unter welchen Bedingungen die dort gefragten Echtzeitsysteme zuverlässig funktionieren, untersuchen **Björn Brandenburg** und sein Team am **Max-Planck-Institut für Softwaresysteme** in Kaiserslautern und Saarbrücken.

TEXT **ALEXANDER STIRN**



Pünktlichkeit ist unterbewertet – zumindest in der Informatik. Wenn der Airbag im Auto ein paar Millisekunden zu spät auslöst, weil sein Steuergerät herumtrödelt, wird es gefährlich. Wenn das Handy den winzigen Augenblick verschläft, für den es von seiner Funkzelle die Erlaubnis zur Kommunikation erhalten hat, dann bleiben die Daten stecken. Wenn ein Pilot ein Flugzeug landen will, seine Kommandos aber nicht rechtzeitig bei den Turbinen oder Landeklappen ankommen, kann das fatale Folgen haben.

„Die physikalische Welt hört nicht auf, bloß weil der Rechner nicht hinterherkommt“, erklärt Björn Brandenburg, Nachwuchsgruppenleiter am Max-Planck-Institut für Softwaresysteme in Kaiserslautern und Saarbrücken. Dort kümmert sich der Informatiker um sogenannte Echtzeitsysteme – Anwendun-

Wenn Bruchteile von Sekunden überlebenswichtig sind: Ehe der Kopf des Fahrers auf das Lenkrad aufprallt, muss der Airbag aufgeblasen sein. Seine Steuerung muss ihn daher absolut pünktlich auslösen.

gen, bei denen ein Computer unter keinen Umständen zu spät dran sein darf.

Die theoretische und praktische Umsetzung solcher Systeme stellt die Informatik vor große Herausforderungen: Normalerweise arbeitet ein Programm korrekt, sobald bestimmte Eingaben zu den logisch korrekten Ergebnissen führen. „Bei uns dagegen ist ein System nur dann korrekt, wenn es die richtigen Ausgaben auch zum richtigen Zeitpunkt macht“, sagt Brandenburg.

Als Leiter der Forschungsgruppe für Echtzeitsysteme untersucht der 30-Jährige daher, wie in einer zunehmend komplexen und miteinander vernetzten Umgebung garantiert werden kann, dass solche Systeme sicher und zuverlässig arbeiten. Während in der technischen Praxis Experimente und Intuitionen immer noch eine wichtige Rolle spielen, setzt

Brandenburg auf harte Mathematik: „Für sicherheitskritische Anwendungen brauchen wir Analysemethoden, die mathematisch wohlfundiert sind und korrekt beweisen, dass ein System stets wie gewünscht funktioniert“, sagt der Max-Planck-Forscher.

Die Anforderungen an Echtzeitsysteme unterscheiden sich damit grundlegend vom Informatikalltag: Ob sich das Programmfenster mit der gerade gelesenen E-Mail sofort nach dem Mausklick oder erst mit etwas Verzögerung schließt – dafür braucht es keine mathematischen Modelle. Selbst wenn manchmal gar nichts passiert, flucht der Anwender vielleicht, aber die Welt geht nicht unter. Sollen derartige Systeme verbessert werden, vertrauen Entwickler folglich auf ihre Erfahrung, auf ihre Ideen. Sie schauen sich den Programmcode an



Anwälte der Pünktlichkeit: Björn Brandenburg (rechts) und Alexander Wieder entwickeln Methoden, um zu beweisen, dass sicherheitsrelevante Systeme den Job, der von ihnen erwartet wird, pünktlich erledigen – immer.

und testen die Neuerungen in groß angelegten Studien. „Wenn das im Schnitt gut funktioniert, ist das für allgemeine Systeme völlig okay“, sagt Brandenburg.

Bei sicherheitskritischen Echtzeitsystemen wie dem Airbag im Auto helfen Durchschnittswerte nicht weiter. Das Produkt muss funktionieren. Punkt. „Im Ganzen sind die Systeme inzwischen allerdings so komplex geworden, dass es in der Praxis nicht mehr reicht, mit dem menschlichen Auge scharf hinzuschauen“, sagt Brandenburg.

MEHR ALS 100 MIKROCOMPUTER IN EINEM LUXUSAUTO

So sind allein in einem modernen Luxusauto mehr als hundert Mikrocomputer verbaut, die sämtliche Systeme vom Airbag über die Motorsteuerung bis hin zum Radio kontrollieren. Die meisten bearbeiten dabei mehrere Aufgaben – das macht die mathematische Beschreibung so kompliziert: „Wenn ich ausschließen will, dass etwas schiefgehen kann, wird das umso schwieriger, je mehr Dinge miteinander interagieren“, sagt Björn Brandenburg.

Der Informatiker vergleicht die Situation gern mit einem Büro: Der dortige Mitarbeiter, der in diesem Bild einen Prozessor darstellt, steht unter Druck. Immer wieder will der Chef etwas von ihm; dessen Aufgaben müssen sofort abgearbeitet werden. Aber auch die Kollegen haben Fragen und wollen mit ihren Anliegen nicht den ganzen Tag warten.

Das Büro funktioniert nur, wenn alle Aufgaben in der gewünschten Zeit gelöst

werden und wenn der arme Angestellte bei Feierabend keinen Berg an Arbeit vor sich herschiebt. Vor allem aber dürfen die einzelnen Wünsche, insbesondere die des Chefs, nicht so lange liegen bleiben, dass schon wieder die nächste Anfrage mit gleicher Priorität eintrudelt. Denn sonst endet all das im Chaos. Die Informatiker sprechen von einem nicht-linearen Verhalten, das urplötzlich zu Sprüngen bei der Reaktionszeit führt.

„Um solche Vorgänge mathematisch beschreiben zu können, brauchen wir Modelle, die die Welt gut abbilden, mit deren Hilfe wir aber gleichzeitig auch beweisen können, dass die Systeme die in sie gesetzten Anforderungen erfüllen“, sagt Brandenburg. Deshalb packen im Fall des Büros – oder eines einfachen Echtzeitsystems – die Informatiker die Häufigkeit der einzelnen Aufgaben, den Arbeitsaufwand für ihre Bearbeitung und die gewünschte Zeit, in der eine Antwort verlangt wird, in mathematische Gleichungen. Oft fällt das Formelsystem dabei so kompliziert aus, dass es sich analytisch nicht mehr lösen lässt. Dann müssen Informatiker durch Annahme eines Startwerts und durch konsequentes Verfeinern Schritt für Schritt eine Lösung suchen – ein Standardverfahren, das Mathematiker Fixpunktiteration nennen.

Ein weiteres Problem besteht darin, realistische Minimal- und Maximalwerte für den Arbeitsaufwand, die Häufigkeit und die erlaubte Antwortzeit zu finden. Nur mit solchen Angaben lassen sich die Formeln auf Herz und Nieren prüfen. „In der Praxis übernimmt

das häufig ein Ingenieur mit viel Erfahrung, der ein bisschen testet und dann noch eine Sicherheitsmarge draufschlägt“, sagt Brandenburg. „In vielen Fällen kann das sogar eine hinreichend gute Abschätzung sein.“

PROZESSOREN SIND HEUTE UNBERECHENBARER ALS FRÜHER

Beim Airbag ergibt sich die maximal erlaubte Dauer der Berechnung zum Beispiel aus der Zeit, die zwischen dem Crash und dem Aufprall des Fahrerkopfs auf das Lenkrad vergehen würde. Bis dahin muss der Airbag komplett aufgeblasen sein – und daraus lässt sich zurückrechnen, wie schnell die Software reagieren muss. „Letztlich leitet sich die Deadline immer aus den physikalischen Anforderungen des Systems ab“, sagt Brandenburg.

Der Motor macht da keine Ausnahme. Bei ihm diktiert die erlaubte Drehzahl die minimale Zeit zwischen zwei Vorgängen. Muss beispielsweise einmal pro Umdrehung die Abgaskonzentration ausgelesen werden, ergibt sich bei einer Maximaldrehzahl von 6000 Umdrehungen pro Minute (oder 100 Umdrehungen pro Sekunde) eine kleinstmögliche Pause von einer Hundertstelsekunde.

Deutlich komplizierter ist es, die tatsächliche Rechenzeit eines modernen Systems zu ermitteln und so abzuschätzen, ob die Arbeit auch im vorgegebenen Rahmen erledigt werden kann. Bei früheren Prozessorgenerationen war das noch vergleichsweise einfach möglich. Damals konnten Ingenieure im

maximale Verzögerung durch Blockierung benötigter Betriebsmittel

$$b_i \triangleq \sum_{T_x \in \tau^i} \sum_{\ell_q \in Q} \sum_{v=1}^{N_{x,q}^i} (X_{x,q,v}^S + X_{x,q,v}^A) \cdot L_{x,q}$$

alle Quellen von Aufgaben

alle Ressourcen

alle kritischen Anfragen

Teil der Anfrage, der zur Verzögerung führt

Länge der Anfrage

Eine Formel für Verzug: Die Max-Planck-Forscher untersuchen Echtzeitsysteme, deren Prozessoren sich andere Ressourcen teilen. Die Systeme erledigen eine sicherheitsrelevante Aufgabe möglicherweise zu spät, weil sie auf eine Ressource nicht zugreifen können. Die maximale Verzögerung ergibt sich aus der Summe Σ aller Teile von Anfragen, die zu Verzögerungen führen, und der jeweiligen Länge dieser Anfragen. Die Anfragenteile können zu verschiedenen Aufgaben gehören, die aus verschiedenen Quellen stammen, und auf mehrere Ressourcen angewiesen sein. Um die Verzögerung berechnen zu können, ist die Bestimmung der Anfragenteile $X_{x,q,v}^S$ und $X_{x,q,v}^A$, die zur Verzögerung führen, entscheidend. Dafür nutzen Björn Brandenburg und seine Kollegen erstmals ein Verfahren namens lineare Optimierung.

Maschinencode abzählen, wie viele Rechenschritte nötig sind, um eine Aufgabe abzuarbeiten. Da der Arbeitstakt des Prozessors bekannt war, ließ sich daraus die benötigte Zeit ermitteln.

Heutige Prozessoren sind viel unberechenbarer: Sie versuchen zu erraten, welche Aufgabe als nächste ansteht, und bereiten sich darauf vor. Sie können ihre Taktfrequenz regulieren. Sie greifen auf eine Vielzahl von Zwischenspeichern zurück. Inzwischen kümmert sich ein eigenes Forschungsfeld der Informatik, die *Worst-Case Execution Time Analysis*, um nichts anderes, als bei einem vorgegebenen Programm und einer vorgegebenen Hardware die maximale Rechenzeit im schlimmsten aller Fälle zu bestimmen.

„Es ist unheimlich schwer, so etwas exakt zu machen“, sagt Brandenburg. „Deshalb kann es sinnvoll sein, echte Systeme zu beobachten und Messwerte zu extrahieren.“ Eine Software protokolliert dabei zum Beispiel alle Kommandos, die während einer Testfahrt im Auto abgearbeitet werden. Ingenieure können daraus Daten wie die maximale Ausführungszeit ableiten. Danach wird noch ein kleiner Sicherheitspuffer eingebaut, fertig sind die Ausgangswerte für die computergesteuerte Analyse der Programme. „Die Puristen in unserem Feld würden sagen: Da ist ja eine Messung drin. Damit kann man doch nicht streng mathematisch beweisen, dass das wirklich der schlimmste anzunehmende Fall ist“, sagt Brandenburg. „Ich bin da pragmatischer. Eine Analyse der Antwortzeiten ist auf

jeden Fall besser als irgendeine Tabellenkalkulation, in die ein paar mehr oder weniger willkürliche Zahlen eingetippt worden sind.“

Erst nachdem alle Randbedingungen ermittelt werden konnten, kommt die Mathematik zum Zug. „Wenn wir dann zeigen können, dass die Antwortzeit selbst in den allerschlimmsten Fällen niemals größer als die gewünschte Deadline ausfällt, wissen wir: Das passt so, das System ist sicher“, sagt Alexander Wieder, Doktorand in Brandenburgs Forschungsgruppe.

INGENIEURE DEFINIEREN DIE ANFORDERUNGEN

So etwas beweisen Mathematiker meist durch ein Verfahren, das sie „Widerspruchsbeweis“ oder auch „indirekten Beweis“ nennen. Die Forscher nehmen dabei an, dass die vorgegebene Ausführungszeit überschritten wurde – dass also genau der Fall eingetreten ist, den sie eigentlich ausschließen möchten. Dann schauen sie, welche Schlussfolgerungen sich daraus ableiten lassen: Wurde die Aufgabe nicht wie geplant erfüllt, gibt es zwei Möglichkeiten: Entweder die Bearbeitung einer Aufgabe hat länger gedauert als angenommen, oder der Prozessor muss noch etwas anderes gemacht haben, während er den sicherheitsrelevanten Job erledigen sollte – er war also offenbar mit Anfragen ausgelastet, die er der wichtigsten Aufgabe vorgezogen hatte.

Im nächsten Schritt schauen sich die Informatiker alle Prozesse genauer an,

analysieren, wie viel Arbeit diese verursachen. Das Verfahren wird Schritt für Schritt verfeinert, bis am Ende ein paar Prozesse übrig bleiben, die unter den gegebenen Annahmen mehr Arbeit verursachen müssen, als sie laut Modell eigentlich dürften. Ein Widerspruch. „Für uns bedeutet das: Entweder ist unser Modell falsch, oder so etwas ist unmöglich“, sagt Brandenburg. Die vorgegebene Ausführungszeit würde somit niemals überschritten. Das System ist hundertprozentig sicher – zumindest unter den gegebenen Modellannahmen.

Die Modelle beruhen auf Anforderungen, die Ingenieure definieren. Jenseits dieser Spezifikationen, wenn der Motor zum Beispiel mit mehr als 6000 Umdrehungen pro Minute läuft, gibt es keine mathematische Sicherheit mehr. Die Software kann noch funktionieren, sie muss aber nicht. Die Ingenieure müssen daher ihr Fachwissen einbringen, um sichere und vollständige Anforderungen an das System zu stellen.

Häufig simuliert wird dagegen eine Art sprunghafter Chef, der viele Aufgaben innerhalb kurzer Zeit verteilt und sich dann erst einmal in sein Büro zurückzieht. *Busty arrivals*, „stoßweise Eingänge“, nennen Informatiker das Phänomen. Es lässt sich recht gut in Algorithmen packen, auch wenn der Aufwand für die Beweisführung dadurch etwas steigt.

Wirklich kompliziert werden Echtzeitanwendungen allerdings, sobald sie auf einem Prozessor bearbeitet werden, der sich mit weiteren Prozessoren andere Ressourcen teilen muss. So können die



links: Dolmetscher zwischen zwei Fachsprachen: Björn Brandenburg versteht sowohl die Ingenieure, die Echtzeitsysteme entwickeln, als auch die Theoretiker, die deren Zuverlässigkeit beweisen wollen. Daher möchte er zwischen beiden Disziplinen vermitteln.

rechte Seite: Damit ein Flugzeug sicher landet, muss die Elektronik die Steuerbefehle des Piloten unbedingt in der vorgegebenen Zeit an die Turbinen oder Landeklappen weitergeben.

Schalteinheiten etwa gemeinsam auf einen Nachrichtenpuffer zugreifen, der Sensordaten speichert, solange sie nicht weiterverarbeitet werden können. Systeme mit geteilten Ressourcen bilden einen Schwerpunkt der Forschung am Max-Planck-Institut für Softwaresysteme.

Im Bild des Büros, in dem ein Mitarbeiter für einen Prozessor steht, hieße das: Den Bürokräften, die normalerweise ungestört nebeneinanderher arbeiten, steht zum Beispiel nur ein Kopierer oder ein Telefon zur Verfügung. Da kommt es unweigerlich zu Diskussionen. Einige Mitarbeiter müssen mit einer Aufgabe dringend fertig werden, andere hätten eigentlich mehr Zeit, wollen aber trotzdem nicht warten. „Je nachdem, in welcher Reihenfolge man die Leute ranlässt, kann das entscheiden, ob alle Deadlines eingehalten werden“, sagt Björn Brandenburg.

In der Praxis verfolgen Informatiker unterschiedliche Ansätze: Die Prozessoren können fein säuberlich in eine Warteschlange eingereiht werden, es lassen sich Prioritäten verteilen, das Los kann entscheiden, oder es kann eine bunte Mischung aus sämtlichen Möglichkeiten zum Einsatz kommen. Auch bei der Frage, wie sich die einzelnen Prozessoren die Wartezeit vertreiben sollten, führen mehrere Wege zum Ziel: Sie können pausenlos fragen: „Kann ich? Kann ich? Kann ich?“, bis sie endlich an der Reihe sind. Oder sie können darauf warten, an den Kopierer gebeten zu werden.

Theoretisch ist das Warten die bessere Lösung, da die Mitarbeiter während dieser Zeit andere, nicht ganz so wichtige Aufgaben anpacken können.

In der Praxis ist der ständige Wechsel zwischen Kopieren und Telefonieren aber mit beträchtlichem Mehraufwand verbunden – nichts kommt wirklich voran. In kritischen Systemen wie dem Auto erhalten daher meistens die quengelnden Prozessoren den Vorzug.

Brandenburg und seine Gruppe sind nicht die Ersten, die sich dieses Problems annehmen. Bislang haben Informatiker die geteilten Ressourcen aber meist von Hand analysiert: Sie haben über mögliche Verzögerungen nachgedacht und daraus einen Maximalwert für die Antwortzeit ermittelt. Dabei genügt allerdings eine falsche Annahme, um zu einem Ergebnis zu kommen, das nicht mehr sicher ist. Zudem fallen die Abschätzungen unglaublich pessimistisch aus. Entsprechend unrealistisch sind die Ergebnisse. „Von den Ingenieuren hört man dann: Schön, dass ihr nun eine sichere Antwort habt, aber in der Praxis wird der Wert nie so hoch sein. Das ist nutzlos“, erzählt Brandenburg.

EINE OBERGRENZE FÜR MÖGLICHE BLOCKADEN

Die Max-Planck-Forscher wählen deshalb einen anderen Weg. Sie erstellen zunächst eine Gesamtmenge von Arbeitsabläufen, die in einem Büro – oder einem Echtzeitsystem – theoretisch nicht unmöglich sind, die also erst einmal nicht ausgeschlossen werden können. Anschließend blenden sie nach und nach all die Fälle aus, die in der Praxis nicht passieren können. Zum Beispiel ist es undenkbar, dass eine Bürokraft alle Geräte gleichzeitig benutzen will.

Letztlich kommen auf diese Weise Dutzende oder gar Hunderte Beschränkungen zusammen. All das lässt sich in Gleichungen packen. Schritt für Schritt schrumpft somit die Menge aller nicht ausgeschlossenen Aufgaben zusammen – so lange, bis eine Obergrenze gefunden ist für all die Prozesse, die die geplanten Abläufe im Büro blockieren können. Dieser Wert kann dann als weiterer Faktor in jene Algorithmen einfließen, mit denen die Pünktlichkeit der Echtzeitsysteme bewiesen wird.

„Lineare Optimierung“ heißt das zugrunde liegende Verfahren, das in der Mathematik seit mehr als sechzig Jahren angewandt wird. Inzwischen haben Informatiker daraus sehr viele, sehr schnelle Analysesysteme entwickelt, deren Algorithmen die Max-Planck-Forscher auf Echtzeitsysteme anpassen können. Brandenburg sagt: „Wir können nun deutlich kompliziertere Zusammenhänge analysieren und haben dadurch unheimliche Fortschritte bei der Genauigkeit gemacht.“

All das ist in der Praxis vor allem deshalb wichtig, weil viele Echtzeitsysteme heutzutage sogenannte Multicore-Prozessoren verwenden. Mehrere voneinander unabhängige Rechenkern teilen sich dabei die Arbeit, sie greifen auf gemeinsame Ressourcen zurück, sie werkeln nebeneinanderher, ohne sich großartig abzusprechen. „Für Echtzeitsysteme stellen Multicore-Prozessoren eine extreme Herausforderung dar“, sagt Björn Brandenburg.

Die Informatik hinkt da hinterher. Lange Zeit galten die komplexen Prozessoren als theoretisches Problem, als et-



was, das bei zeitkritischen Anwendungen nicht verbaut wird. Heute sind die Anforderungen selbst im Auto so hoch, dass Multicore-Prozessoren fast schon Standard geworden sind. Die bewährten Algorithmen funktionieren hier nicht mehr, alles muss neu entwickelt werden. „Das bislang verwendete Argument: Wenn ein Prozessor einer Aufgabe nachgeht, dann können andere, potenziell störende Aktivitäten zur gleichen Zeit nicht stattfinden, ist ein unheimlich mächtiges Element in der Beweisführung“, sagt Brandenburg. „Bei Multicore-Systemen funktioniert das nicht mehr, da weiß ich nie, was die anderen Kerne gerade machen.“

Vor allem die maximal benötigte Rechenzeit, die sich bereits auf modernen Einkernprozessoren kaum ermitteln lässt, stellt Informatiker vor große Herausforderungen. Auch die Frage, wie stark ein Multicore-Prozessor ausgelastet ist und wie viel Zeit er sich mit seinen Antworten lässt, ist ungeklärt. Bislang konnten die Forscher lediglich zeigen, dass der schlimmste anzunehmende Fall, in dem sämtliche Prozesse mit hoher Priorität den Rechner gleichzeitig auslasten, unter gewissen Umständen existieren muss. Wie er aussieht, wie er in Formeln gepackt werden kann und wie sich dadurch die Analyse verbessern lässt, bleibt offen.

Noch ein weiteres – wesentlich menschlicheres – Problem macht den Max-Planck-Forschern zu schaffen. Viele Theoretiker, die an neuen Algorithmen für Mehrkernprozessoren tüfteln, sind zwar mathematisch gut geschult, sie sitzen jedoch selten im Labor und

schreiben Programme. Die Ingenieure in der Industrie dagegen sind hochspezialisiert und bringen mit ihren Tricks sogar die obskursten Systeme zum Laufen. Sie sind aber nicht unbedingt die besten Mathematiker.

Stattdessen versuchen sie, ihre Erfahrung in mehrere Tausend Seiten umfassende Regelwerke zu pressen, die – wie beispielsweise im Automobilbau – die Anforderungen an jedes System

im Detail vorgeben. Das wiederum missfällt den Theoretikern, die für ihre Sicherheitsbeweise so wenige Vorgaben wie möglich bevorzugen. „Ein Teil meiner Forschungsarbeit besteht darin, in der Mitte zu sitzen und zu sagen: Ich verstehe die Mathematiker, ich verstehe die Praktiker, ich versuche da mal zu dolmetschen“, sagt Brandenburg. Gerade in der Echtzeitforschung ist es dafür höchste Zeit. ◀

AUF DEN PUNKT GEBRACHT

- Wenn es etwa um die Sicherheit von Autos oder Flugzeugen geht, muss Elektronik Daten absolut zuverlässig in einer festgelegten Zeit verarbeiten. Ob solche Echtzeitsysteme tatsächlich pünktlich ihre Aufgaben erledigen, können Experimente nicht zweifelsfrei belegen. Dafür braucht es mathematische Beweise.
- Moderne elektronische Prozessoren besitzen mehrere Rechenkerne, bearbeiten mehrere Aufgaben parallel und variieren ihre Taktfrequenz. Das macht die mathematische Beschreibung solcher Systeme und die Beweise, dass sie funktionieren, sehr kompliziert.
- Max-Planck-Forscher gehen bei der Beweisführung teilweise neue Wege, etwa indem sie auf die lineare Optimierung setzen. So können sie kompliziertere Zusammenhänge genauer analysieren als bisher.

GLOSSAR

Echtzeitsystem: Ein System, wie etwa eine elektronische Steuerung oder ein Mikrocomputer, das einen Prozess zwingend innerhalb einer vorgegebenen Zeit abarbeiten muss. Echtzeitsysteme kommen bei sicherheitsrelevanten Aufgaben, etwa der Steuerung eines Airbags, zur Anwendung.

Lineare Optimierung: Sucht für ein Problem, das als lineare mathematische Gleichung oder Ungleichung formuliert werden kann, die optimale Lösung unter gegebenen Randbedingungen, die sich ebenfalls in linearen Gleichungen oder Ungleichungen ausdrücken lassen.

Widerspruchsbeweis: Ein indirekter Beweis, der eine Aussage belegt, indem er ihr Gegenteil widerlegt. Die zu widerlegende Aussage wird dabei so weit reduziert, dass sich ein Widerspruch zu einer als gesichert angenommenen These ergibt.

Ein Weg aus dem inneren Gefängnis

Die Lähmung beginnt schleichend, doch mit der Zeit erfasst sie den ganzen Körper. Irgendwann können Menschen, die an amyotropher Lateralsklerose erkranken, keinen Muskel mehr bewegen und auch nicht mehr mit ihrer Außenwelt kommunizieren. Forscher um **Moritz Grosse-Wentrup** suchen am Tübinger **Max-Planck-Institut für Intelligente Systeme** nach Wegen, die Betroffenen aus ihrer Isolation zu befreien, indem sie dem Computer beibringen, Gedanken zu lesen.

TEXT **TIM SCHRÖDER**

Dass etwas nicht stimmt, merkt Wilfried Leusing, nachdem ihm Ärzte Implantate für eine Zahnprothese in den Kiefer gesetzt haben. Die Zunge fühlt sich taub an. Er kann nur undeutlich sprechen. Die Zunge müsse sich erst von der Operation erholen, sagen die Ärzte. Doch es wird nicht besser. Eine Neurologin schickt ihn in die Uniklinik Tübingen. Die Diagnose ist ernüchternd: „Verdacht auf Motoneuronerkrankung.“ Motoneurone sind Nervenzellen, die die Muskeln steuern – in den Fingern, im Brustkorb, in der Zunge.

Die Schaltzentrale dieser Neurone befindet sich oben in der Mitte des Gehirns, in der Hirnrinde: ein dichtes Geflecht aus Nervenzellen, der Motorcortex. Versagen die Nervenzellen im Motorcortex, kann der Körper die Muskeln nicht mehr bewegen, obwohl diese intakt sind. Wilfried Leusing trägt es mit Fassung: „Es war kein Schlag für mich, aber für meine Frau“, sagt er heute. Damals, im Frühjahr 2010, sucht er weitere Spezialisten in Kliniken in München und Ulm auf: doch überall derselbe Befund.

Wilfried Leusing hat ALS, amyotrophe Lateralsklerose, eine Krankheit, bei der die Zellen im Motorcortex langsam

absterben. Das Tempo, mit dem die Neurone ausfallen, variiert von Patient zu Patient. Manche Menschen können zwei Jahre nach der Diagnose Arme und Beine nicht mehr bewegen. Bei Wilfried Leusing schreitet die Krankheit langsamer voran.

VIELE ERKRANKTE WOLLTEN AN DER STUDIE TEILNEHMEN

Heute, vier Jahre nach dem Befund, kann er kaum noch sprechen. Auch das Schlucken fällt ihm schwer. Seit seine Zunge halbseitig gelähmt ist, sei ihm klar geworden, was für komplexe Vorgänge Kauen und Schlucken sind, schreibt er auf seiner Website „Das Alternativ“. „Die Zunge schiebt den Nahrungsbrei zwischen die Zähne und befördert ihn schließlich nach hinten.“ Mit der Lähmung geht das nicht mehr. Wilfried Leusing presst sich jetzt Flüssignahrung über einen kleinen Schlauch in den Magen. Was er erzählen möchte, tippt er in einen Tablet-PC ein. Ein Programm liest den Text dann vor.

„Durch die Krankheit habe ich das Schreiben neu für mich entdeckt“, erzählt er über seinen Computer. Er könne zwar nicht mehr durch Sprechen kommunizieren. Aber es gebe ja auch andere Wege, Inhalte und Emotionen

rüberzubringen. „Ich habe ganz neue Erfahrungen gemacht, nicht trotz, sondern gerade wegen meiner Erkrankung.“ Seit wenigen Monaten nimmt Wilfried Leusing an einer Studie des Max-Planck-Instituts für Intelligente Systeme in Tübingen teil; auch das ist eine neue Erfahrung. Der Projektleiter ist Moritz Grosse-Wentrup, als Elektrotechniker zuständig für die Forschungsgruppe „Gehirn-Computer-Schnittstellen“.

Im vergangenen Jahr hatte Moritz Grosse-Wentrup im Internet Probanden gesucht. Rund 15 000 ALS-Erkrankte gibt es in Deutschland – viele haben sich gemeldet. Zunächst hat er vier



Der direkte Weg vom Gehirn zum Computer: Die Elektroden, die am Kopf des Studenten Sebastian Weichwald befestigt sind, messen die Aktivität in verschiedenen Hirnarealen. Durch den Wechsel zwischen beiden Konzentrationszuständen, die charakteristische Erregungsmuster erzeugen, versucht Weichwald, einen Ball auf einem Monitor zu steuern, der im Bild nicht zu sehen ist.



Wegbereiter aus der Isolation: Moritz Grosse-Wentrup (links) hat einen Denkprozess gefunden, über den ALS-Patienten möglicherweise auch noch mit der Außenwelt kommunizieren können, wenn ihr Motorcortex stark geschädigt ist. Über die Aktivität im sogenannten Default-Mode-Network aus verschiedenen Hirnarealen, die etwa bei Emotionen besonders aktiv sind, sollen Patienten einen Ball auf einem Bildschirm steuern. In einer Studie wird die Software derzeit mit ALS-Erkrankten und gesunden Probanden wie Sebastian Weichwald, der zum Max-Planck-Team gehört, getestet.

Menschen für die Studie ausgewählt; einer von ihnen ist Wilfried Leusing, der ebenfalls in Tübingen lebt und Moritz Grosse-Wentrup mit seiner lebensbejahenden Haltung beeindruckt hat.

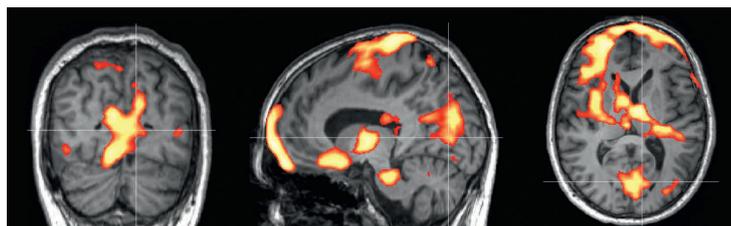
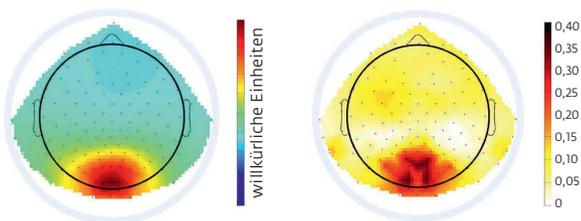
MANCHER PATIENT IST IM KÖRPER EINGESCHLOSSEN

Das Fatale an der Krankheit ALS ist, dass nach und nach alle Funktionen, für die der Körper Muskeln einsetzt, ausfallen. Es beginnt mit kleinen Lähmungen, dann versagen die Gliedmaßen. Zunge und Kehlkopf streiken, was das Schlucken unmöglich macht. Irgendwann

liegt der Erkrankte da, unfähig, sich zu regen und zu kommunizieren, denn auch sprechen kann er nicht mehr. In manchen Fällen setzt die Augenmuskulatur aus. Dann können die Patienten ihr Gegenüber nicht mehr fixieren. „Fachleute nennen diesen Zustand locked-in“, sagt Grosse-Wentrup. „Der Patient ist in seinem Körper völlig eingeschlossen.“ Im Spätstadium können die Betroffenen nicht einmal mehr mitteilen, ob ihnen etwas wehtut. „Wir wissen von Patienten, deren Lungenentzündung zu spät bemerkt worden ist, weil sie sich nicht mehr mitteilen konnten.“

Einige Wissenschaftler, wie der Neurobiologe Niels Birbaumer von der Universität Tübingen, gehen davon aus, dass die Patienten nach und nach in einen traumartigen Zustand hinübergleiten. Ihre Theorie: Für gewöhnlich kann ein Mensch die Umwelt beeinflussen, durch Anfassen, Gesten, Sprache oder Blicke kommunizieren. Verliert der Mensch die Fähigkeit zur Interaktion, kehrt sich sein Bewusstsein nach innen. Es gibt keinen Kontakt mehr zur Außenwelt.

Die Verbindung nach draußen möchte Moritz Grosse-Wentrup wenigstens zu einem kleinen Teil wiederherstellen. Sein Ansatz klingt kühn: Im Spätstadium,



Nahe am Ideal: Damit ALS-Patienten über ihre Hirnaktivität mit der Außenwelt kommunizieren können, möchten Max-Planck-Forscher im EEG ein Aktivitätsmuster im hinteren Bereich des Gehirns aufzeichnen, wie es im Bild ganz links zu sehen ist. In der Messung an einem ALS-Erkrankten beobachteten sie das im mittleren Bild dargestellte Erregungsmuster, das sehr gut mit dem gewünschten Muster übereinstimmt. Dazu gehören Aufnahmen im funktionellen Kernspintomografen, bei denen eine wesentliche Aktivität ebenfalls im hinteren, durch das Fadenkreuz markierten Bereich des Gehirns zu beobachten ist.

wenn nichts mehr geht, soll der Patient über seine Gedanken, oder besser: die Hirnaktivität, kommunizieren. „Der Patient soll auf diese Weise Antworten auf einfache Ja/Nein-Fragen geben“, sagt Grosse-Wentrup. Haben Sie Schmerzen? Möchten Sie Radio hören?

Um ALS-Patienten diesen Weg aus dem inneren Gefängnis zu öffnen, müssen Grosse-Wentrup und seine Mitarbeiter zunächst aber lernen, die Denkaktivität richtig zu deuten. Sie sind nicht die Einzigen, die Gelähmten einen direkten Weg aus dem Gehirn zur Außenwelt verschaffen möchten – ohne Vermittlung irgendeiner Muskulatur. Unter anderen versuchen Forscher der Brown University in Providence in den USA mit Experten vom Deutschen Zentrum für Luft- und Raumfahrt, Signale aus dem Gehirn auszulesen und zu nutzen. Sie haben eine Methode entwickelt, mit der beispielsweise Querschnittsgelähmte eine Roboterhand bewegen können. Ihre Videos im Internet zeigen eine Probandin, die mit der Kraft ihrer Gedanken die Roboterhand zu einer Plastikflasche führt. Die Frau lächelt glücklich, als sie zum ersten Mal ohne Hilfe am Strohhalm saugt.

Die US-Forscher verwenden für ihre Experimente kleine Elektroden, die sie den Patienten unter den Schädelknochen direkt in den Motorcortex implantieren. Diese Elektroden nehmen die Aktivität der Neurone wahr. Der Trick besteht darin, dass sogar gedachte Bewegungen die Neurone im Motorcortex anregen. Der Motorcortex ist bei vielen Gelähmten also auch dann aktiv, wenn der Körper die Bewegung gar nicht ausführt. Die Elektroden nehmen die Signale der Neuronen auf und leiten sie zu einem Computer, der die Impulse in Steuerbefehle für den Roboterarm übersetzt. Natürlich muss der Patient lange trainieren. Am Ende aber reicht es, dass er sich eine Handlung vorstellt, um den Roboter zu steuern. Die Erfolge der US-Forscher sind beeindruckend.

Bei ALS-Patienten aber klappt das nicht, weil bei ihnen ja ausgerechnet

der Motorcortex gestört ist. „Wir müssen also andere Hirnregionen, andere Signale finden, über die der ALS-Patient kommunizieren kann“, sagt Grosse-Wentrup. Es sieht ganz so aus, als habe Grosse-Wentrup einen Weg gefunden. Seit einigen Jahren wissen Neurologen, dass bei verschiedenen Tätigkeiten verschiedene Hirnbereiche gleichzeitig aktiv sind. Das Denken findet nicht an einem einzigen Punkt im Gehirn statt. Stattdessen funken bestimmte Areale bei verschiedenen Denkprozessen in einer Art fein abgestimmter Polyphonie.

Besonders interessant ist für Moritz Grosse-Wentrup ein Aktivitätsmuster, das auftritt, wenn ein Mensch sich auf sich selbst konzentriert, die Gedanken nach innen richtet, meditiert: das Default-Mode-Network oder Ruhezustandsnetzwerk. Dabei sind gleichzeitig ein Bereich hinter der Stirn und ein zweiter tiefer im Gehirn aktiv. Konzentriert sich der Mensch hingegen auf eine Tätigkeit – liest oder rechnet er –, dann nimmt die Aktivität des Default-Mode-Networks ab.

DAS RUHEZUSTANDSNETZ IST WENIGER BETROFFEN VON ALS

Grosse-Wentrup glaubt, dass ALS-Patienten durch einen solchen Wechsel zwischen zwei Konzentrationszuständen auch im Spätstadium kommunizieren und Ja/Nein-Antworten geben können. Denn das Ruhezustandsnetzwerk ist von der ALS-Erkrankung weniger betroffen als der Motorcortex.

Das Experiment der Tübinger sieht folgendermaßen aus: Mithilfe ihrer Gedanken müssen die Patienten versuchen, eine Kugel auf einem Bildschirm nach oben oder unten zu bewegen. Oben heißt „Ja“, unten heißt „Nein“. Die Höhe der Kugel entspricht der Stärke der Aktivität im Default-Mode-Network – Änderungen im Erregungszustand bewegen den Ball daher. Seitlich kann sich der Ball derzeit nicht verschieben.

Anders als die Forscher in den USA benutzt Grosse-Wentrup keine Elektro-



Wilfried Leusing, der an ALS erkrankt ist, möchte dazu beitragen, anderen Patienten das Leben zu erleichtern. Daher nimmt er an der Studie der Max-Planck-Forscher teil.

den, die direkt in den Cortex implantiert werden. Die Infektionsgefahr sei zu groß, sagt er. Außerdem bildeten sich durch Abstoßungsreaktionen des Körpers auf den Elektroden häufig Beläge, sodass die Signalleitung zum Computer gestört wird. Er benutzt daher lieber das klassische Elektroenzephalogramm (EEG). Der Proband setzt dafür eine Haube mit vielen kleinen Elektroden auf, welche die elektrischen Signale der Neuronen durch den Schädelknochen hindurch wahrnehmen. Natürlich ist ein solches Signal ungenauer als jenes von Elektroden, die direkt auf dem Gehirn sitzen. Doch das reiche erst einmal, sagt Grosse-Wentrup.

„Ich gebe den Probanden möglichst wenig vor“, sagt er. „Jeder Patient muss für sich einen eigenen Weg finden, Gehirnaktivität im Default-Mode-Network zu beeinflussen und dadurch den Ball nach oben oder unten zu bewegen.“ Sich meditativ nach innen zu wenden ist nur eine Möglichkeit, das Ruhezustandsnetzwerk zu aktivieren. Einigen gelingt das auch, indem sie verschiedene Emotionen in sich wecken. Denn verschiedene Gefühle führen auch zu einer unterschiedlichen Aktivität im Default-Mode-Network. >



Lehrmeister für Computer: Moritz Grosse-Wentrup und Bernhard Schölkopf bringen Computern bei zu lernen. Damit die von ihnen entwickelte Software Muster in Signalen erkennt, muss sie mit vielen Daten trainiert werden.

Die Elektroden der EEG-Haube werden mit etwas Gel eingeschmiert, damit sie die elektrische Erregung im Gehirn besser aufnehmen. „Und so hatte ich nach meiner ersten Sitzung im Januar zum ersten Mal in meinem Leben Gel im Haar“, sagt Wilfried Leusing, der einen langen weißen Bart und lange Haare trägt.

Knapp zehnmal waren Grosse-Wentrup und seine Leute inzwischen bei ihm und den anderen Probanden. „Mit Auf- und Abbau dauert eine solche Sitzung etwa fünf Stunden, das ist ganz schön aufwendig“, lässt Leusing seinen Computer sagen. „Aber es ist ein Supergefühl, wenn man mit tollen Menschen zusammen etwas erarbeiten kann, das sinnvoll ist. Und mein Beitrag bin einfach ich.“ Inzwischen kann Leusing den Ball flott nach oben bewegen. „Wenn er sich in eine falsche Richtung bewegt, bekomme ich ihn mit einem gedachten ‚Nein‘ wieder in die andere Richtung.“ Bewusst nach unten drücken kann er ihn jedoch noch nicht. Übung macht eben den Meister.

Für Moritz Grosse-Wentrup und seine Mitarbeiter beginnt die eigentliche Arbeit, wenn sie wieder im Institut sind: die Analyse des EEG. Als Laie erkennt man im Elektroenzephalogramm zunächst nur einige Zitterlinien, die

langsam von rechts nach links über den Bildschirm kriechen. Sie zeigen die Hirnaktivität als elektrische Spannung an. Die Linien unterscheiden sich in der Geschwindigkeit des Zitterns, der Geschwindigkeit der Spannungsänderung. Mediziner sprechen von Frequenzbändern oder Wellen.

DIE SOFTWARE LERNT DIE ZITTERMUSTER ZU DEUTEN

Und von den Wellen gibt es viele: Die Hauben, die Grosse-Wentrup und seine Mitarbeiter ihren Probanden aufziehen, sind mit 128 Elektroden bestückt, die jeweils 40 Frequenzbänder aufnehmen. Pro Messung kommen so mehr als 5000 Variablen zusammen. Eine Datenfülle, die kein Mensch überblicken kann. Um die Signale zu interpretieren, nutzt Grosse-Wentrup deshalb statistische Rechenverfahren, die im Max-Planck-Institut für Intelligente Systeme entwickelt worden sind. Ziel ist es, in dem Gewimmel aus Zitterlinien charakteristische Muster zu erkennen, die immer dann auftreten, wenn der Patient den Ball bewegt.

Welches Zittermuster typisch ist, findet die Software durch eine Art Lernprozess heraus, in dem sie die vielen Messwerte ordnet. Wie das funktio-

niert, erläutert Bernhard Schölkopf, Direktor am Institut und zuständig für die Abteilung Maschinelles Lernen, an einem einfachen Beispiel. „Stellen Sie sich vor, ein Computer müsse zwischen einer undeutlich hingeschmierten Acht und einer Neun unterscheiden“, sagt Schölkopf. „Das ist zunächst unmöglich. Wenn man dem Computer aber unzählige Achten und Neunen präsentiert, ihn also auf die Zahlen trainiert, dann lernt er zu unterscheiden.“

Bei einem solchen Verfahren ordnet der Computer die Pixel, aus denen die Zahl besteht, in einem multidimensionalen Raum an und vergleicht sie mit den antrainierten Daten. Er vergleicht und analysiert, mit welcher Wahrscheinlichkeit die Pixel eher mit dem erlernten Muster der Acht oder jenem der Neun deckungsgleich sind.

Nach ähnlichen statistischen Lern- und Entscheidungsverfahren arbeiten auch vollautomatische Postsortiermaschinen, die hingeschmierte Buchstaben auf Briefumschlägen erkennen können. Moritz Grosse-Wentrup versucht jetzt, den Computer auf die Frequenzbänder des EEG zu trainieren. Der Computer soll lernen, charakteristische Aktivitätsmuster im Hirn schneller und sicher zu erkennen, wenn der Patient den Ball bewegt.

Letztlich geht es darum, dass Proband und Computer sich schnell verstehen. Immerhin soll der Computer die gedachten Befehle des Probanden künftig zügig in eine Antwort umsetzen. Der Patient muss lernen, den Ball auf dem Bildschirm zu steuern, der Computer, wie die entsprechenden Aktivitätsmuster aussehen, damit er sie sicher und zügig in die Ballhöhe umsetzt. „Wir sehen bereits, dass wir auf Fragen desto schneller eine richtige Antwort erhalten, je besser der Computer die Frequenzmuster erlernt“, sagt Grosse-Wentrup. Für den Alltag der ALS-Patienten wird das später essenziell sein, denn auf eine einfache Frage wie „Haben Sie Schmerzen?“ soll es natürlich eine schnelle Antwort geben.

Zusammen mit Niels Birbaumer von der Universität Tübingen arbeitet Schölkopfs Abteilung seit zehn Jahren daran, mit ALS-Kranken über Denkbefehle zu kommunizieren. Allerdings hatten sie zunächst Denkprozesse und Vorstellungen gewählt, die letztlich ungeeignet waren. Es zeigte sich, dass die Denkprozesse und Spannungsmuster der Neuronen zu stark von der Tagesform des Patienten abhängen und der Computer das Denken nur schlecht interpretieren konnte. Als die Krankheit fortschritt, versagten die Methoden irgendwann ganz. „Moritz scheint ein anderes Paradigma, einen anderen Denkprozess gefunden zu haben, der robuster ist“, sagt Schölkopf.

Um den Computer mit vielen Trainingsdaten füttern zu können, testet Grosse-Wentrup sein Verfahren auch an gesunden Studienteilnehmern. In den vergangenen fünf Jahren haben er und seine Mitarbeiter bei etwa hundert Studenten EEG-Messungen vorgenommen. Es sieht ganz so aus, als sei Grosse-Wentrup Verfahren tatsächlich robust. Zwar muss sich die Computer-Lernmaschine bei jedem Versuch einige Zeit auf die Denkmuster des Probanden einstellen, doch recht bald bewegt sich der Ball. Ganz offensichtlich gibt es also Denkmuster, die bei allen Menschen ähnlich genug sind, sodass maschinelle Lernverfahren sie erkennen können. Dabei laufen Denkprozesse im Detail bei jedem Patienten etwas anders ab und verändern sich mit der Tagesform.

Da Moritz-Grosse Wentrup erst seit knapp einem halben Jahr mit Wilfried Leusing und den anderen ALS-Patienten arbeitet, ist noch offen, ob seine Methode auch im Spätstadium der Krankheit funktionieren wird. Dass sie schon jetzt sehr robust ist, lässt ihn hoffen. Bei einem seiner Patienten schreitet die Krankheit schnell voran, er hat bereits Schwierigkeiten, die Gliedmaßen zu bewegen. Bei ihm könnte sich als Erstem zeigen, ob die neue Methode ein verlässlicher Weg zur Außenwelt ist, wenn sich der Körper langsam schließt.

MEHR MESSDATEN NÖTIG

Moritz Grosse-Wentrup hatte sich ursprünglich für das Elektrotechnik-Studium entschieden, um später in die Robotik einzusteigen. Dann erfuhr er von den Arbeiten an ALS-Patienten. Die Arbeit für Menschen sei für ihn heute sehr viel erfüllender als Robotik, sagt er. Sollte sich zeigen, dass seine Methode, sein Denkmuster-Paradigma, auch im Spätstadium der Krankheit funktioniert, dann kann er sich vorstellen, vom EEG auf implantierte Elektroden um-

zusteigen, die nicht über ein Kabel an einen Computer angeschlossen sind, sondern die Daten per Funk übertragen. Entsprechende Elektroden werden derzeit entwickelt. Eine solche Elektrode wäre für den Alltags Einsatz ideal. Und sie würde deutlichere Frequenzsignale liefern.

Doch zunächst benötigt Grosse-Wentrup mehr Messdaten von seinen ALS-Patienten. Wilfried Leusing will seinen Teil dazu beitragen und sich weiterhin einmal pro Woche mit den Forschern treffen. Grosse-Wentrup oder seine Mitarbeiter kommen dann jedes Mal mit einem Wäschekorb voller Kabel und Elektroden vorbei. „Es ist für jeden Menschen wichtig, dass ihm bewusst ist, welche Rolle er in seinem Leben spielt“, teilt Wilfried Leusing über seinen Computer mit. Eine seiner Rollen ist die des Probanden, der seinen Teil dazu beiträgt, ALS-Kranken künftig ein Stück weit das Leben zu erleichtern – selbst wenn er davon vielleicht nicht mehr selbst profitieren wird. ◀

 www.mpg.de/filme/gehirn_computer_schnittstelle

AUF DEN PUNKT GEBRACHT

- **Patienten, die an amyotropher Lateralsklerose (ALS) erkranken, leiden unter einer fortschreitenden Lähmung. Irgendwann können sie nicht mehr sprechen und manchmal nicht einmal mehr die Augen bewegen. Damit verlieren sie jede Möglichkeit, mit der Außenwelt zu kommunizieren.**
- **Forscher um Moritz Grosse-Wentrup vom Max-Planck-Institut für Intelligente Systeme in Tübingen wollen ALS-Patienten einen Weg aus der inneren Isolation öffnen. Sie bringen den Betroffenen bei, über die Aktivität im Default-Mode-Network einen Ball auf einem Computerbildschirm zu steuern und so Ja/Nein-Antworten zu geben.**
- **Die Aktivität im Default-Mode-Network greifen die Wissenschaftler mithilfe von Elektroden ab, die wie beim EEG am Kopf angebracht werden. Mit Methoden des maschinellen Lernens bringen sie einem Computer bei, das Erregungsmuster im Gehirn zu interpretieren und in Steuersignale umzusetzen.**
- **Derzeit verfeinern die Forscher die Methoden, mit denen die Gehirnaktivität analysiert wird, mithilfe von vier ALS-Patienten und rund hundert gesunden Probanden.**

GLOSSAR

Amyotrophe Lateralsklerose – ALS: Bei dieser neurodegenerativen Erkrankung sterben die Nervenzellen im Motorcortex langsam ab, sodass betroffene Patienten letztlich keine Bewegung mehr ausführen können.

Default-Mode-Network: Das Default-Mode-Network, auch Ruhezustandsnetzwerk genannt, besteht aus Arealen im vorderen und hinteren Bereich des Gehirns, die besonders im Ruhezustand, aber auch bei Emotionen aktiviert sind.

Maschinelles Lernen: Dabei lernen Computer, Muster in Daten zu erkennen, indem sie Beispiele analysieren und daraus allgemeine Regeln ableiten. Auf diese Weise können sie etwa Handschriften entziffern oder Aktivitätsmuster im Gehirn interpretieren.



Dialog der Maschinen

Damit es im Straßenverkehr sicherer zugeht oder Strom aus regenerativen Quellen optimal genutzt werden kann, sind cyber-physikalische Systeme gefragt. Sie verbinden Fahrzeuge mit Sensoren, die den Verkehr beobachten, und schicken etwa bei Gefahr Bremsbefehle an Autos. Oder sie verteilen den Strom aus vielen Kraftwerken möglichst effizient an die Verbraucher.

Rupak Majumdar, Direktor am **Max-Planck-Institut für Softwaresysteme** in Kaiserslautern, entwickelt mathematische Methoden, um die Zuverlässigkeit der vernetzten Systeme zu garantieren.

TEXT **GORDON BOLDUAN**

Alles ist vorbereitet im Konferenzsaal der Universität des Saarlandes. Angestellte der Presseabteilung haben die Tische über den hellen Parkettboden zu einem U zusammengeschoben und darauf Namensschilder platziert. Dazwischen steht das orangefarbene Mikrofon des Deutschlandfunks. Am offenen Ende des U haben sich Reporter des saarländischen Rundfunks samt Kamera und Stativ positioniert. Sie drehen für die *Tagesschau*. Für einen kurzen Moment macht der Kameramann eine Großaufnahme des Namensschildes, auf dem „Rupak Majumdar“ zu lesen ist. Dann zieht er das Bild groß. Es zeigt einen Mann, der ein schwarzes Sakko und darunter ein hellblaues Hemd ohne Krawatte trägt. Seine Haare sind schwarz, seine Augen hellbraun. Rupak Majumdar stammt aus Indien, ist 38 Jahre alt und Direktor des Max-

Planck-Instituts für Softwaresysteme in Kaiserslautern, Rheinland-Pfalz. Die Pressekonferenz findet statt, weil drei Informatikprofessoren der Universität des Saarlandes und er den höchstdotierten Preis des Europäischen Forschungsrates gewonnen haben. Mit 9,3 Millionen Euro sollen sie in den nächsten sechs Jahren erforschen, wie sich im World Wide Web der Widerspruch zwischen Sicherheit und Freiheit vereinbaren lässt. Das Internet ist ein Randgebiet von Majumdars Forschung.

Sein Fokus liegt auf den Grundlagen sogenannter cyber-physikalischer Systeme (CPS). Sie versprechen nicht nur wirtschaftliches Wachstum, sondern auch Antworten auf große gesellschaftliche Herausforderungen. Ihre Stärke: Sie sind sowohl in realer als auch in digitaler Welt verankert. Sie verbinden physikalische Sensoren und Steuerungen in Geräten, Gebäuden, Fahrzeugen,

Cyber-physikalisches Stromnetz: In Zukunft sollen mehr Solar- und Windkraftanlagen unsere Elektrizität liefern. Da ihr Angebot schwankt, könnte eine zentrale Regelung Angebot und Nachfrage erfassen und die Versorgung entsprechend steuern.

medizinischer Ausrüstung mit Kommunikationsnetzen wie dem Internet. Auf diese Weise können physikalische Daten in einer realen Umgebung erfasst und an jedem beliebigen Ort des Erdballs ausgewertet werden. Je nach Bedarf können die Ergebnisse weitere Rechenbefehle auslösen, welche dann wiederum über spezielle Aktoren die reale Welt verändern. Majumdar entwickelt Algorithmen, also Rechenverfahren, die es bereits in der Entwurfsphase ermöglichen, die Zuverlässigkeit solcher komplexer Systeme zu erhöhen.

Die Pressekonferenz ist zu Ende. Majumdar wischt schnell auf dem Smartphone empfangene E-Mails weg, dann eilt er zu seinem Fahrzeug. Kaiserslautern ist rund 70 Kilometer von Saarbrücken entfernt. Seit 2010 leitet er dort nicht nur das Max-Planck-Institut, er lebt dort auch mit seiner Frau und seinen zwei Söhnen. Majumdar ist in Eile. Er hat versprochen, seinen älteren Sohn von der Schule abzuholen und zu einem Kindergeburtstag zu bringen. Dafür muss er in rund einer Stunde in Kaiserslautern sein. In Zukunft sollen cyber-

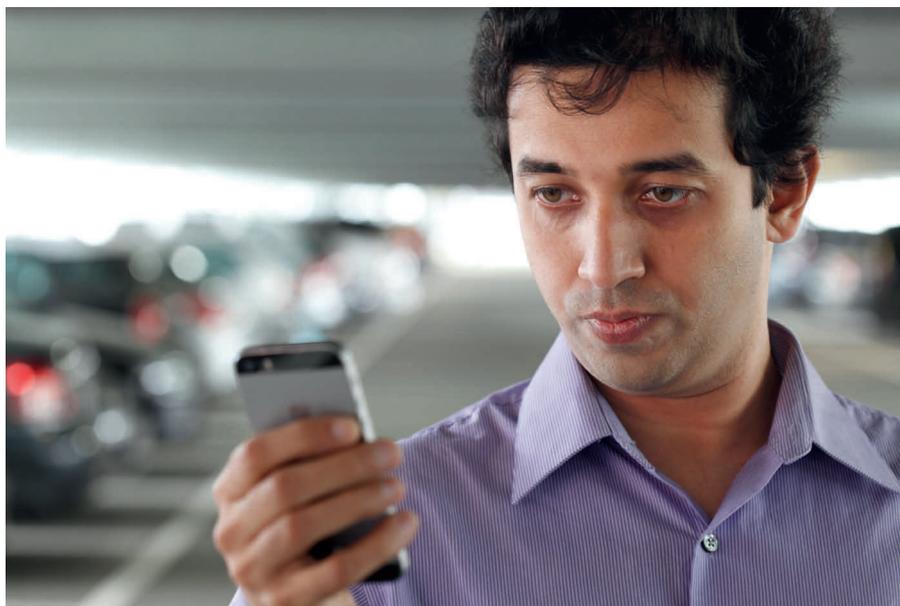
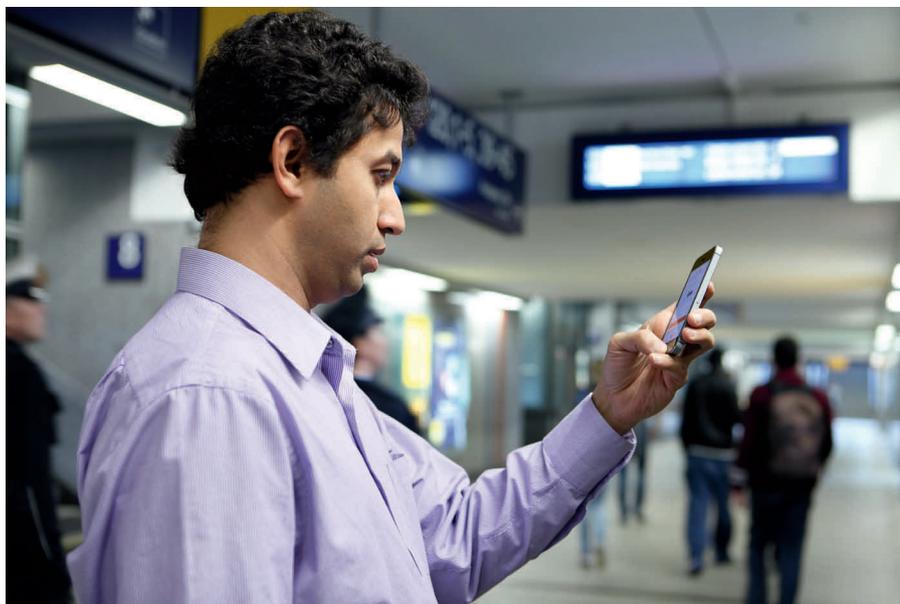
physikalische Systeme auch bei einem solchen Unterfangen helfen. Laut der Studie *agendaCPS* der Deutschen Akademie für Technikwissenschaften könnte das dann so aussehen:

Majumdar tippt das Fahrtziel in sein Smartphone und gibt zusätzlich die gewünschte Ankunftszeit, Zwischenstationen und Kosten an. Das Smartphone ist über das Internet mit verschiedenen Dienstleistern verbunden, kontaktiert diese und listet danach die Optionen auf. Majumdar entscheidet sich für die Regionalbahn. Sie ist preiswert, und er kann im Zug arbeiten. Das Smartphone schlägt ihm darauf vor, in Kaiserslautern in der Nähe des Bahnhofs das Angebot eines Car-Sharing-Anbieters wahrzunehmen. Mit dem Wagen könne er seinen Sohn von der Schule abholen und ihn zum Kindergeburtstag fahren.

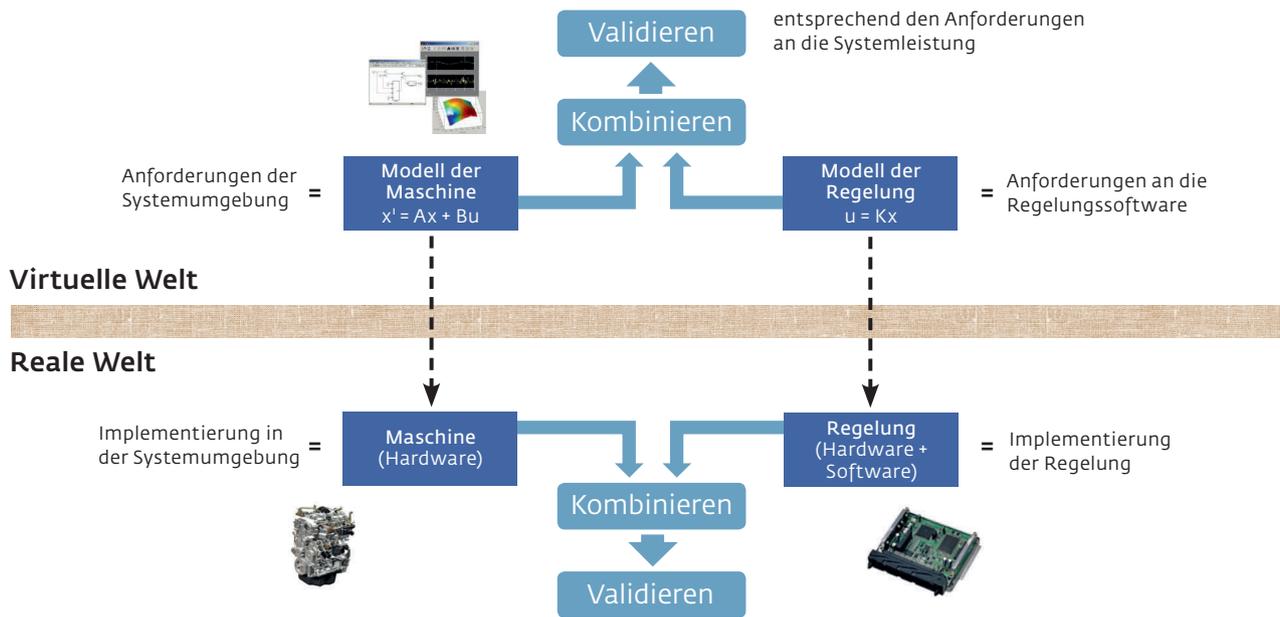
Majumdar stimmt zu. Auf dem Weg zum Saarbrücker Bahnhof piepst sein Handy. Die Kurznachricht besagt, dass ein technisches Problem bei einem vorausfahrenden Zug seinen 20 Minuten später eintreffen lässt, ergo sein Zeitplan gefährdet ist. Alternativ schlägt das System vor, bereits ab Saarbrücken einen Wagen zu mieten. Erneut stimmt Majumdar zu, das System startet im Hintergrund zwei weitere Aktionen: Es storniert das Ticket für die Regionalbahn und bucht den Mietwagen schon ab Saarbrücken. Um weiterhin während der Fahrt arbeiten zu können, klickt Majumdar noch auf die Option „selbstständig fahrendes Auto“. Als er wenige Minuten später die Autotür öffnet, hat das System bereits die komplette Route auf den Bordcomputer des Wagens gesendet.

Das ist möglich, weil das Smartphone mit einer Art virtuellem Butler im Internet verbunden ist. Dieser berechnet dort Majumdars Tagesplanung, basierend auf seinen Vorgaben. Der Assistent fordert stets auch aktuelle Daten an, beispielsweise bei Verkehrsmanagement-Systemen und den Betreibern des öffentlichen Nahverkehrs. Daraus berechnet er Alternativen und stellt

Persönliche Verkehrsplanung: Rupak Majumdar führt vor, wie ein cyber-physikalisches System künftig helfen könnte, verschiedene Verkehrsmittel wie den öffentlichen Nahverkehr und Autovermietungen miteinander zu vernetzen. Über Smartphones könnten wir die jeweils günstigsten Verbindungen ermitteln und auch spontan umdisponieren, zum Beispiel wenn ein Zug Verspätung hat.



Entwicklung einer Systemregelung



Lücke im System: Zwischen der virtuellen oder mathematischen Welt, in der eine Regelung entwickelt wird, und der realen Welt, in der Hard- und Software implementiert, also umgesetzt werden, klappt eine semantische Lücke. Daher können Mathematiker in vielen Fällen zwar beweisen, dass ein cyber-physikalisches System eine gewünschte Eigenschaft besitzt. Diese lässt sich wegen technischer Unzulänglichkeiten aber möglicherweise in der realen Welt nicht wie gewünscht umsetzen. Diese Kluft möchten Max-Planck-Forscher schließen.

diese zur Auswahl. Hat sich Majumdar entschieden, übernimmt der virtuelle Assistent regelmäßig den Realitätscheck. Treten Störungen auf, zeigt er Hinweise auf dem Display des Smartphones an und informiert darüber hinaus alle anderen Beteiligten über die Änderungen.

„In Los Angeles hätte so etwas mein Leben um einiges erträglicher gemacht“, erklärt Majumdar hinter dem Steuer seines Wagens. Sechs Jahre hat er dort als Professor an der University of California gelehrt und geforscht.

Die Szenarien der CPS-Propheten gehen noch weiter. Cyber-physikalische Systeme sollen den Verkehr nicht nur komfortabler und stressfreier, sondern auch sicherer machen. Dazu sollen Laternen, Häuserfassaden, Gehwege und Fahrzeuge mit Sensoren ausgerüstet werden, die frühzeitig gefährliche Objekte und gefährdete Personen erfassen.

Würde sich Majumdar beispielsweise der Schule seines Sohnes nähern und dabei einen haltenden Bus passieren, könnte das Auto plötzlich stark bremsen. Der mögliche Grund: Die Sensorik der Straße könnte ein Kind hinter dem Bus erkannt haben. Als dessen Position ohne zeitliche Verzögerung an den As-

sistenzdienst in Majumdar's Wagen übermittelt wird, entscheidet sich dieser sofort, auf Nummer sicher zu gehen. Er leitet die Bremsung ein und informiert gleichzeitig über sogenannte Fahrzeug-zu-Fahrzeug-Kommunikation die hinter Majumdar fahrenden Wagen. Diese bremsen ebenfalls ab, sodass es keinen Auffahrunfall gibt. Auf diese Weise hofft man, die Anzahl der Verletzten und Toten im Straßenverkehr erheblich zu senken.

HILFE FÜR SENIOREN IM NOTFALL UND BEIM EINKAUFEN

Auch zwei weitere gesellschaftliche Herausforderungen könnten sich mithilfe cyber-physikalischer Systeme leichter meistern lassen. Damit Senioren so lange wie nur möglich in ihrer gewohnten Umgebung bleiben können, sollen ihre Wohnungen, ihre Häuser mit Sensoren ausgerüstet werden, Elektrogeräte per Sprache steuerbar sein. Vernetzt bilden sie ein cyber-physikalisches System, das Verhaltensmuster des gesunden Bewohners erstellt und im Falle von Abweichungen einen Arzt alarmiert. Das System könnte für demente Menschen,

basierend auf ihren Vorräten, auch Einkauflisten erstellen und die Einnahme von Medikamenten überwachen. Es soll sogar erkennen, wenn Senioren stürzen, und Notfallmaßnahmen einleiten.

Auch bei der Energiewende spielen cyber-physikalische Systeme eine wichtige Rolle. Energie aus Sonne und Wind soll mehr und mehr den Bedarf decken. Doch die Beiträge dieser Energiequellen schwanken naturgemäß. Damit das Angebot dennoch stets die Nachfrage deckt, muss der Strom geschickt geregelt werden. Die Grundlage dafür ist ein riesiges Energieinformationsnetz, das die Steuerung des Stromnetzes mit Verbrauchern, Stromerzeugern und Stromspeichern kombiniert. Wichtige Komponenten dieses gigantischen Systems sind unter anderem Sensoren, die sich in Form von intelligenten Stromzählern in den Haushalten befinden, Informations- und Kommunikationstechnologie und lernfähige Rechenverfahren. Im Gegensatz zu bisherigen Stromzählern geben sie Verbrauchern unter Berücksichtigung des momentanen Strompreises und der aktuellen Netzlast Hinweise auf Stromfresser und einen sparsameren Verbrauch. >

„Ohne zwei entscheidende Entwicklungen der vergangenen Jahre wären solche Szenarien nicht einmal denkbar“, erklärt Manfred Broy, Professor für Informatik an der Technischen Universität München: „Da ist der Siegeszug des Internets, beflügelt durch immer leistungsstärkere und gleichzeitig preiswertere Rechner“, so der Professor. Dann sei da der zunehmende Einsatz eingebetteter Systeme. Das sind kleine Rechner, die in ihrer Leistungsfähigkeit zwar eingeschränkt sind, jedoch über Sensoren und Aktoren die physikalische Welt erfassen und steuern.

Allein diese Systeme stellen Forscher und Ingenieure bereits vor Herausforderungen, was Entwurf und Ent-

wicklung angeht. Cyber-physikalische Systeme erhöhen die Schwierigkeiten um ein Vielfaches. „Die Komplexität der Systeme, die wir bauen wollen, ist immer höher als die Komplexität, die wir noch auf vernünftige Weise überschauen können“, erklärt Majumdar. Das lässt sich auch an den Bremsen eines Autos nachvollziehen.

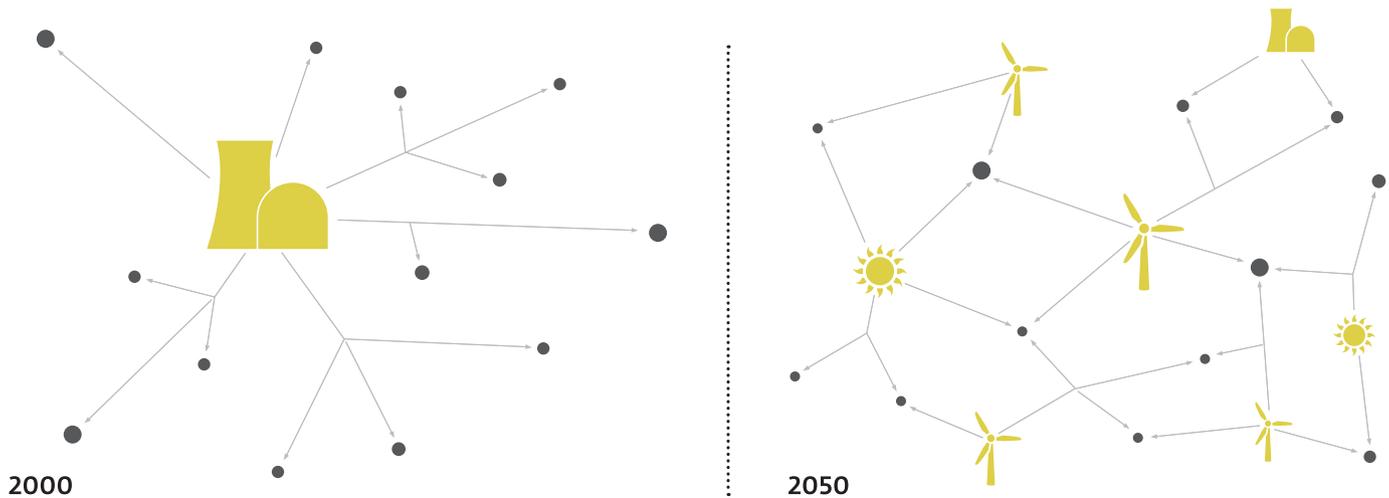
MEHR KOMPLEXITÄT: EIN NETZWERK VON FAHRZEUGEN

Im Jahr 1978 galt das Antiblockiersystem, ABS, als Meilenstein, um Lenkbarkeit und Spurtreue beim Bremsen zu erhöhen. Siebzehn Jahre später führte der Automobilzulieferer Bosch für die

Mercedes-S-Klasse das „elektronische Stabilisierungsprogramm“, kurz ESP, ein. Als Kombination von ABS, Antischlupfregelung und elektronischer Bremskraftverteilung sollte es durch gezieltes Abbremsen einzelner Räder dem Ausbrechen des Fahrzeugs entgegenwirken. 2003 brachte der japanische Autohersteller Honda dann das „Collision Mitigation Brake System“ auf den Markt. Diese Art von Notbremsassistent leitet das Bremsen per Bordcomputer automatisch ein, sobald er eine Situation als kritisch einstuft. Das System erkennt mittels Funkwellen und Laserstrahlen die Entfernung zwischen Fahrzeug und Hindernis. Ist diese zu gering, leitet es sogar eine Vollbremsung ein.



Vorausschauendes System: Die Sicherheit im Straßenverkehr ließe sich mit cyber-physikalischen Systemen erhöhen. Sensoren entlang der Straßen könnten unvorhersehbare Ereignisse registrieren – zum Beispiel dass ein Kind auf die Straße läuft. Eine Regelung, die mit den Sensoren und den Fahrzeugen vernetzt ist, würde ein nahendes Auto und auch folgende Autos dann automatisch stoppen.



Systemwechsel: Wenn uns künftig nicht mehr zentrale Großkraftwerke, sondern viele dezentrale Wind- und Solaranlagen mit Strom versorgen, könnte das elektrische Netz zu einem cyber-physikalischen System werden.

Mehr Funktionalität bedingt mehr Sensoren und Aktoren, deren korrektes Zusammenspiel erhöht die Komplexität. Ein ABS wirkt nur auf die Raddrehzahl und Bremskraft, per ESP werden der Lenkwinkel sowie verschiedene Beschleunigungskräfte überwacht, einzelne Räder gezielt angesteuert und der Motor gedrosselt. Der Notbremsassistent nimmt bereits die Umgebung wahr und erkennt Hindernisse. Aktuelle Technologien wie Computer Vision erkennen bereits Fußgänger. „Das alles spielt sich in einem Fahrzeug ab, und jetzt wollen wir auf ein Netzwerk zugreifen, das sich zwischen fahrenden Autos aufbaut. Das ist noch einmal eine ganz neue Komplexitätsebene“, erläutert Majumdar.

CYBER-PHYSIKALISCHES SYSTEM MIT VERANTWORTUNG

Diese zunehmende Komplexität immer zu beherrschen ist nur eine von vielen Herausforderungen, die Forscher auf diesem Gebiet meistern müssen. Aber auch die Gesellschaft ist gefordert. Sie muss sich nicht nur fragen, ob sie Sensoren und Programmcode die Verantwortung für eine Vollbremsung überlässt, sondern auch Regeln und Richtlinien festlegen für andere Einsatzgebiete der cyber-physikalischen

Systeme wie die Betreuung von Senioren und die Energieversorgung.

Zuvor muss die Bevölkerung cyber-physikalische Systeme allerdings zunächst akzeptieren. Dazu müssen die Systeme stets verlässlich funktionieren. Sie sollten nicht nur funktionieren, wie Anwender und Ingenieure es erwarten, sondern niemals ausfallen, immer verfügbar sein. Selbst wenn Komponenten durch Schäden und Unfälle ausfallen, müssen die Folgen minimal bleiben. Und dies muss bereits beim Entwurf dieser Systeme sichergestellt werden. Hier kommt Rupak Majumdar ins Spiel.

Die Treppe, eine Kombination aus hellem Holzparkett, Metall und Beton, knarrt, als er zu seinem Büro im dritten Stock des Max-Planck-Instituts für Softwaresysteme in Kaiserslautern hochsteigt. Das Gebäude riecht noch immer wie neu – erst im Juli des vergangenen Jahres haben die Forscher es bezogen. Sechs Etagen umgeben mit Büros, Besprechungs- und Aufenthaltsräumen ein Atrium von quadratischem Grundriss. Mit seinem zweiten Standort in Saarbrücken ist das Institut, neben dem Max-Planck-Institut für Informatik, das zweite innerhalb der Max-Planck-Gesellschaft, das sich ausschließlich der Informatik widmet. An ihm erforschen die Wissenschaftler alle Arten von Strukturen und

Verknüpfungen von Softwaresystemen. Majumdar entwickelt hier mit seiner Gruppe Methoden, mit denen sich die Betriebssicherheit von CPS automatisch überprüfen lässt.

HOHE ANFORDERUNGEN AN DIE ZUVERLÄSSIGKEIT

„Klar sollte das System nie ausfallen“, erklärt er, während er von seinem Büro zur Besprechung mit seiner Gruppe geht. Bisher hätte man die Software zur Not noch einmal starten können. „Aber die Anforderungen sind natürlich viel höher, wenn man das Steuerungssystem für ein Stromnetz entwirft“, sagt Majumdar und fügt hinzu: „Wenn bestimmte Funktionen nicht in einer klar definierten Zeitspanne das richtige Ergebnis liefern, kann das zu hohen Kosten, im schlimmsten Falle zu einer Katastrophe führen.“ Die Zuverlässigkeit sicherzustellen ist schon bei eingebetteten Systemen schwierig. Bei cyber-physikalischen Systemen kommt noch eine weitere Schwierigkeit hinzu. Deren Komponenten arbeiten sowohl in der analog-realen als auch in der digitalen Welt. Dies muss auch bei der Modellierung beachtet werden.

Zuverlässigkeit ist in der digitalen Welt als „Robustheit“ definiert. Informatiker verstehen darunter, dass ein

System trotz Störungen auf zufriedenstellende Art und Weise weiterarbeitet. In der realen Welt, beschrieben durch Regelungssysteme und Differentialgleichungen, versteht man darunter die „Eingangs-Ausgangs-Stabilität“. Am Beispiel einer Schraubenfeder, an deren Ende ein Gewicht hängt, erklärt, heißt das: Egal, wie sehr man das Gewicht nach unten zieht, beim Loslassen wird das Federpendel nicht weiter ausschlagen, als das Gewicht gezogen wurde. Die Schwerkraft lässt die Schwingung abklingen. Die Eigenschaft, dass das begrenzte Eingangssignal, das Ziehen an der Feder, im System des Federpendels auch ein begrenztes Ausgangssignal, nämlich die Schwingung des Federpendels, hervorruft, bezeichnet man als Eingangs-Ausgangs-Stabilität.

KOPFZERBRECHEN WEGEN DER MENSCHLICHEN FAKTOREN

Robustheit oder Eingangs-Ausgangs-Stabilität lassen sich nur in ihrem Bereich anwenden. Sie für „hybride“ Systeme wie cyber-physikalische Systeme auszudrücken und zu berechnen ist daher nicht möglich. Doch gerade deren Zuverlässigkeit prüfen zu können ist ausgesprochen wichtig, etwa um die stete Stromversorgung aus Sonnen- und Windenergie zu gewährleisten. Majumdar hat dazu einen wichtigen Beitrag geleistet. Er hat die Definition

von Eingangs-Ausgangs-Stabilität aus der Welt von realen Reglern so erweitert, dass mit ihr nun auch in der Welt von Bits und Bytes gearbeitet werden kann. Ein wichtiges Puzzlestück, um auch Aussagen über die Zuverlässigkeit von cyber-physikalischen Systemen machen zu können.

Doch nicht nur unterschiedliche Ansätze bei der Modellierung aus der Regelungs- und Softwaretechnik, auch menschliche Faktoren bereiten Majumdar Kopfzerbrechen. Er nennt es die „semantische Lücke“: Bei der Entwicklung eines Regelungssystems kommen verschiedene Spezialisten zum Einsatz. Diese behandeln jedoch nur ihre Abstraktionsebene, was wiederum zu Fehlern im Gesamtsystem führen kann. Majumdar will daher durch eine integrierte Programmanalyse alle Eigenschaften eines solchen Systems überprüfen.

Majumdars Gruppe hat sich im Raum versammelt, der einen weiten Blick über den Campus der Technischen Universität Kaiserslautern bietet. Sie sitzen auf blauen Stühlen an weißen Tischen und schauen auf eine Forscherin, die bereits am Whiteboard steht. Rayna Dimitrova hat ihren Doktor in Saarbrücken gemacht, und jetzt forscht sie in Kaiserslautern. Sie trägt blaue Jeanshosen und einen weißen Fleecepulli. Schnell füllt sie beide Tafeln mit Pfeilen, lateinischen und griechischen Buchstaben, runden und ge-

schwungenen Klammern. Wenn sie etwas erklärt, drückt sie mit ihrer rechten Hand die Kappe des dicken Filzstiftes auf und zu.

SCHRITT FÜR SCHRITT ZUR BESTEN ABSTRAKTION

Dimitrova beschäftigt sich mit der Verfeinerung von Abstraktionen. „Das ist das Spiel“, erklärt Majumdar: „Wir werfen bestimmte Informationen weg, stellen aber sicher, dass wir noch genug Informationen für die Analyse haben.“ Dieser Ansatz ist auch für das Überprüfen der Systemmodelle geeignet. Bisherige Verfahren haben einen entscheidenden Nachteil: Will man alles genau modellieren, wird die Menge der möglichen Zustände, die ein solches System einnehmen könnte, so groß, dass zu viele Computer zu lange an dem Modell herumrechnen. Wenn dies überhaupt noch möglich ist.

Majumdar und andere Forscher haben den Ansatz zum „Counterexample-Guided Abstraction Refinement“ weiterentwickelt. Man startet dabei mit einer sehr grobkörnigen Abstraktion. Anstatt alles zu modellieren, tut man dies nur so grob wie möglich. Findet das Rechenverfahren einen Fehlerkandidaten, wird dieser als Ausgangspunkt benutzt, um das Modell an dieser Stelle genauer zu beschreiben. Das macht man so lange, bis die Analyse keinen

Flugzeuge und Züge – aber auch moderne Autos – enthalten heute so viele vernetzte physikalische Sensoren und Aktoren, die in der physikalischen Welt wirken, dass sie komplexe cyber-physikalische Systeme darstellen.



Fotos: fotolia (links), istockphoto (rechts)



Beweise der Zuverlässigkeit: Filip Niksic, Johannes Kloos, Wei Li, Rupak Majumdar und Rayna Dimitrova entwickeln Methoden, um zu garantieren, dass cyber-physikalische Systeme fehlerlos arbeiten. Zu dem Zweck stellen sie Modelle der Systeme auf und suchen etwa nach sinnvollen Abstraktionen, um die mathematische Komplexität zu reduzieren.

Fehlerkandidaten mehr findet. Auf diese Weise erarbeiten sich die Forscher Schritt für Schritt die beste Abstraktion. Mit deren Hilfe können die Forscher letztlich mathematisch beweisen, dass das System als Ganzes korrekt arbeitet.

Nach dem Vortrag sitzt Majumdar in seinem Büro und geht seine E-Mails durch, die Füße wippen unter dem Tisch im Takt der Tasten. Ein Dinosaurier, ausgemalt mit allen möglichen Buntstiftfarben, hängt an der Schranktür und bildet damit einen starken Kontrast zum Whiteboard. Das haben zu viele Formeln in roter, blauer und schwarzer Farbe in eine graue Fläche verwandelt. In der linken oberen Ecke steht die To-do-Liste. Die ersten zehn Aufgaben sind in großer schwarzer Schrift notiert, danach sind die Buchstaben rot und klein. „Wir machen Fortschritte, aber viele Fragen sind noch unbeantwortet“, erklärt Majumdar. Wie kann man prüfen und bescheinigen, dass die Systeme selbst bei böswilligen Angriffen funktionieren? Wie sicherstellen, dass sie die Daten ihrer Nutzer

schützen? Und wie kann man dafür sorgen, dass ihre Handhabung selbst Laien keine Schwierigkeiten bereitet?

Es ist schon lange dunkel, als er in seinen zehn Jahre alten Mercedes-Benz

steigt und nach Hause fährt. Eins ist sicher: Wenn sich die cyber-physikalischen Systeme entwickeln wie erhofft, muss er sich um die Sicherheit auf seinem Heimweg weitaus weniger Sorgen machen. ◀

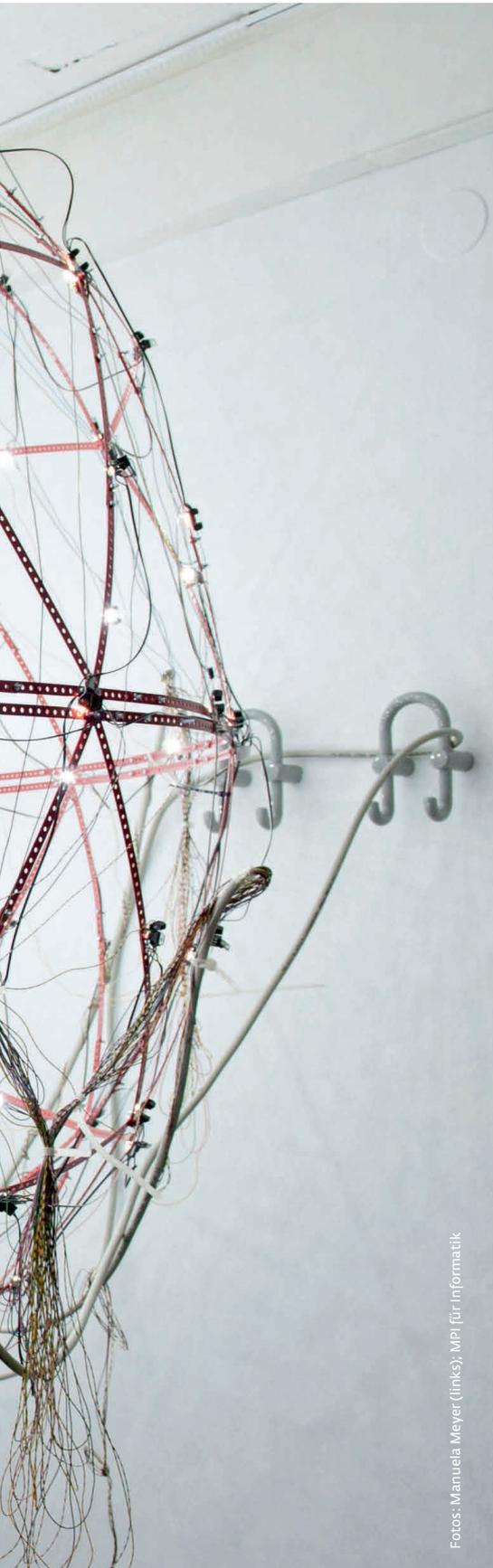
AUF DEN PUNKT GEBRACHT

- Cyber-physikalische Systeme können den Straßenverkehr sicherer machen, bei der Logistik für mehr Effizienz sorgen oder in einem Elektrizitätsnetz mit schwankendem Stromangebot eine kontinuierliche Versorgung sichern.
- Zuverlässigkeit wird in der Informatik mit Modellen untersucht, die nicht kompatibel sind mit den Modellen aus der physikalischen Welt. Um zu garantieren, dass ein hybrides, also in beiden Welten verankertes System zuverlässig funktioniert, ist ein umfassendes Modell nötig.
- Max-Planck-Forscher entwickeln Methoden, welche die Zuverlässigkeit von cyber-physikalischen Systemen sicherstellen. Um deren hohe Komplexität beherrschen zu können, suchen die Wissenschaftler nach sinnvollen Abstraktionen. Diese helfen ihnen, letztlich die Zuverlässigkeit des gesamten Systems zu gewährleisten.

GLOSSAR

Cyber-physikalische Systeme: Systeme, in denen Sensoren für Prozesse in der physikalischen, also der realen Welt, digitale Steuereinheiten und Aktoren in der physikalischen Welt miteinander vernetzt sind. Sie nutzen physikalische Informationen, um mit entsprechender Software digitale Steuerbefehle für Geräte zu erzeugen, die wiederum in der physikalischen Welt wirken.





Fotos: Manuela Meyer (links), MPI für Informatik

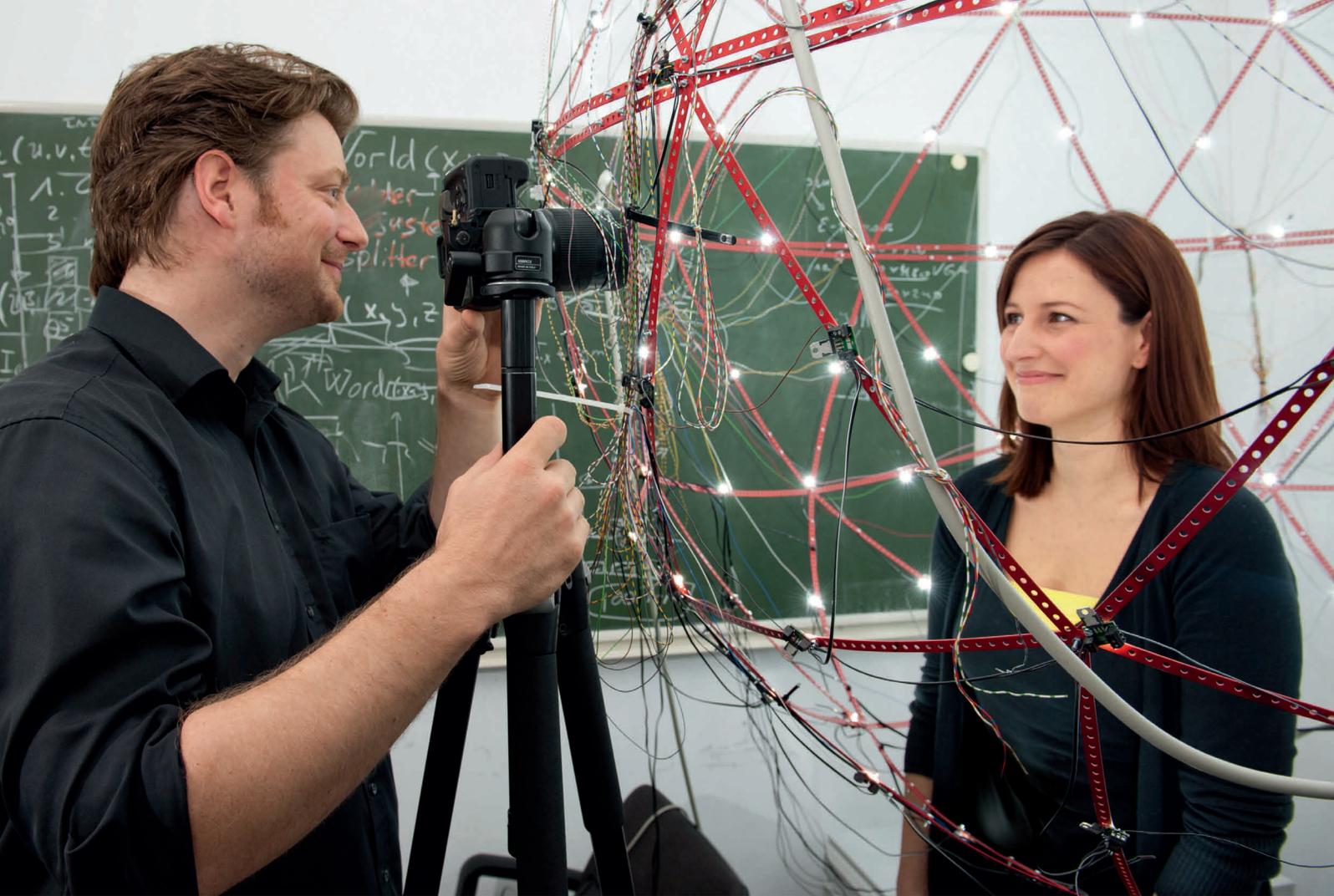
Bilder nehmen Formen an

Menschen reicht ein zweidimensionales Foto oder ein Film, um ein Gesicht oder einen Körper auch in 3-D zu erfassen. Diese Fähigkeit bringen Forscher um **Thorsten Thormählen** am **Max-Planck-Institut für Informatik** in Saarbrücken Computern bei und schaffen so neue Möglichkeiten, Bilder und Filme zu bearbeiten. Auch Anwendungen gibt es schon: einen 3-D-Schminkratgeber und ein Programm, mit dem sich menschliche Körper in Filmen manipulieren lassen.

TEXT **TIM SCHRÖDER**



Die Lichtkugel (links) hilft bei der Entwicklung des Programms zur Gesichtserkennung. Mit ihrer Hilfe erzeugen die Saarbrücker Forscher unterschiedlich beleuchtete Bilder, um die dreidimensionale Struktur zu analysieren.



In den vergangenen Monaten sah es in Thorsten Thormählen's Labor recht weihnachtlich aus. Eine gewaltige Leuchtkugel hing von der Decke herab. Thormählen hatte mit seinen Kollegen Lochstreifen aus einem Metallbaukasten zu einem runden Skelett zusammenschraubt und dann mehrere Dutzend Leuchtdioden daran montiert und verkabelt. Gut zwei Meter im Durchmesser misst die Lichtkugel, die der Forscher braucht, um Gesichter zu fotografieren.

Thorsten Thormählen und seine Mitarbeiter am Saarbrücker Max-Planck-Institut für Informatik arbeiten im Grenzbereich zwischen Realität und Computerwelt. Sie verpflanzen Bilder realer dreidimensionaler Objekte in virtuelle Szenen oder manipulieren die Körper von Filmstars in Videosequenzen.

Was beinahe nach Datenfälschung klingt, ist echte Grundlagenforschung. Denn die Saarbrücker wollen nicht weniger, als dem Computer beibringen, Szenen zu verstehen. Ein Mensch erkennt in einem Video intuitiv einen anderen Menschen. Füttert man aber

Fotosession für die Wissenschaft: Thorsten Thormählen nimmt zu Testzwecken seine Kollegin Kristina Scherbaum auf. Anhand solcher Bilder ermitteln die Forscher ein Standard-Gesicht und legen eine Bibliothek verschiedener Typen an.

einen Computer mit einer Bildsequenz, sieht der nur eine Wolke bunter Pixel. „Wir wollen, dass der Computer aus einer zweidimensionalen Szene reale, dreidimensionale Objekte herausliest“, sagt Thormählen, ganz im Geiste seiner Arbeitsgruppe „Bildbasierte 3-D-Szenenanalyse“. Auch das ist für uns Menschen kinderleicht. Selbst auf einem zweidimensionalen Foto erkennen wir, ob ein Haus oder ein Auto im Vordergrund steht. Den Computer derart schlau zu machen, dazu gehört allerhand.

ZWEIDIMENSIONALE BILDER LIEFERN 3-D-INFORMATIONEN

Zum Beispiel eine große Leuchtkugel. Damit treiben die Forscher eine Idee weiter, die Kristina Scherbaum und ihr Mentor Volker Blanz vor einigen Jahren umgesetzt haben. Ihnen war es gelungen, aus einem gewöhnlichen Foto ein dreidimensionales Abbild des Gesichts

zu rekonstruieren. Die virtuellen, dreidimensionalen Gesichter verschönern Thormählen, Scherbaum und ihre Kollegen nun, indem sie dazu das passende Make-up kreieren.

„Es funktioniert“, sagt Thormählen. „Auf der CeBIT haben wir Frauen fotografiert und unsere neu entwickelte Software das jeweils passende Make-up errechnen lassen. Es wird auf einem dreidimensionalen Abbild des Gesichts dargestellt.“ Die ideale Schminkvorlage in 3-D? Das klingt fast trivial. Tatsächlich aber bewegt sich Thormählen mit dieser Software an den Leistungsgrenzen der Computergrafik – und sie wird zum Testfall dafür, ob der Computer aus einem zweidimensionalen Bild korrekte 3-D-Information ermitteln kann. Doch wozu die Lichtkugel?

Sie ist das entscheidende Hilfsmittel, um Gesichter unter verschiedenen Belichtungen im Detail zu fotografieren. Will man dem Computer beibrin-

»» Das große Ziel der Grafiker ist ein Kunstkopf, den man nicht mehr vom echten unterscheiden kann. Für Videospiele, Kinofilme oder Internet-Anwendungen wäre er gleichermaßen attraktiv.

gen, zweidimensionale Fotogesichter in 3-D-Modellköpfe zu verwandeln, muss man ihn vorher nämlich mit 3-D-Gesichtsdaten trainieren. Zu diesem Zweck hatten die Forscher am Anfang des Projekts nacheinander 56 Frauen in der Kugel Platz nehmen lassen und aus verschiedenen Winkeln und unter unterschiedlichen Beleuchtungsbedingungen aufgenommen. So wurden den Probandinnen in der Lichtkugel Streifenmuster aufs Gesicht projiziert, die die Wölbungen von Nase, Wange oder Kinn anzeigen.

MATHEMATISCHE FORMELN FÜR DETAILS IM GESICHT

Dann kam die bewährte Software von Scherbaum und Blanz zum Einsatz, die 3-D-Köpfe erzeugt. Diese Software sammelte die Informationen aller 56 Gesichter und ermittelte daraus einen Standardkopf, einen digitalen Gesichtsröhling sozusagen, einen Datensatz, mit dem der Computer später in einem Bild treffsicher ein Gesicht als solches erkennt.

Speist man anschließend die zweidimensionale Fotografie eines neuen Gesichts in das System, wird das Porträt anhand des Standards vermessen und in ein 3-D-Gesichtsmodell gewandelt, gemorphet, wie Spezialisten es nennen. Das Programm beschreibt das neue Gesicht also anhand des gespeicherten Wissens – eine Nase wie Gesicht 25, Wangenknochen wie Gesicht 34, ein Kinn wie Gesicht 56.



Schminkratschläge aus dem PC: Das Programm erzeugt zunächst ein realistisches Bild eines Gesichts (links) und empfiehlt dann ein Make-up (Mitte). Zum Vergleich das Gesicht mit unvoreilhaftem Make-up (rechts).

Die Software vollzieht dabei einen Optimierungsprozess. Sie erzeugt ein 3-D-Abbild des Gesichts, rechnet dann zurück nach 2-D, gleicht die Daten mit der Fotovorlage ab und verbessert im Zweifelsfalle das 3-D-Abbild erneut. Bis schließlich alles passt. Eine Schwierigkeit dieses Prozesses liegt darin, die zahllosen Details, die Menschen auf einen Blick erfassen, in eine mathematische Beschreibung zu fassen. Denn nur anhand von Formeln kann der Rechner ein neues Gesicht mit den gespeicherten Mustern abgleichen.

Nicht nur die exakte dreidimensionale Form eines Gesichts finden die Forscher auf diese Weise heraus, sie bestimmen auch die Eigenschaften der Haut. Diese Details kann der Computer anhand der Reflexion auf der Oberfläche für jedes Pixel exakt berechnen, da die Position der Leuchtdioden im Lichtzelt genau bekannt ist. Sogar die Lage und Tiefe einzelner Hautporen ermittelt der Computer. So entsteht im Computer ein sehr lebensechtes „Hautmodell“.

Natürlich ist das etwas viel Aufwand für einen schnöden Schminkratgeber. Tatsächlich geht es Thormählen um mehr. Er versucht, dem lebensechten Abbild des Menschen so nah wie möglich zu kommen – und folgt damit einem Trend in der Computergrafik. Das gro-

DAS ZIEL: EIN LEBENSECHTES ABBILD DES MENSCHEN

DAS ZIEL: EIN LEBENSECHTES ABBILD DES MENSCHEN

Um ein lebensechtes Modell eines Gesichts zu erzeugen, werden verschiedene Informationen gespeichert (von links): Diffuser Anteil des reflektierten Lichts, Normalenrichtung auf der Oberfläche (farbcodiert), 3-D-Position der Oberfläche (farbcodiert), Stärke des gerichteten Anteils des reflektierten Lichts, Stärke des Glanzes und Stärke der Volumenstreuung.



Um ein lebensechtes Modell eines Gesichts zu erzeugen, werden verschiedene Informationen gespeichert (von links): Diffuser Anteil des reflektierten Lichts, Normalenrichtung auf der Oberfläche (farbcodiert), 3-D-Position der Oberfläche (farbcodiert), Stärke des gerichteten Anteils des reflektierten Lichts, Stärke des Glanzes und Stärke der Volumenstreuung.

ße Ziel der Grafiker ist ein Kunstkopf, den man nicht mehr vom echten unterscheiden kann. Für Videospiele, Kinofilme oder Internet-Anwendungen wäre der gleichermaßen attraktiv.

Dabei kommt es auf Nuancen an, vor allem das Zusammenspiel von Licht

und Gesichtsoberfläche. Denn Menschen sind unerhört gut darin, echte von falschen Gesichtern zu unterscheiden. Eine falsche Reflexion in der Iris, und schon wirkt ein digitaler Android abstoßend künstlich. Auch das Lichtspiel der Haut ist wichtig. Ein Gesicht

reflektiert das Licht nicht wie ein Spiegel. Bestimmte Teile werden gestreut und diffus zurückgeworfen. Hinzu kommt das Licht, das in die Haut eindringt und von den tieferen Hautschichten reflektiert wird. Es verleiht dem Gesicht den typischen warmen, lebensechten Charakter. Ein Grund dafür, dass zu dick aufgetragene Schminke unecht wirkt.

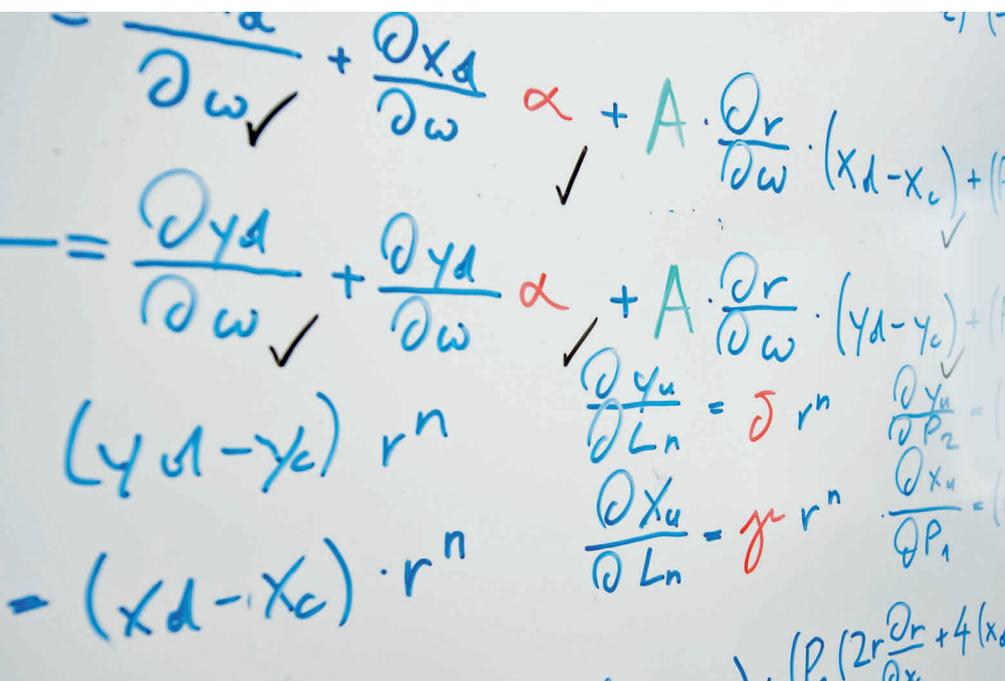
Thormählen versucht, dem naturgetreuen Kunstkopf mit seinem Make-up-Modell möglichst nahe zu kommen. Für den Hightech-Schminkassistenten in 3-D muss der Rechner natürlich zusätzlich mit Make-up-Information gespeist werden. Thormählen und Scherbaum fotografierten die Probandinnen daher einmal ungeschminkt und einmal geschminkt. Dafür engagierten sie eigens eine professionelle Kosmetikerin aus einem Saarbrücker Theater, die die Frauen je nach Typ optimal schminkte.

DER COMPUTER BEANTWORTET DIE TYP-FRAGE

Das umfangreiche Wissen der Kosmetikerin, welches Make-up zu welchem Typ, also zu welchem Teint, welcher Augen- und Haarfarbe passt, müssen die Saarbrücker Informatiker nun wieder in Daten fassen. Diese kommen zu den Datenbergen des Morphable Face Models, des veränderbaren Gesichtsmodells, und den Hautinformationen aus der Lichtkugel dazu. All diese Informationen müssen die Forscher nun zusammenführen, und zwar nicht intuitiv, wie Menschen das können, sondern in der analytischen Formelsprache, die Computer verstehen.

Scannt man jetzt ein Foto, generiert der Computer ein 3-D-Gesichtsmodell, das er mit den bekannten Gesichtern in der Datenbank abgleicht: Ein heller Typ? Da wären etwas weniger Rouge und ein wenig mehr Lid-

Kristina Scherbaum und Thorsten Thormählen diskutieren neue Ideen. Hund Filou passt auf, dass keiner einen Zettel mit neuesten Forschungsansätzen klaut, und kann außerdem verschiedene Kunststücke vorführen.

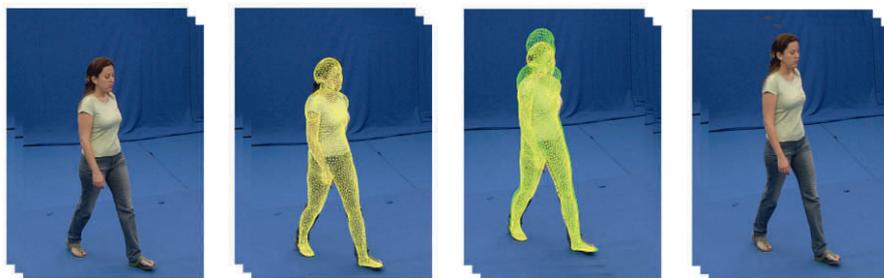
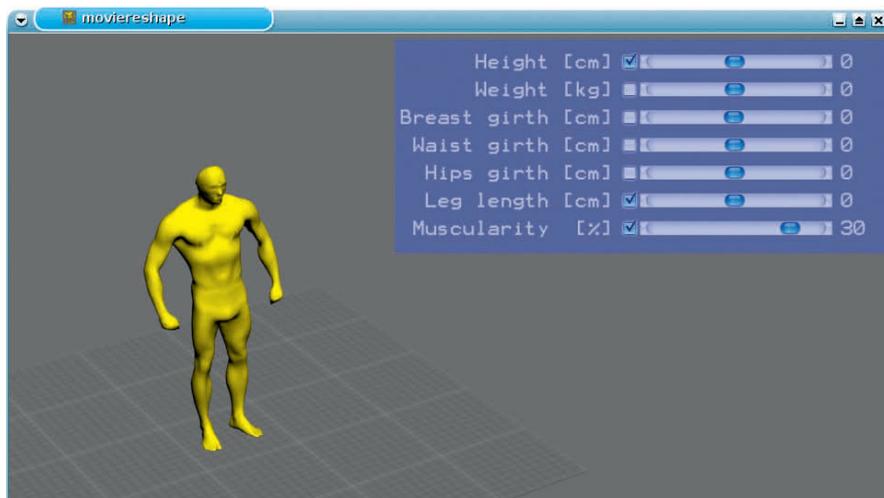


schatten geeignet. Am Ende liefert die Software das Make-up, das am besten zu dem neuen Gesicht passt. Das Kunstgesicht lässt sich drehen und neigen und unter verschiedenen Belichtungen betrachten – im Sonnenschein oder im schummrigen Diskolicht. Und dank der hochaufgelösten Fotos aus der Lichtkugel haben die Gesichter eine täuschend echte Anmutung.

REALE HAUTMODELLE FÜR COMPUTERSPIELE

Ursprünglich wollte Thormählens Team eine Software entwickeln, die Frauen ein Make-up vorschlägt, mit dem ihr Gesicht dem theoretischen Schönheitsideal nahe kommt. Nach Erkenntnissen von Psychologen zeichnet sich ein solches Ideal unter anderem durch braunere Haut, vollere Lippen, dünnere Augenlider, lange dunkle Wimpern, höhere Wangenknochen und eine schmale Nase aus. Mit ausreichend Schminke könnte man Gesichter tatsächlich in diese Richtung trimmen. Am Ende erschien es den Forschern aber sinnvoller, das individuelle Optimum und nicht den idealen Standard zu suchen.

Mit dem Make-up-System verknüpfen die Informatiker Highlights der Computergrafik. Ausgereifte Morphable Models und reale Hautmodelle sind dabei Errungenschaften der vergangenen fünf Jahre, für die es eine ganze Reihe potenzieller Einsatzgebiete gibt: Internetservices zum Beispiel, in denen naturgetreue, virtuelle Mitarbeiter sprechen, Tipps geben oder bei der Bedienung von Geräten helfen. Und dann wäre da der wachsende Markt der Computerspiele-Industrie. Nach Angaben des Bundesverbands Interaktive Unterhaltungssoftware und der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers expandiert die Branche enorm. So spülte der Verkauf von Computerspielen 2008 weltweit gut 50 Milliarden US-Dollar in die Kassen der Spiele-Industrie. Damit hat der Spielmarkt längst das Geschäft mit Spielfilm-DVDs und Blu-rays überflügelt. Mit diesen wurden im selben Jahr nur knapp 35 Milliarden US-Dollar umgesetzt.



Virtuelles Bodyshaping: Das 3-D-Modell eines Körpers lässt sich beliebig verformen – der Mann oben hat besonders kräftige Muskeln verpasst bekommen. Da das Modell gemäß den natürlichen Proportionen manipuliert wird, erscheint ein Körper auch in der Bewegung natürlich (unten).

Je realistischer die künstlichen Gestalten und die virtuellen Welten wirken, desto attraktiver sind sie – und desto mehr Geld sind die Kunden bereit auszugeben. Lebenschte Gesichter spielen dabei eine wichtige Rolle. Die Bewegung der Figuren aber auch. Was das betrifft, hat Thormählen im vergangenen Jahr einen Coup gelandet. Es gelang ihm mit der neuen Software MovieReshape, in einem realen Video die Gestalt der Protagonisten zu verändern.

VIRTUELLE PFUNDE FÜR HOLLYWOODSTARS

Talentierte Computergrafiker konnten so etwas bislang nur mit Fotos machen, sie retuschieren zum Beispiel den Bauchansatz von Politikern oder Fältchen von Fernsehstars weg. Für Filme mit 25 Bildern pro Sekunde war das undenkbar.

Mit der neuen Software aber lassen sich Menschen im Film spielend leicht modifizieren. Es genügt, kleine Schieberegler auf dem Bildschirm hin- und herzubewegen, und schon schrumpft oder wächst der Darsteller.

Ein Produkt gibt es noch nicht. Aber der Prototyp der neuen Bildbearbeitungssoftware funktioniert überzeugend. Im Internet wurde das Demo-Video schon hunderttausendfach angeklickt: Ein männlicher „Baywatch“-Star joggt durch den Strandsand, mal mit flachem Brustmuskel, mal mit gewölbtem. In einem anderen Film wirft ein Sportler Basketbälle in den Korb, während ihm ein Bierbauch wächst.

„Jetzt sind nicht einmal mehr Videos vor Fälschern sicher“, schimpfen Kritiker. Thorsten Thormählen kennt die Bedenken. Für ihn aber ist die neue Software vor allem ein verlockendes

» Thorsten Thormählen hat im vergangenen Jahr einen Coup gelandet. Es gelang ihm mit der neuen Software MovieReshape, in einem realen Video die Gestalt der Protagonisten zu verändern.

Hilfsmittel, um professionelle Videoaufnahmen aufzupeppen. „Bislang futtert sich mancher Hollywoodstar für eine Filmrolle Pfunde an“, sagt Thormählen. „Mit unserer Software ließe sich das völlig stressfrei am Computer erledigen.“

DAS PROGRAMM LERNT KÖRPER ZU UNTERSCHIEDEN

Die Leichtigkeit, mit der der „Baywatch“-Adonis über den Strand läuft, täuscht darüber hinweg, dass die Entwicklung von MovieReshape harte, auch mathematische Arbeit war. Wie beim Kunstkopf musste zunächst ein digitales Modell geschaffen werden – in diesem Fall ein Morphable Body Model. Auch hier berechnet der Computer aus einer zweidimensionalen Szene ein realistisches, dreidimensionales Modell. Denn am Ende wirkt die Manipulation an einer Filmsequenz nur dann überzeugend, wenn sie einer realistischen Veränderung im dreidimensionalen Filmobjekt entsprechen könnte.

Für das dreidimensionale Modell haben die Forscher zunächst die Körper von etwa 100 Probanden eingescannt. Damit lernte der Computer, zwischen dick und dünn, lang und kurz, starkem oder schmalem Oberschenkel zu unterscheiden. Füttern die Forscher ihren Computer jetzt mit einer Videosequenz, passt das Programm das digitale Körpermodell automatisch an die Gestalt im Bild an – und zwar für jedes Einzelbild einer Filmsequenz. Bei einem flimmerfreien Video sind das die besagten 25 Bilder pro Sekunde. Eine solche automatische Bildanalyse dauert derzeit noch Stunden. Dann aber geht es schnell. Hat der Computer alle Bilder und die Position des Darstellers analysiert, genügt ein Zug am Schieberegler, und der Körper wächst oder schrumpft nach Gutdünken – und zwar konsistent in allen Bildern der Videosequenz.

Das klingt simpel. Der Trick aber besteht darin, den Körper anatomisch korrekt zu verformen. Es genügt nicht, Bauch und Beine in die Länge zu zie-

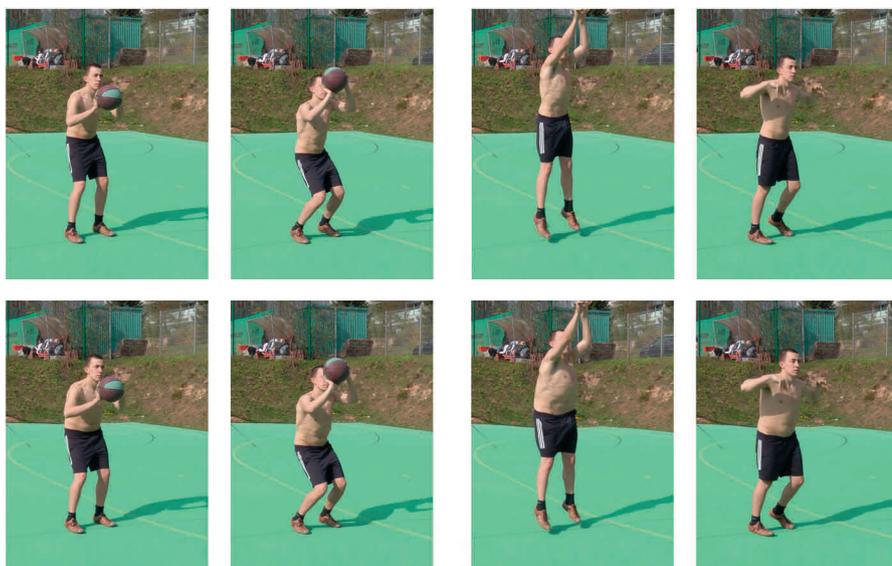
hen. Auch die Dicke der Gliedmaßen oder des Rumpfes muss sich ändern. Sonst wirkt die Figur schnell wie eine Karikatur. Das mathematisch formalisierte Wissen über die richtigen Proportionen zieht die Software aus den gespeicherten Körperscans.

Und noch etwas benötigt der Computer: das Wissen, wie sich ein Skelett anatomisch korrekt bewegt. Thormählen konnte dafür auf ein etabliertes Verfahren zurückgreifen, das schon länger von Informatikern genutzt wird. Bei diesem Verfahren wird ein Skelett verwendet, das definiert, welche Stellungen Knochen und welche Winkel Gelenke einnehmen können. Dieses künstliche Skelett hat Thormählen mit seinem Morphable Body Model gekoppelt. „Damit kann die Software in einer Bildfolge Beine und Arme anatomisch korrekt positionieren“, sagt er.

DAS 3-D-MODELL LÄSST CHARLIE CHAPLIN AUFERSTEHEN

Thormählen und seine Kollegen haben die Bearbeitung bewegter Bilder damit also quasi automatisiert. Das ist genau das, was die Computergrafik-Branche braucht. Gefragt sind Programme, die einen Computer mit Vorwissen über die Gestalt des Menschen füttern. Erst mit diesem Vorwissen und entsprechender Software kann der Computer die Gestalt dann halb automatisch oder künftig vielleicht sogar von ganz allein verändern. „Heute macht man noch viel von Hand, schiebt Pixel am Bildschirm mit der Maus hin und her, färbt Flächen ein und um“, sagt Thormählen. Programme, die diese zeitraubende Arbeit automatisieren, sind deshalb heiß begehrt.

Und mithilfe des dreidimensionalen Modells lassen sich nicht nur die Körper der Schauspieler an die Vorgaben des Drehbuchs oder auch nur an den Publikumsgeschmack anpassen, sie könnten auch helfen, Schauspieler



Zugelegt trotz Sport: Dem jungen Mann wächst beim Wurf auf den Basketballkorb ein Bauch.



Dreh für die Video-Modifikation: Kristina Scherbaum und Thorsten Thormählen nehmen im Video-Studio Bildfolgen für das MovieReshape-Verfahren auf. Mit dem einfarbigen Hintergrund ist es für die Software einfacher, das künstliche Skelett des digitalen Körpermodells an die aufgenommenen Bildfolgen anzupassen als mit realem Hintergrund.

zu animieren. Sehr weit gesponnen, ließen sich manche Dreharbeiten eines Tages vielleicht durch einen Fototermin ersetzen – in Bewegung würden Filmemacher ihre Akteure dann am Computer versetzen. So könnte man auch Charlie Chaplin wiederauferstehen lassen. Es genügte, Kopf und Körper aus alten Spielfilmsequenzen in den Computer einzuspielen. Damit könnte der Rechner Chaplin dann nach Belieben laufen und springen lassen. „Hier sind noch nicht alle Probleme gelöst, aber mit ein wenig Arbeit können wir das unserer Software beibringen“, sagt Thormählen. Im vergangenen Dezember hat er MovieReshape auf der Siggraph Asia, einer der weltweit wichtigsten Konferenzen in der Computergrafik, vorgestellt.

Auch für die Sportanalyse wäre die Software sinnvoll. So könnte man einem Sportler am eigenen Bild beispielsweise einen idealen Bewegungsablauf vorführen. Und im Fitnessstudio könnte man Motivationsvideos anbieten: „So werde

ich aussehen, wenn ich dreimal die Woche trainiere.“

Das nächste Ziel von Thormählens Team ist es, das Morphing noch schneller zu machen, weiter zu automatisieren; die Zeit zu verkürzen, die der Computer braucht, um die Videodaten zu analysieren. Und was die Gesichter betrifft, wünscht er sich noch mehr Leben. Die Haut wirkt schon echt. Jetzt soll eine überzeugende Bewegung, die

täuschend echte Mimik hinzukommen. Auch dafür sind neue, schnellere Algorithmen nötig. „Damit könnte ein Computersystem sogar Stimmungen erkennen“, sagt Thormählen. Denkbar sei es auch, den Computer mit Gesten oder Mimik zu steuern. Das würde nicht nur Computerspiel-Freaks erfreuen. Querschnittgelähmten könnte eine solche Funktion die Arbeit am Computer erleichtern. ◀

GLOSSAR

Morphable Body Model: Körpermodell, das sich in drei Dimensionen realistisch verformen und bewegen lässt. Es dient als Vorlage für Manipulationen in zweidimensionalen Filmsequenzen. Analog zum 3-D-Gesichtsmodell wird es von einer Software erzeugt, die Körper aus beliebigen zweidimensionalen Filmsequenzen mit einem Katalog gescannter Körperformen und -gesten abgleicht.

Morphable Face Model: Wörtlich: Formbares Gesichtsmodell. Dreidimensionales Modell eines Gesichts, das Manipulationen zulässt. Eine Software erstellt es von einer beliebigen Person, indem sie das Gesicht mit einem Katalog vorhandener Gesichter abgleicht.

MovieReshape

Ermöglicht die schnelle und einfache Manipulation der Körperformen und -proportionen von Darstellern in Filmen. Die Software arbeitet mit einem 3-D-Körpermodell (siehe oben).

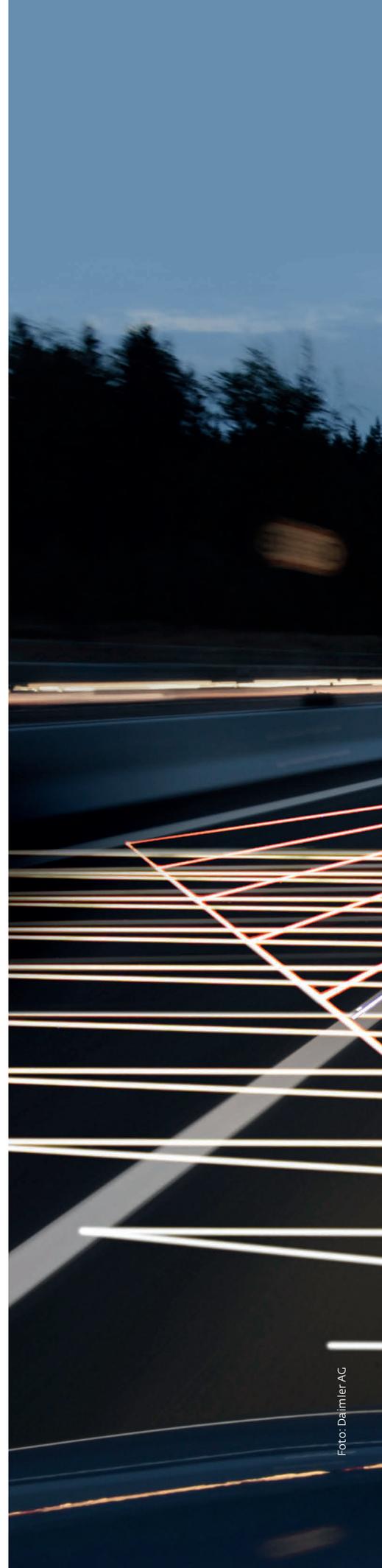
Bordcomputer mit 7. Sinn

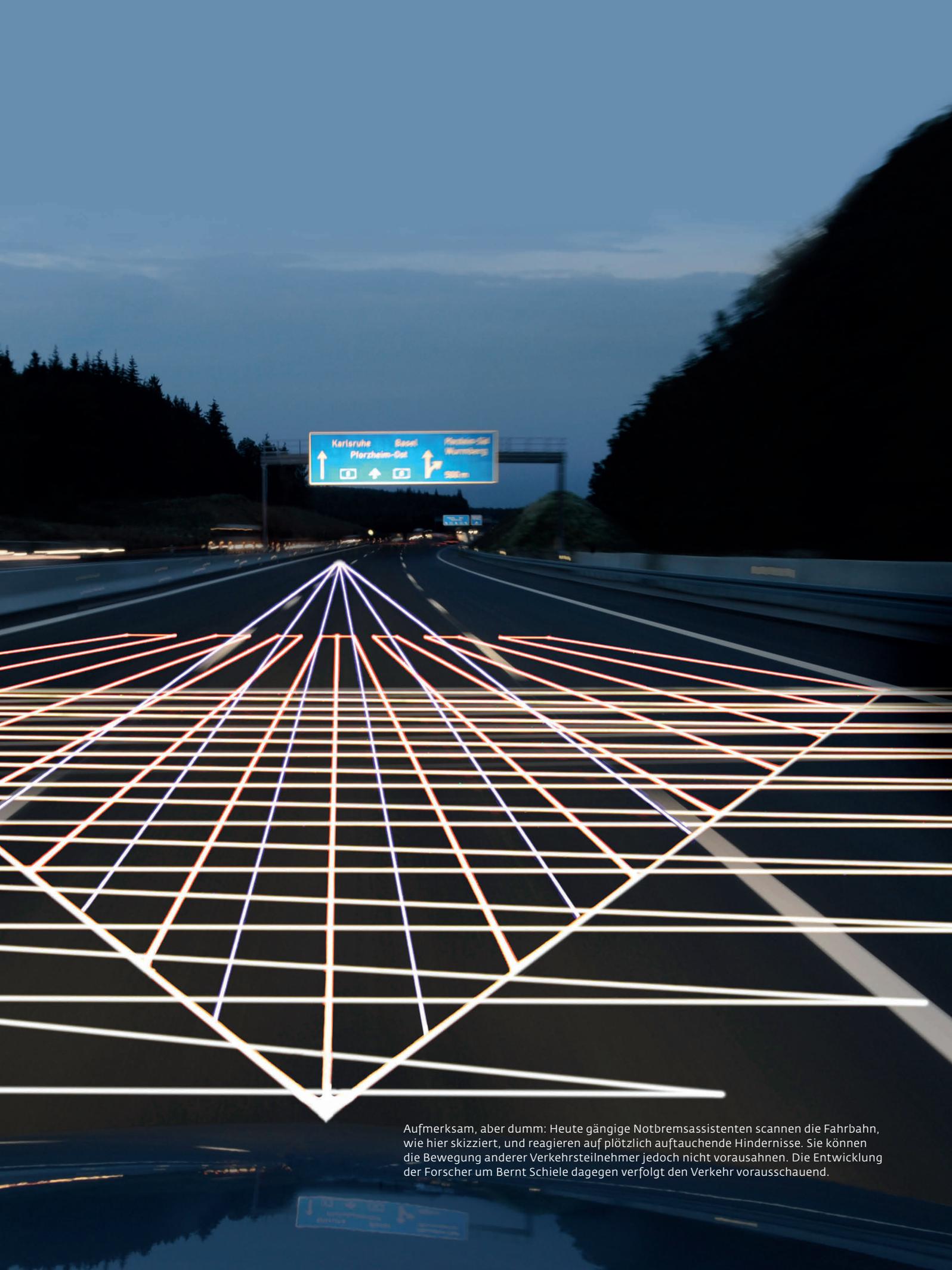
Notbremssysteme verhindern heute schon manchen Unfall im Verkehr, einen richtigen Überblick über das Geschehen auf der Straße haben elektronische Assistenten aber noch nicht. Das will **Bernt Schiele**, Direktor am **Max-Planck-Institut für Informatik** in Saarbrücken ändern. Er bringt Computern bei, die Wege von Fahrzeugen und Fußgängern vorauszuahnen.

TEXT **TIM SCHRÖDER**

Sie heißen Forward Alert, Pre-Safe oder PreSense und finden sich vor allem an Bord teurer Autos. Bei den Systemen mit den kernigen englischen Namen handelt es sich um sogenannte Notbremsassistenten. Läuft plötzlich ein Kind auf die Straße oder braust bei Rotlicht ein Raser über die Kreuzung, dann geht der Assistent von allein in die Bremsen – selbst wenn der Fahrer noch starr vor Schreck ist. Mit kleinen Infrarotkameras oder Radarsensoren tasten diese Systeme die Straßenszene vor dem Auto ab. Objekte auf Kollisionskurs erfasst der Notbremsassistent in Sekundenbruchteilen, zum Beispiel einen Fußgänger, der gedankenverloren auf die Straße tritt. In Millisekunden analysiert der Mikroprozessor die Lage: Wie schnell ist das Objekt? Kommt es zum Zusammenstoß? Achtung. Stopp!

Die Fahrzeughersteller betonen, dass die Notbremsassistenten allein in Europa jedes Jahr Tausende von Unfällen verhindern. Die Technik funktioniert und ist in Schrecksekunden schneller als der Fahrer. Doch ist sie auch heute noch vergleichsweise dumm. Notbremsassistenten und vergleichbare Sensorensysteme im Auto können nur auf die letzte Sekunde reagieren. Sie konzentrieren sich voll auf ein herannahendes Objekt – mehr aber nicht. Ein ausgeruhter Autofahrer hingegen hat die ganze Szene im Blick. Den Rettungswagen, der sich von weit rechts nähert zum Beispiel, oder ein flottes Auto, das an einer mehrspurigen Kreuzung kurz von einem Lkw verdeckt ist und dann über die Kreuzung saust. Kurz: Notbremsassistenten können im letzten Moment einschreiten, aber nicht vorausschauend fahren. >





Aufmerksam, aber dumm: Heute gängige Notbremsassistenten scannen die Fahrbahn, wie hier skizziert, und reagieren auf plötzlich auftauchende Hindernisse. Sie können die Bewegung anderer Verkehrsteilnehmer jedoch nicht voraussagen. Die Entwicklung der Forscher um Bernt Schiele dagegen verfolgt den Verkehr vorausschauend.

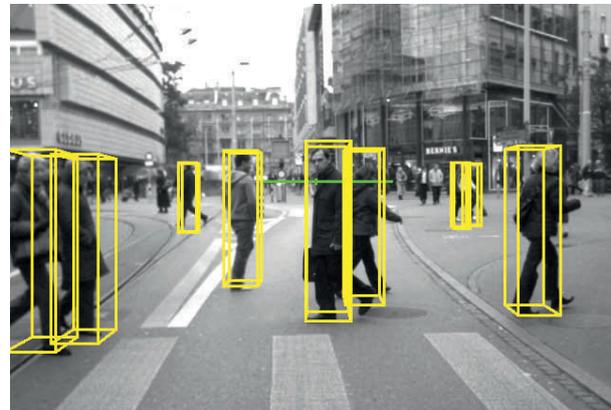


Das Gleiche gilt für andere Automaten, für Assistenzroboter zum Beispiel. Sie sind heute durchaus in der Lage, ein Tablett vom Küchentisch zu nehmen und an Hindernissen vorbei ins Wohnzimmer zu tragen. Eine komplexe Szene, in der der Hund durch die Küche springt und Kinder vor den Schränken toben, bringt die blechernen Helfer aber noch völlig aus dem Konzept. Das Ziel der Forscher ist es, ihren Maschinen beizubringen, ganze Szenen zu erfassen und vor allem Bezüge zwischen den Objekten herzustellen. Bremst ein Auto, dann bremst auch das nachfolgende. Eine so simple Logik beherrschen die modernen Automaten meist nicht. Das ist ein Grund dafür, warum es bis heute keine Assistenzkameras für Blinde gibt. Zu komplex sind die Zusammenhänge. Fußgänger weichen einander aus, queren plötzlich den Weg. Und halb verdeckte Fußgänger oder Autos werden von Automaten regelmäßig übersehen.

EIN AUTO SOLL AUTONOM DURCH DEN VERKEHR NAVIGIEREN

Assistenzsysteme klüger zu machen, das ist das Ziel von Bernt Schiele, Direktor der Abteilung Computer Vision und Multimodal Computing am Max-Planck-Institut für Informatik in Saarbrücken. Er will Computern beibringen, eine Szene wie ein Mensch zu verstehen – und entsprechend zu handeln. Schieles Arbeitsgruppe hat raffinierte Rechenvorschriften entwickelt, die eine Straßenszene vollständig analysieren, alle Objekte erfassen, Fußgänger, Autos und Lkw, ganz gleich, ob diese gut zu sehen oder halb verdeckt sind. Wenn Schiele und seine Mitarbeiter dürften, wie sie wollen, dann würden sie ein Auto mit ihrer Software autonom durch den Verkehr navigieren lassen. In den Bildern einer Videokamera, die hinter der Windschutzscheibe montiert ist und den Verkehr beobachtet, können sie bereits gan-

Fußgänger von rechts: Die Software der Saarbrücker Informatiker analysiert die Szene. Sie erkennt die Fahrzeuge und den Passanten, verfolgt die Bewegung aller Verkehrsteilnehmer und berechnet, ob ein Zusammenprall droht. Bei Gefahr reagiert sie autonom.



Wie ein Computer unübersichtliche Verkehrssituationen versteht: Ein Classifier ermittelt, mit welcher Wahrscheinlichkeit es sich bei einer bestimmten Pixelwolke um einen Fußgänger handelt. Detektoren tragen die Ergebnisse in einer Art Landkarte (links) ein, in der die grünen Bereiche mit hoher Wahrscheinlichkeit Fußgänger darstellen. Die identifizierten Verkehrsteilnehmer rahmt die Software farbig ein (rechts), um sie zu verfolgen und ihre Bewegungen zu antizipieren.

ze Straßenszenen erfassen. „Autonomes Fahren wird kommen, ist aber natürlich – noch – nicht erlaubt“, sagt Schiele.

Szenen verstehen. Das klingt so simpel. Dank unserer Erfahrung erfassen wir Menschen die Situation an einer Kreuzung sofort. Ampel rot: Die Leute bleiben stehen. Ampel grün: Ich darf gehen. Uns ist es egal, wie viele Menschen hin und her eilen. Was ein Computer aus dem Bild einer Kamera herausliest, ist etwas gänzlich anderes. Er sieht Tausende von Bildpunkten, helle, dunkle, rote, grüne, und muss erst lernen, was diese überhaupt zu bedeuten haben.

Für die Szenenanalyse braucht man deshalb ein ganzes Bündel an ausgeklügelten Algorithmen, mit denen der Computer Stück für Stück analysiert, was Sache ist. Zunächst Algorithmen, die bestimmte Strukturen erkennen. Fußgänger sind länglich und haben eine bestimmte Höhe. Sie besitzen zwei Arme und zwei Beine. Autofronten sind flach, Lkw-Fronten hoch. In einem nächsten Schritt muss die Software herausfinden, ob und wohin sich die Objekte bewegen. Und drittens muss der Computer logische Schlüsse ziehen: Hält Auto eins an der Ampel, so tut das aller Voraussicht nach auch Auto zwei dahinter.

Grundlage all dieser Analysen ist die Wahrscheinlichkeitsrechnung. Mit Milliarden von Rechenoperationen pro Se-

kunde fragt das Programm ab, mit welcher Wahrscheinlichkeit ein Haufen Bildpunkte tatsächlich ein Gegenstand ist. „Probabilistische 3D-Szenenanalyse“ nennt Schiele diese komplexe Form des Computerverstehens. Bemerkenswert ist, dass Schiele für die dreidimensionale, also räumliche Analyse eine einzige Kamera benutzt. Menschen haben zwei Augen, um räumlich sehen zu können. „Wir berechnen die dreidimensionale Information aus dem zweidimensionalen Computerbild“, sagt Schiele.

DIE SOFTWARE LERNT, WIE AUTOS ODER FUSSGÄNGER AUSSEHEN

Doch zunächst mussten die Saarbrücker Forscher ihre Algorithmen anlernen: Sie fütterten den Computer mit Trainingsdaten – mit Hunderten Bildern von Fußgängern, Autos und Lkw. Die Software lernte damit nach und nach, wie ein Auto oder Fußgänger aussieht. „Classifier“ heißen diese Erkennungsprogramme, die in den Pixelwolken des Kamerabildes nach bestimmten Objekten forschen. Kanten von Objekten zum Beispiel detektieren sie anhand abrupter Veränderungen der Farbe oder der Helligkeit benachbarter Pixel. Am Ende werfen sie „Scores“ aus – Werte, die angeben, wie wahrscheinlich es ist, dass es sich bei einer bestimmten Pixelstruktur tatsächlich um ein Objekt handelt.

Für die komplexen Straßenszenen benötigt Schiele eine ganze Reihe verschiedener Classifier, zum Beispiel solche, die Umgebungsstrukturen wie eine Straße oder einen Baum erkennen, und solche, die im Pixeldurcheinander diskrete Objekte wie Autos, Lkw und Fußgänger erspähen. Dabei reichen Classifier, die nur ganze Objekte erkennen, nicht aus. Zum Einsatz kommen außerdem spezielle Classifier, die Schiele und seine Mitarbeiter mit Objektteilen trainiert haben: einem Arm, einem halben Rücken, einer Kühlerhaube. Denn nur so lassen sich später verdeckte Objekte sicher detektieren. Die Ergebnisse der Classifier, die Scores, werden von größeren Algorithmen, den Detektoren, ausgewertet. Die Detektoren erstellen für jedes einzelne Bild einer Videosequenz eine Art Landkarte, eine Score-Map, auf der für jedes Pixel verzeichnet ist, mit welcher Wahrscheinlichkeit es zu einem bestimmten Objekt gehört.

Um festzustellen, ob das Detektorergebnis plausibel ist, gleicht der Computer die Score-Map-Werte mit seinem Weltwissen ab. Anhand der Trainingsdaten hat er gelernt, wie eine Straße oder ein Auto aussieht. Hinzu kommt das dreidimensionale Wissen. Autos, die entgegenkommen, wirken umso kleiner, je weiter weg sie sind. Darüber hinaus befinden sich weiter entfernte Autos im Kamerabild weiter oben als

» Ein wesentlicher Unterschied zum klassischen Auto-Assistenzsystem liegt darin, dass die Software die Bewegung der Objekte permanent verfolgt.

nahe Autos. Gemäß erlerntem Weltwissen könnte beispielsweise ein großes Auto nicht am oberen Bildrand erscheinen. Eine Straßenlaterne wiederum ist kein Fußgänger, weil sie deutlich größer ist. So prüft der Computer für jedes Videokamerabild die Plausibilität seiner Analyse: Wie wahrscheinlich ist es, dass die Objekte in dieser Szene tatsächlich der realen Szene entsprechen?

So trainiert und mit Weltwissen ausgestattet, musste sich die Software einem Test stellen: Die Forscher spielten ihr reale Videosequenzen vor, die sie im fahrenden Auto aufgenommen hatten und in denen Fußgänger zu sehen sind,

die beispielsweise durch die Straßen von Zürich eilen. ETH-Loewenplatz, ETH-Linthescher oder ETH-PedCross2 heißen diese Bildfolgen, die Forscher von der ETH Zürich aufgenommen haben, an der Schiele einige Zeit verbracht hat.

DAS SYSTEM AHNT BEWEGUNGEN DER OBJEKTE VORAUSS

Dabei zeigte sich, dass die Classifier und Detektoren oftmals danebenlagen, wenn sie nacheinander jedes Bild einzeln auswerten. Vor allem verdeckte Objekte wurden häufig übersehen. Das änderte sich, wenn die Algorithmen etwa fünf

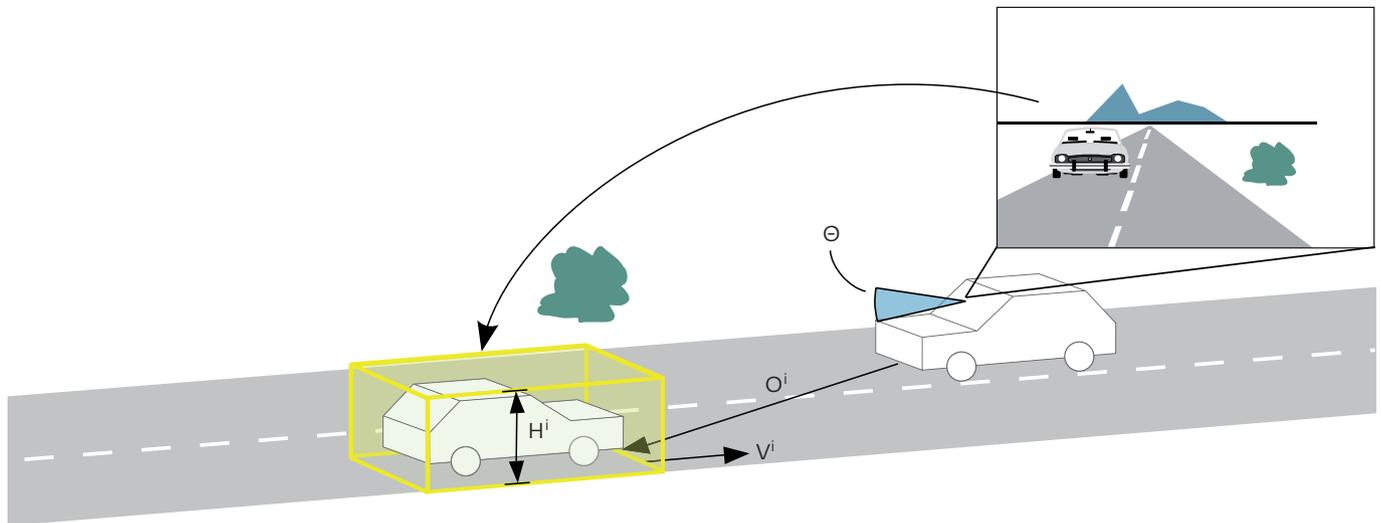
aufeinanderfolgende Bilder miteinander abglichen. Eine flimmerfreie Filmsequenz besteht aus mindestens 24 Bildern in der Sekunde. Bewegte Objekte verändern ihre Position wie in einem Daumenkino von Bild zu Bild minimal. Berücksichtigen die Algorithmen mehrere aufeinanderfolgende Bilder, erkennen sie vor allem die verdeckten Objekte besser. „Die Bilderkennung wurde sehr viel robuster“, sagt Schiele. „Tracklets“ nennt Schiele diese analytisch verschmolzenen kurzen Bildfolgen.

Ein wesentlicher Unterschied zum klassischen Auto-Assistenzsystem liegt darin, dass die Software die Bewegung der Objekte von Tracklet zu Tracklet permanent verfolgt. Notbremsassistenten nehmen Gefahren wahr, die blitzartig auftauchen. Bei Schiele hingegen „propagieren“ die Objekte: Hat die Software auf dem Bildschirm ein Objekt erfasst, wird es farbig umrahmt. Von Tracklet zu Tracklet bewegt sich der farbige Rahmen mit dem Objekt mit, bis dieses aus der Szene verschwindet. Wird es auf der Straße voll, bewegen sich Dutzende dieser Rahmen über das Videobild. Dank des Weltmodells kann das System sehr genau vorausahnen, wie sich ein Objekt bewegt. Ein Fußgänger wird bei Grün nicht plötzlich auf Autogeswindigkeit beschleunigen. Und ein Fahrzeug, das kurz hinter einem Gegenstand im Vordergrund verschwindet, bewegt sich im Gedächtnis der Software weiter, wenn alle anderen Fahrzeuge mit derselben Fahrtrichtung ihren Weg ebenfalls fortsetzen.

Beachtlich ist das Tempo der Analyse. Es geht nicht allein um 24 Bilder pro Sekunde. Wer den fließenden Verkehr im Auge behalten und in Echtzeit ana-

Bringen dem Bordcomputer den 7. Sinn bei: Bernt Schiele (oben), Bojan Pepik, Jan Hosang und Mykhaylo Andriluka (unten, von links) entwickeln eine Software, die es Autos sogar ermöglicht, autonom zu fahren.





Aus einem zweidimensionalen Bild, wie es rechts in der Grafik dargestellt ist, gewinnt der Bordcomputer des rechten Autos ein dreidimensionales Verständnis der Verkehrssituation. Eine Kamera filmt die Straßenszene mit dem Winkel θ . Anhand ihres antrainierten Weltwissens berechnet die Software aus der Höhe H^i den Abstand O^i zu einem nahenden Fahrzeug und aus der Veränderung der Höhe dessen Geschwindigkeit V^i .

lysieren will, muss schneller sein. So läuft die ganze komplexe Wahrscheinlichkeitsrechnung in Millisekunden ab. Diese permanente schnelle Analyse hat den Vorteil, dass sie vor bösen Überraschungen schützt. Ein Auto, das verdeckt durch eine Schlange stehender Fahrzeuge in die Kreuzung rast, wird vom Notbremsassistenten möglicherweise übersehen. Mit der 3D-Szenenanalyse dürfte es frühzeitig entdeckt werden, wenn es in den Lücken zwischen den stehenden Fahrzeugen kurz auftaucht.

VIDEOS VON EINER KAMERA IM RÜCKSPIEGEL

Fahrzeugen ein vorausschauendes Verständnis für das Beizubringen, was um sie herum geschieht, interessiert natürlich auch Autohersteller. Tatsächlich kooperiert Schiele seit Jahren mit solchen Unternehmen. Für die Aufnahme der Auto-Videosequenzen wurde ihm und seinen Mitarbeitern beispielsweise ein Fahrzeug mit einer kleinen Kamera am Rückspiegel zur Verfügung gestellt. „Doch es geht hier ja nicht nur um Autos“, sagt Schiele. Die probabilistische 3D-Szenenanalyse eigne sich vielmehr für die Analyse sehr verschiedener Filmsequenzen – zum Beispiel auch für die Bilder aus den Kameraaugen eines Roboters im Haushalt oder in einer Fabrik.

Einige der von Schiele und seinen Mitarbeitern entwickelten Softwarebausteine werden demnächst erstmals

in den USA in einem autonom fahrenden Auto zum Einsatz kommen. Zunächst sollen die Fußgänger- und Objektdetektoren zeigen, was sie leisten können. Dabei will Schiele möglichst praxisnah testen, wie die Detektoren mit Radar- und Laserscannern zusammenarbeiten. Ein Ziel ist es, mit möglichst wenigen und vor allem handels-

üblichen Radar- und Kamerasystemen auszukommen, wie sie heute bereits in Autos eingesetzt werden. Denn nur wenn sich das System mit vertretbarem technischem Aufwand realisieren lässt, kann es einem Fahrer künftig vielleicht einen 7. Sinn für den Verkehr geben oder irgendwann gleich ganz das Steuer übernehmen. ◀

AUF DEN PUNKT GEBRACHT

- **Notbremssysteme stoppen im letzten Moment, wenn ein Kind oder ein Fahrzeug vor einem Auto auftaucht. Das Verhalten anderer Verkehrsteilnehmer können sie weder analysieren noch voraussehen.**
- **Die automatische 3D-Szenenanalyse erkennt anhand einer Wahrscheinlichkeitsanalyse andere Teilnehmer im Straßenverkehr, auch wenn diese zeitweise verdeckt sind, und kann ihre Bewegungen im Voraus berechnen.**
- **Vorausschauende Assistenten lassen sich mit geringem technischem Aufwand realisieren und könnten ein Auto autonom steuern; sie ermöglichen Robotern aber auch die Bewegung in einer komplexen Umwelt.**

GLOSSAR

Classifier: Eine Software, die Objekte in Verkehrssituationen erkennt. Der Classifier entscheidet anhand von Wahrscheinlichkeitswerten, sogenannten Scores, ob es sich bei einer bestimmten Pixelansammlung im Bild einer realen Szene um das Objekt handelt, auf das er mit Bildern – etwa von Autos oder Fußgängern – trainiert wurde. Für jede Objektklasse sind spezielle Classifier nötig.

Detektor: Ein Programm, das die Ergebnisse der Classifier in einer Score-Map zusammenführt. Es verzeichnet für jedes Pixel eines Bildes, wie hoch die Wahrscheinlichkeit ist, dass es zu einem bestimmten Objekt gehört.

Tracklet: Abfolge von etwa fünf Bildern einer Videosequenz, die für die Auswertung einer Szene zusammengefasst werden. Da sich von Tracklet zu Tracklet größere Sprünge in einer Bewegung ergeben, erkennt der Detektor vor allem teilweise verdeckte bewegte Objekte zuverlässiger.



Spione im Dienst der Sicherheit

Ob E-Mail-Verkehr oder Onlinebanking, unser Alltag am Computer steckt voller Fallen. **Michael Backes**, Fellow am **Max-Planck-Institut für Softwaresysteme** in Saarbrücken, kümmert sich um solche Sicherheitslücken. Dabei arbeiten er und sein Team mit erstaunlichen Methoden.

TEXT **TIM SCHRÖDER**

James Bond lässt grüßen: Mit unkonventionellen Methoden geht das Team um Michael Backes vermeintlichen Sicherheitslücken in unserem elektronisch geprägten Alltag auf den Grund. So rekonstruieren die Informatiker aus der Aufzeichnung von Druckerlärm den Inhalt der ausgedruckten Texte oder entschlüsseln mithilfe des Teleskops die Inhalte von Monitoren, deren Bilder sich etwa in gläsernen Teekannen spiegeln (Seite 74/75).

Der Normalsterbliche hat bereits einen Knoten im Hirn, wenn er nur versucht zu begreifen, womit sich Michael Backes tagtäglich beschäftigt. Backes hingegen versteht auch die abgrundtiefe Mathematik, die dahintersteckt, die verschlungenen Pfade durch eine Welt voller Abstrakta. Backes ist Informatiker, 32 Jahre alt und war mit 26 Jahren jüngster Professor Deutschlands. Er tüfelt an mathematischen Beweisen, an logischen Folgen, an verworrenen Wenn-dann-Beziehungen, bei denen eine Annahme gilt, wenn der Wert X Element einer bestimmten Teilmenge ist oder wenn Sigma die Eigenschaft H hat.

Michael Backes ist Professor für Kryptografie an der Universität Saarbrücken und zugleich Fellow am Saarbrücker Max-Planck-Institut für Software-systeme. Er knobelt am liebsten an Dingen, die andere für sicher halten. „Wenn jemand eine neue Verschlüsselungstechnik entwickelt hat, denke ich: toll – und dann versuche ich, sie kaputt zu machen.“ Backes stöbert nach Sicherheitslücken in unserem Hightech-Alltag, nach Datenlöchern, die noch niemandem aufgefallen sind. Und er versucht, die Löcher mit besseren Sicherungsstöpseln zu stopfen.

Über eine Methode hat Backes in den vergangenen Monaten besonders nachgedacht – den Zero-Knowledge Proof, ein mathematisches Beweisverfahren. Eine jener alten Ideen, die zwar faszinieren, aber als völlig alltagsuntauglich in der Mottenkiste verschwinden. Backes hat den Zero-Knowledge Proof aus der Mottenkiste geholt, abgestaubt – und damit ein neues Kapitel der Internetsicherheit aufgeschlagen: Der Zero-Knowledge Proof ist zwar abstrakt, aber er hat das Zeug dazu, den Internetnutzer ein für allemal von der Last des Passworts zu befreien. Sender und Empfänger erkennen sich auch ohne kryptische Zahlen- und Buchstabenkombination.

Der Zero-Knowledge Proof ist eine paradoxe Angelegenheit. Das macht schon die deutsche Übersetzung des Begriffs klar: beweisen, ohne Information preiszugeben. Wie soll das gehen? Zero knowledge – null Wissen? Michael Backes erklärt das an einem Beispiel. Man stelle sich vor, ein Schatzsucher habe im Meer ein lange vermisstes Schiffswrack mit einem Goldschatz aufgespürt. Jetzt sucht er einen Finanzier, der das Schiff heben kann, will aber den Fundort nicht verraten. Als Beweis bringt er deshalb nur einige Münzen oder ein Stück des Wracks mit. „Dieser Vergleich hinkt ein wenig“, gibt Backes zu. „Bei einem echten Zero-Knowledge Proof hätte der Schatzsucher nicht einmal die Geldstücke zeigen müssen, um zu beweisen, dass er den Fundort kennt.“

VERTRAUENSWÜRDIGKEIT – EINE SACHE DER MATHEMATIK

Ganz ähnlich muss jeder Internetnutzer heute permanent beweisen, dass er tatsächlich er selbst ist – etwa wenn er das Passwort seines Bankkontos oder die Nummer seiner Kreditkarte beim Online-Versandhandel eintippt. Und manch einer hat leise Befürchtungen, dass irgendwo jemand sitzt, der die Daten abfängt und die Geheimnummer hackt. Das heutige Internet gilt vielen als wenig vertrauenswürdige Instanz, rechtsfrei wie die Straßen von Chicago während der Prohibition.

Der Wunsch nach mehr Sicherheit ist groß, und genau die könnten die Zero-Knowledge-Proof-Ideen von Backes künftig bieten. Ein solches Verfahren prüft mathematisch, ob eine Information zuverlässig ist. Voraussetzung ist, dass der Nutzer ein verlässliches Datendokument besitzt, das Echtheit garantiert – etwa einen elektronischen Ausweis, der zuverlässig darüber Auskunft gibt, ob der Nutzer volljährig ist. Der Zero-Knowledge Proof ist dann so etwas wie eine mathematische Schnittstelle.

Sie teilt dem Empfänger zwar mit, dass die Angaben des Senders, etwa das Alter, stimmen. Das Geburtsdatum aber bleibt geheim. Der Computer des Empfängers kann damit aus den mathematischen Codes herauslesen, ob der Sender zu einer Gruppe vertrauenswürdiger Personen zählt. Wer der Sender ist, erfährt der Empfänger selbstverständlich nicht. Der Sender kann anonym bleiben.

Wer heute ein Horrorvideo von einem Onlinedienst herunterladen will, muss nachweisen, dass er volljährig ist. Dazu muss man unter anderem das Geburtsdatum oder andere persönliche Daten angeben – und die sind in der Welt des Internets eben nicht besonders gut aufgehoben. Das Zero-Knowledge-Proof-Verfahren aber kommt ohne das Geburtsdatum aus, denn es beweist einfach nach mathematischen Regeln, dass die Person volljährig ist.

Was nach der Quadratur des Kreises klingt, funktioniert tatsächlich. In den 1980er-Jahren hat man den Zero-Knowledge Proof entwickelt. Und tatsächlich kann man damit die Zuverlässigkeit des Senders und die Wahrheit einer Aussage prüfen. Doch die mathematische Kommunikation zwischen Sender und Empfänger ist aufwendig und für das flinke Internet viel zu schwerfällig. Kein Wunder, dass die Methode lange im Dornröschenschlaf schlummerte.

Seit einiger Zeit gibt es Konzepte, wie man praxistauglichere Lösungen entwickeln könnte. Darauf baut Backes jetzt neue vereinfachte Internetprotokolle, kleine Sende- und Empfangsprogramme auf, die auf Zero-Knowledge Proof basieren. Lange konnte niemand in überschaubarer Zeit prüfen, wie sicher diese Zero-knowledge-Proof-Abkömmlinge eigentlich sind. Michael Backes hat das geschafft. Er hat eine Software entwickelt, die in Sekundenschnelle berechnen kann, ob das Protokoll tatsächlich dichthält. Damit ebnet er der guten alten Zero-knowledge-Proof-Idee den Weg ins Internet. Mehr noch: Zusammen mit seinen Mitarbeitern hat er eine Art ma-



thematischer Blackbox entwickelt, welche die vertraulichen Informationen eines Internetnutzers enthält, etwa die Daten eines Personalausweises.

Je nach Art der Anfrage, etwa nach dem Alter, kann die Box selektiv antworten. Allerdings gibt sie nicht die vertraulichen Daten selbst aus. Sie ist vielmehr der Datenspeicher, auf den die Zero-knowledge-Proof-Maschinerie zugreift, um die Korrektheit der Daten zu beweisen. Wer im richtigen Leben seinem Gegenüber seine wahre Identität beweisen will, ohne Vertrauliches zu verraten, der geht zum Notar. Der Notar überprüft die Angaben auf dem Personalausweis und bestätigt dem Dritten, dass man der ist, für den man sich ausgibt. In einem sicheren Internet der Zukunft könnte den Job des Notars die Zero-knowledge-Proof-Methode übernehmen. Und niemals mehr müsste sich jemand ein Passwort merken.

Als Fellow der Max-Planck-Gesellschaft kann Backes zusammen mit seinen Mitarbeitern frei von Verpflichtungen forschen. Er arbeitet auf hohem Abstraktionsniveau, und es gibt Leute, die ihn unumwunden als genial bezeichnen. Doch seine Arbeit ist keineswegs so abgehoben, dass sie an Bodenhaftung verliert. Sie ist praxisrelevant. „Deshalb bin ich ja Kryptograf geworden“, sagt er. „Ich wollte mich in ein Fachgebiet einarbeiten, bei dem die Menschen noch nachvollziehen können, was ich mache.“

Der Forscher war nach nur zwei Semestern mit dem Informatikgrundstudium fertig und musste sich ein weiteres Jahr später schon für das Diplomthema entscheiden. Er wählte die Datenverschlüsselung und ist auch jetzt noch mit Begeisterung dabei. „Beim Thema Sicherheit geht man immer von bestimmten Annahmen aus – dem Hacker, der sich über die Datenleitung einwählt etwa. Und dann konstruiert man eine Gegenmaßnahme. Wirklich spannend aber wird es erst, wenn man die Annahmen verschiebt und plötzlich ganz andere Bedrohungen denkbar werden“, sagt Backes.

DIE PUPILLE WIRD ZUM GEHEIMNISTRÄGER

Mindestens einmal jährlich gönnt er sich den Luxus, diesen Gedanken auf die Spitze zu treiben und Bedrohungen zu erforschen, mit denen er im Alltag eigentlich nichts zu tun hat und die vor ihm noch niemandem aufgefallen sind. So kam er auf die Idee, die Bilder von Computermonitoren mit einem starken Teleskop und einer Kamera aus der Ferne abzufotografieren. Das wäre keine große Leistung gewesen, wenn Backes und seine Mitarbeiter die Bildschirme direkt abgelenkt hätten. Doch meist stehen die Monitore mit der Rückseite zum Fenster. Das fiel Backes beim Gang in die Mensa und beim Blick in die Büros der Kollegen auf.

Dann kam ihm der zündende Gedanke: Es müsste doch möglich sein, die Reflexion des Bildschirms von spiegelnden Oberflächen im Büro abzufotografieren? Die Ergebnisse waren beeindruckend. Fast jeder glänzende Gegenstand im Zimmer wirft das Computerbild quasi zum Fenster hinaus. Reflexions-Spitzenreiter war eine gläserne Teekanne. Aus einer Entfernung von zehn Metern konnten die Saarbrücker Wissenschaftler auf der gewölbten Oberfläche noch gespiegelte 12-Punkt-Schrift erkennen – mit einer Ausrüstung, die gerade einmal 1200 Euro gekostet hatte: einer Digitalkamera, zwei Teleskopen und ein wenig Bildanalysesoftware. Auch Brillengläser und sogar die Pupille des Computernutzers spiegeln passabel. Bei der Bildanalyse unterstützten Backes Kollegen aus dem Institut und aus der Universität.

„Sich in die Sicherheitssysteme von Behörden, Firmen oder Labors einzuhacken, das ist heutzutage im Grunde viel zu aufwendig“, sagt Backes. Datenräuber sind deshalb kreativ und erfinden neue Spionagewerkzeuge. Und Backes tut das auch. „Wie klagt man geheime Patientendaten?“, fragte er sich vor einiger Zeit und landete damit den Spionagecoup 2009. „Nicht unbedingt, indem man versucht, die Datenleitung anzuzapfen.“ Seine Mitarbeiter und er grübelten eine Weile in großer Runde im Büro: Druckergeräusche, das war's.

Ärzte sind verpflichtet, Rezepte für verschreibungspflichtige Medikamente

mit Nadeldruckern auszustellen, weil sich damit, anders als bei Tintenstrahldruckern, Durchschläge machen lassen. Die Saarbrücker überlegten, ob man aus dem Druckerlärm, der seit Jahrzehnten gänzlich ungefiltert aus den Nadeldruckern quillt, auf die gedruckten Worte schließen könnte. Zunächst versuchten die Forscher in dem Geräuschbrei einzelne Buchstaben zu erkennen, doch die verschmierten im Lärm.

Dann verlegten sie sich darauf, Texte wortweise zu erlauschen. Zuerst ließen sie einen Nadeldrucker einzelne Wörter ausdrucken, nahmen den Klang auf und lernten damit ein Lautanalyseprogramm an. Danach spielten sie dem Computer kleine Texte zu verschiedenen Themen vor – einen Artikel aus Wikipedia über Computertechnik, einen über Barack Obama und einen über Architektur. Und wirklich: Der Rechner erkannte 65 bis 70 Prozent der Wörter richtig. Das reichte, um den Textinhalt zu verstehen.

Anschließend folgte der Praxiseinsatz. Backes fragte in einer Saarbrücker Praxis an, montierte ein kleines Funkmikrofon unter dem Drucker und setzte sich mit einem Laptop ins Wartezimmer. Wann immer der Drucker lärmte, schnitt das Notebook den akustischen Schwall mit. Trotz der Hintergrundgeräusche, Unterhaltungen am Tresen oder Telefongespräche, sezierte die Lauterkennungssoftware anschließend sauberlich Wörter und Zahlen aus dem Klangteppich – selbst Abkürzungen wie „Müllersche Tabletten bei Halsschm.“ erkannte sie einwandfrei.

Datenklau auf neuen Wegen, das ist es, was Backes reizt. Er wollte wissen, wie groß die Gefahr wirklich ist, und startete eine Umfrage bei Ärzten und auch bei Banken, denn dort werden Kontoauszüge und andere Dokumente ebenfalls noch immer mit Nadeldruckern ausgedruckt. „Die Ergebnisse haben uns selbst völlig überrascht: 60 Prozent aller Arztpraxen und 30 Prozent aller Banken setzen heute noch Nadeldrucker ein, und bisher schert sich niemand um die akustische Abstrahlung“, sagt der Informatiker.

Michael Backes kann am besten denken, wenn er spazieren geht. Ihm gibt es mehr, mit Freunden ins Café oder in die Bar zu gehen, als stundenlang am Computer zu hocken. Viel-

leicht ist das sein Erfolgsrezept. Denn für das, was er schon erreicht hat, die Auszeichnungen, die er schon erhalten hat, brauchen andere Jahrzehnte. Im Jahr 2009 kürte ihn das US-amerikanische Wissenschaftsmagazin *TECHNOLOGY REVIEW* des angesehenen Massachusetts Institute of Technology zu einem der „TR35“, der weltweit 35 besten Jungforscher, die die Welt verändern werden. Bisher wurde die Ehre noch keinem anderen Deutschen zuteil.

INTIMES IM INTERNET FÜR DIE EWIGKEIT

Dieser Erfolg rührt freilich auch daher, dass sich Backes mit einem Massenmedium wie dem Internet beschäftigt. Das geht jeden an, jeder ist von dessen Sicherheit oder Unsicherheit betroffen. Wer heute private Daten und Intimes ins Internet stellt, muss sich darüber im Klaren sein, dass sich die Information bis in alle Ewigkeit perpetuieren und damit unauslöschlich sein wird. Im Zweifelsfall ist das Internet ein moderner, nicht enden wollender Pranger. Doch was sind intime Daten? Und was oder wie viel darf ich von mir preisgeben, um noch anonym zu bleiben? Auch mit solchen Gedanken beschäftigt sich Backes.

„Es ist erstaunlich, wie schnell man aus kleinen Fragmenten, aus eigentlich harmlosen Informationen, auf das persönliche Profil eines Nutzers schließen kann“, sagt der Forscher. Längst gibt es Softwareprogramme, welche die Übereinstimmung zwischen verschiedenen Informationen miteinander abgleichen.

Durch dieses „Matching“ lassen sich Daten zusammentragen, die zu einem gemeinsamen Profil passen – zu ein und derselben Person. Bewertet jemand anonym Videofilme für Erwachsene in einem Internetforum, klingt das zunächst wenig problematisch. Diskutiert er einen Teil der Filme aber nicht-anonym in einem anderen öffentlichen Forum, kann ein Matching-Programm die Ähnlichkeiten erkennen und die anonymen Daten der Person zuordnen.

„Noch sind diese Matching-Werkzeuge nicht leistungsstark genug, um die gigantischen Datenmengen im Internet auf wirklich systematische Art zu durchforsten“, sagt Michael Backes, „doch die Gefahr besteht, dass persönliche Daten künftig verstärkt genutzt und ausgenutzt werden.“ Er versucht deshalb, den Verlust an Privatsphäre einzuschätzen. „Wie anonym bin ich noch, nachdem ich eine bestimmte Information im Internet eingegeben habe?“ Backes entwickelt Programme, sogenannte Protokolle, die diesen Verlust korrekt einschätzen können.

Nach seinem Informatikstudium hatte Backes zunächst am IBM-Forschungslabor im schweizerischen Rüschlikon an Sicherheitssystemen gearbeitet. Danach berief ihn die Universität Saarbrücken zum Professor auf Lebenszeit. Das ist jetzt sechs Jahre her. Angesichts der hohen Schlagzahl, die Backes vorlegt, darf man gespannt sein, was als Nächstes kommt. Und wer weiß – vielleicht hat er inzwischen sogar eine Fangemeinde, die geduldig auf das nächste Spionage-Highlight des Jahres wartet. ◀

GLOSSAR

Kryptografie: Schon im Alten Ägypten nutzte man die Verschlüsselung von Informationen und damit Techniken der Kryptografie. Das Wort stammt aus dem Griechischen und bedeutet so viel wie „geheim schreiben“. Heute befasst sich die Kryptografie vor allem mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Systemen, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind.

Matching: Matching heißt im Englischen so viel wie „Abgleich“. In der Kryptografie ist die Suche nach Übereinstimmungen zwischen verschiedenen Informationen gemeint. So kann ein entsprechendes Softwareprogramm etwa Ähnlichkeiten erkennen und anonyme Daten einer bestimmten Person zuordnen.

Zero-Knowledge Proof: Bei dieser Methode kommunizieren zwei Parteien (der Beweiser und der Verifizierer) miteinander. Der Beweiser überzeugt dabei den Verifizierer mit einer gewissen Wahrscheinlichkeit davon, dass er ein Geheimnis kennt, ohne dabei Informationen über das Geheimnis selbst bekannt zu geben. Beweiser und Verifizierer tauschen dazu mathematische Schlüssel aus.

Standorte

- Institut / Forschungsstelle
- Teilinstitut / Außenstelle
- Sonstige Forschungseinrichtungen
- Assoziierte Forschungseinrichtungen

Niederlande

- Nimwegen

Italien

- Rom
- Florenz

USA

- Jupiter, Florida

Brasilien

- Manaus

Luxemburg

- Luxemburg



MAX-PLANCK-GESellschaft

Impressum

MAXPLANCKFORSCHUNG wird herausgegeben von der Wissenschafts- und Unternehmenskommunikation der Max-Planck-Gesellschaft zur Förderung der Wissenschaften e. V., vereinsrechtlicher Sitz: Berlin.
ISSN 1616-4172

Redaktionsanschrift

Hofgartenstraße 8, 80539 München
Telefon: 089 2108-1276 (Fax: -1405)
E-Mail: mpf@gv.mpg.de
Internet: www.mpg.de/mpforschung
Kostenlose App: www.mpg.de/mpf-mobil

Verantwortlich für den Inhalt

Dr. Christina Beck (-1276)

Redaktionsleitung

Peter Hergersberg (Chemie, Physik, Technik; -1536)
Helmut Hornung (Astronomie; -1404)

Redaktion

Susanne Beer (Kultur, Gesellschaft; -1342)
Dr. Elke Maier (Biologie, Medizin; -1064)
Dr. Harald Rösch (Biologie, Medizin; -1756)

Bildredaktion

Susanne Schauer (-1562)

Wissenschaftlicher Beirat

Prof. Dr. Gerhard Wegner
Prof. Dr. Heinz Wäßle
Prof. Dr. Wolfgang Prinz

Gestaltung

Julia Kessler, Sandra Ostertag
Voßstraße 9
81543 München
Telefon: 089 2781 8770
E-Mail: projekte@designergold.de

Litho

kaltner verlagsmedien GmbH
Dr.-Robert-Zoller-Straße 1
86399 Bobingen

Druck & Vertrieb

Vogel Druck- & Medienservice GmbH
Leibnizstraße 5, 97204 Höchberg

Anzeigenleitung

Beatrice Rieck
Vogel Druck- & Medienservice GmbH
Leibnizstraße 5, 97204 Höchberg
Telefon: 0931 4600-2721 (Fax: -2145)
E-Mail: beatrice_rieck@vogel-druck.de

MAXPLANCKFORSCHUNG berichtet über aktuelle Forschungsarbeiten an den **Max-Planck-Instituten** und richtet sich an ein breites wissenschaftsinteressiertes Publikum. Die Redaktion bemüht sich, auch komplexe wissenschaftliche Inhalte möglichst allgemeinverständlich aufzubereiten. Das Heft erscheint in deutscher und englischer Sprache (**MAXPLANCKRESEARCH**) jeweils mit vier Ausgaben pro Jahr; die Auflage beträgt derzeit 85 000 Exemplare (**MAXPLANCKRESEARCH**: 10 000 Exemplare). Der Bezug ist kostenlos. Ein Nachdruck der Texte ist nur mit Genehmigung der Redaktion gestattet; Bildrechte können nach Rücksprache erteilt werden. Die in **MAXPLANCKFORSCHUNG** vertretenen Auffassungen und Meinungen können nicht als offizielle Stellungnahme der **Max-Planck-Gesellschaft** und ihrer Organe interpretiert werden.

Die **Max-Planck-Gesellschaft** zur Förderung der Wissenschaften unterhält 83 Institute und Forschungseinrichtungen, in denen rund 21 600 Personen forschen und arbeiten, davon etwa 5 500 fest angestellte Wissenschaftlerinnen und Wissenschaftler. Der Jahresetat 2014 umfasst insgesamt 1,6 Milliarden Euro. Die **Max-Planck-Institute** betreiben Grundlagenforschung in den Natur-, Lebens- und Geisteswissenschaften. Die **Max-Planck-Gesellschaft** ist eine gemeinnützige Organisation des privaten Rechts in der Form eines eingetragenen Vereins. Ihr zentrales Entscheidungsgremium ist der Senat, in dem Politik, Wissenschaft und sachverständige Öffentlichkeit vertreten sind.



MAXPLANCKFORSCHUNG wird auf Papier aus vorbildlicher Forstwirtschaft gedruckt und trägt das Siegel des Forest Stewardship Council (FSC)

Forschung für unterwegs

Die **MaxPlanckApp** für iOS und Android
mit Nachrichten, Videos, Podcasts



„Ich finde alles sehr gelungen, vom Inhalt bis zur Darstellung.“

„Gerade als Lehrer muss man sich ständig weiterbilden. So bin ich am Puls der Zeit und kann auch bei aktuellen Themen meinen Schülern Hintergrundwissen liefern. Tolle App.“

„Nur zu empfehlen und vor allem kostenlos. Also zugreifen.“

Kostenloser Download



Für iOS:
<http://itunes.apple.com/de/app/maxplanckapp/id506613606>



Für Android:
<https://play.google.com/store/apps/details?id=de.mpg.mpgapp>



MAX-PLANCK-GESELLSCHAFT