
TU Graz
Graz University of Technology
Graz University of Technology
MAN
TU GRAZ

Witterungsbedingungen und Belastungen standhalten. Eine latente Bedrohung sind zudem Sabotage und Terroranschläge, denn eine Cyberattacke etwa auf ein Energie- oder Wassernetz etc. könnte in kürzester Zeit eine ganze Gesellschaft lähmen. „Das Internet der Dinge ist deshalb besonders schwer zu schützen, weil man über die einzelnen Geräte leicht an das Gesamtsystem herankommen kann“, erklärt Kay Römer. Der dritte Grund für die Verwundbarkeit des IdD ist seine gewaltige Komplexität. Damit es störungsfrei arbeiten kann, müssen Milliarden kleiner Geräte funktionieren und kooperieren.

Lernende Modelle der Realität

Diese drei mächtigen Gefahrenquellen sollen mithilfe neuen Wissens eingedämmt werden: „Zunächst wollen wir ein tiefgreifendes Verständnis der diversen Umgebungseinflüsse erarbeiten und dieses Know-how in die Geräte integrieren, sodass sie ihr Verhalten daran anpassen können“, erläutert der Informatiker. „Zu diesem Zweck entwickeln wir lernende Modelle der Realität, die auch gefährliche Situationen antizipieren können. Damit lässt sich sicherstellen, dass sich die einzelnen Geräte und damit das gesamte System in Notfällen richtig verhalten.“ Wenn ein Gerät eine Bedrohung erkennt, soll es sich selbstständig vom System abkoppeln und damit die Gefahr bannen.

Während an der TU Graz bereits zahlreiche Teilaspekte des Internets der Dinge erforscht wurden, soll im neuen Leadprojekt das große Ganze und alle denkbaren Wechselwirkungen der kommunizierenden Objekte ins wissenschaftliche Visier genommen werden. „Wir haben das Potenzial, in diesem Bereich ein internationales Leuchtturmprojekt aufzubauen“, ist Kay Römer überzeugt. ■

present.” The researchers have identified three main reasons: one big risk factor is the adversities of the environment such systems are exposed to. For example, sensors integrated in roads or vehicles need to withstand extreme weather conditions and loads. Also sabotage and acts of terrorism are recognized as a latent danger, simply because a cyber attack against an energy or water supply network could bring an entire society to a standstill in virtually no time at all. “The Internet of Things is very difficult to protect because all it takes to gain access to the complete system is a single device,” explains Kay Römer. The third reason for the vulnerability of the IoT is its enormous complexity. Its faultless operation depends on billions of small devices which must all function properly and cooperate.

Self-learning models of reality

Newly generated knowledge is to help control these three powerful sources of danger. Römer continues, “the first step must be to gain an intimate understanding of the various environmental influences and then to integrate this know-how in the devices so that they can adjust their behaviour accordingly. We do this by developing self-learning models of reality that are able to anticipate dangerous situations. This will ensure that the various devices and therefore the entire system behaves correctly in case of an emergency.” If a device recognises a threat, it should take itself out of the system and therefore eliminate the danger.

Graz University of Technology has already researched numerous partial aspects of the Internet of Things. Now this lead project will concentrate on the big picture and scientifically investigate all conceivable interactions of the communicating objects. Kay Römer is convinced that Graz University of Technology has the potential to build an international flagship project in this sector. ■

Abbildung 4:
Die Fahrzeuge kommunizieren selbstständig miteinander und ermitteln über Sensoren ihre genaue Position.
Figure 4:
Vehicles communicate autonomously with each other and determine their positions via sensors.