Doris Griesser

Ein Sicherheitsnetz für unsere smarte neue Welt

A Safety Network for our Smart New World

Das „Internet der Dinge“ (IdD) wird unser Leben auf noch kaum vorstellbare Weise verändern. Vom selbst fahrenden Auto bis zum smarten Energiesystem wird die Welt demnächst von intelligenten, sich selbst regulierenden Objekten wimmeln. Dadurch wird vieles leichter, doch das IdD birgt auch große Gefahren. An der TU Graz soll nun jenes Know-how erarbeitet werden, mit dem sich die Risiken des neuen Meganetzes minimieren lassen.

Im Internet der Dinge können sich die unterschiedlichsten Gegenstände vernetzen und drahtlos miteinander kommunizieren. Ermöglicht wird das durch die extreme Miniaturisierung von Computern, die in Form winziger Systeme in alle nur denkbaren Objekte integriert werden können. Beispielsweise in „intelligente“ Heizungs- und Beleuchtungssysteme von „Smart Homes“ oder in Duschkabinen, die selbsttätig den Notdienst verständigen, wenn die Benutzerin oder der Benutzer stürzt. Geschätzte 50 Milliarden Geräte sollen bis 2020 bereits mit dem Internet verbunden sein.

The “Internet of Things” (IoT) will change our lives in a way that we can hardly imagine now. From the autonomously driving car to the smart energy system, the world will soon be full of intelligent self-regulating objects. This will make many things easier, but of course there are also many risks and dangers to the IoT. Graz University of Technology is now planning to develop the know-how to minimise the risks of the new mega-network.

In the Internet of Things, all kinds of objects can form networks and engage in wireless communication. This has been made possible by the extreme miniaturisation of computers that can now be integrated as small systems in all manner of objects. For instance in the intelligent heating and lighting systems of “smart homes” or shower cabins that call the emergency services when the user slips and falls. According to current estimates about 50 billion devices will be connected to the Internet as early as 2020.

Abbildung 1:
Modell-Lkw sollen dank Vernetzung in einem neu gestalteten Testlabor selbstständig verschiedenste Manöver ausführen.
Figure 1:
Networked heavy goods vehicles will drive autonomously in a new test laboratory.

Kommunizierende Fahrzeuge
Auch die TU Graz arbeitet in etlichen Bereichen an dieser Entwicklung mit: etwa im Feld der Produktion, wo sich mithilfe dieser Technologie inzwischen ein Trend zur Einzelanfertigung im industriellen Maßstab durchgesetzt hat. Basis dafür ist die Vernetzung der zu produzierenden Gegenstände mit den Maschinen. Diese erhalten ihre Arbeitsaufträge in Form der gewünschten Maße und Ausführungen etc. direkt von den Produkten, die so zu Maßanfertigungen werden.

Immer smarter werden auch unsere Fahrzeuge. Über eingebaute Sensoren werden Autos in naher Zukunft miteinander sowie mit der benutzten Infrastruktur kommunizieren, um ihre Lenkerin oder ihren Lenker rechtzeitig vor brenzligen Situationen zu warnen. „Mittels Sensoren können auch Objekte und Menschen sichtbar gemacht werden, die sonst in der Dunkelheit oder im toten Winkel des Spiegels verborgen wären“, erläutert Kay Römer vom Institut für Technische Informatik der TU Graz. Lkw sollen dank Vernetzung selbstständig in einem genau berechneten Abstand im Konvoi fahren können – wobei nur im ersten Fahrzeug tatsächlich ein Mensch sitzen muss. Ein entsprechendes Testlabor zur Überprüfung und Verbesserung der Sicherheit dieser Technologie wird an der TU Graz gerade aufgebaut.

Parkplatzsuche in Zeiten des IdD
Auch die Verkehrsinfrastruktur wird im Internet der Dinge kräftig mitmischen. So haben Forschende der TU Graz gemeinsam mit spanischen Kolleginnen und Kollegen ein System zum schnellen Auffinden freier Parkplätze entwickelt. Diese werden >

Communicating vehicles
Graz University of Technology is also contributing to this development in various areas. For instance in production where this technology has driven a trend towards individual production at industrial scale. This is based on networking the objects produced on the machines with the machines that produced them. The machines receive the job orders, for instance the desired dimensions and features etc., directly from the products themselves and thus become tailor-made creations.

Our vehicles are constantly becoming smarter, too. In the near future cars will be equipped with sensors to communicate between themselves and with the infrastructure they are using to warn the driver in time that there is a tricky situation heard. “Sensors can also make objects and people visible that would otherwise be hidden in the dark or in the blind spot of the rear view mirror,” explains Kay Römer from the Institute of Technical Informatics at Graz University of Technology. Networked heavy goods vehicles, of which only the first vehicle needs to have a human driver, will drive in a convoy, keeping a precisely calculated distance between each other. At Graz University of Technology we are currently setting up a test laboratory to validate and improve the safety of this technology.

Looking for a parking space in the era of the IoT
The Internet of Things will also leave a big mark on the traffic infrastructure. Working in cooperation with Spanish colleagues, researchers at Graz University of Technology recently developed a system to locate available parking spaces quickly. These parking spaces are fitted with sensors that tell the internet whether they are currently free or occupied. A special app guides the driver to the nearest vacant parking space. And as another Graz University of Technology initiative shows, even pipelines can >

© Baustädter – TU Graz

Abbildung 2:
Insgesamt stehen drei Modell-Lkw im Testlabor zur Verfügung. Adaptiert wurden sie direkt an der TU Graz.
Figure 2:
Three miniature HGVs are to be tested in the new test laboratory. They were adapted for the project at TU Graz.

mit Sensoren versehen, die dem Netz mitteilen, ob sie gerade frei oder besetzt sind. Eine spezielle App lotst die Fahrerin oder den Fahrer zum nächsten freien Abstellplatz. Selbst Rohrleitungen können auf diese Weise „intelligent" gemacht werden, wie eine andere TU Graz-Initiative zeigt: Indem man sie mit Minicomputern ausstattet, die wiederum mit Sensoren verbunden sind, können die Leitungen Daten über die Wassermengen liefern, die durch sie fließen. „So ließen sich Lecks deutlich kostengünstiger ermitteln und genauer lokalisieren", erklärt Kay Römer. „In der Folge reguliert sich der Wasserdruck automatisch, sodass kaum noch Wasser verloren ginge." Da in österreichischen Leitungen zurzeit bis zu 25 Prozent des Wassers durch undichte Stellen verloren gehen, ist für Wasserverteilnetze der Aufstieg in die höhere Intelligenzklasse eine Frage der Wirtschaftlichkeit.

Intelligente Energienetze

Ebenso verhält es sich mit den Energienetzen, bei denen überdies die ökologische Dimension eine zentrale Rolle spielt: Da immer mehr kleine, dezentrale Lieferantinnen und Lieferanten ihre aus Wasser, Sonne oder Umgebungswärme eher unregelmäßig gewonnene Energie in das Netz einspeisen, kann es zu großen Schwankungen bei der gerade verfügbaren Energie kommen.

be 'smarted up' in this way. If they are equipped with sensor-connected minicomputers, the pipelines will be able to send data about of the water volume that flows through them. According to Kay Römer, this would be a much more effective and accurate method to locate leaks. In the end the water pressure would be regulated automatically to almost completely prevent the loss of water. As Austrian pipelines currently lose about 25 percent of the water they carry through leaks, upgrading the water distribution networks to a higher level of intelligence is simply a question of economy.

Intelligent energy networks

The same applies to energy networks. In this case the ecological dimension plays a key role. As an increasing number of small decentralised suppliers feed their irregularly generated hydropower, solar power or ambient heat from water, sun or heat into the grid, the energy available at any one particular moment in time can fluctuate quite considerably. Computers on the feed-in and tapping points are useful to balance out energy consumption and energy supply. At the final consumer's end, the smart meter measures and controls the energy consumption. But while this helps considerably to optimise the energy efficiency and minimise carbon dioxide emissions, what happens with the personal data in

Computer an den Einspeise- und Entnahmestellen sollen helfen, Energieverbrauch und Energieangebot in eine Balance zu bringen. Bei den Endverbraucherinnen und Endverbrauchern ist es der „Smart Meter", mit dem das Energiekonsumverhalten gemessen und gelenkt werden soll. In Hinblick auf die Energieeffizienz und damit die Kohlendioxidemissionen ist das ein großer Fortschritt – doch was passiert mit all den persönlichen Daten im IdD, aus denen man ziemlich genau herauslesen kann, was jemand zu welcher Zeit in seiner Wohnung tut? Was ist, wenn Hackerinnen und Hacker in dieses riesige Netz eindringen und es manipulieren oder zerstören? Ist man für solche Fälle gerüstet? Wie sicher ist überhaupt die schöne neue Welt des IdD, in der man über den Computer ganze Energie- und Wasserleitungssysteme, Kraftwerke und Straßen lahmlegen kann? Erhöht sich doch durch die unzähligen vernetzten Geräte auch die Menge und Reichweite derartiger Gefahren.

Leadprojekt für mehr Verlässlichkeit und Sicherheit

„Technisch ist zwar vieles schon in Prototypen umgesetzt, doch eine hundertprozentige Zuverlässigkeit dieser Technologie ist heute noch nicht gegeben", bekennt Kay Römer. „Deshalb wollen wir an der TU Graz unser Know-how bündeln, um deren Verlässlichkeit und Sicherheit zu erhöhen." Zu diesem Zweck wird im kommenden Jahr ein Leadprojekt unter dem Titel „Verlässlichkeit im Internet der Dinge" gestartet, in dem unter Römers Leitung zehn Wissenschafter der Fakultät für Informatik und Biomedizinische Technik sowie der Fakultät für Elektrotechnik und Informationstechnik die Grundlagen für ein zuverlässiges IdD erforschen wollen. Das generierte Wissen soll in realen Anwendungen umgesetzt werden. Die Forschungsinitiative wird für drei Jahre mit zwei Millionen Euro von der TU Graz gefördert und kann bei Erfolg um weitere drei Jahre verlängert werden. „Wir betrachten dieses Projekt als eine Art Keimzelle, aus der sich zahlreiche neue Forschungsaufgaben für die verschiedenen Fields of Expertise der TU Graz entwickeln sollen", so Römer.

Die drei großen Gefahrenquellen

Wie aber kann die Verwundbarkeit und Störanfälligkeit eines so umfassenden Netzes wie des Internets der Dinge minimiert werden? „Wir müssen von den Ursachen ausgehen, warum solche Systeme heute noch nicht verlässlich funktionieren", erläutert der Wissenschafter. Drei Hauptgründe haben die Forschenden identifiziert: So erwächst eine zentrale Gefahr durch die Widrigkeiten der Umgebung, denen solche Systeme ausgesetzt sind. In Straßen oder Fahrzeuge integrierte Sensoren beispielsweise müssen extremen >

the IoT? After all, with this information it is not too difficult to find out quite precisely what somebody is doing in his home and at which time. What if a hacker broke into this huge network and manipulated or destroyed it? Are we prepared for such risks? How safe can it be if all you need in the brave new world of the IoT to paralyse entire energy and water supply systems, power stations and roads is a simple computer? After all, the countless networked devices also multiply the number and magnify the impact of such risks.

Lead project for more reliability and safety

"Technically many of these systems already exist as prototypes, but at present we cannot guarantee that this technology is 100 percent reliable," admits Kay Römer. "At Graz University of Technology we want to concentrate our know-how to increase its reliability and security." This is precisely why a lead project with the title of "Dependable Internet of Things in Adverse Environments" will be launched next year. Under Römer's leadership, 10 scientists from the Faculty of Computer Science and Biomedical Engineering and the Faculty of Electrical and Information Engineering will investigate the basic requirements for a reliable IoT. The knowledge generated in the course of the project should then be translated into real-life applications. For this research initiative Graz University of Technology will provide funds to an amount of € 2 million over three years. If it is successful, it can be extended by a further three years. This project is regarded as a kind of incubator that can breed numerous new research tasks for various fields of expertise at Graz University of Technology.

Three big sources of danger

So how can we reduce the vulnerability and chances of failure of a massive network such as the IoT? According to Römer, "the question always has to be why such systems are not working reliably at >

© TU Graz

Abbildung 3:
Zehn Forscher von zwei Fakultäten beteiligen sich am Leadprojekt „Verlässlichkeit im Internet der Dinge".
Figure 3:
10 scientists from two different faculties are taking part in the lead project "Dependable Internet of Things in Adverse Environments".