Security in Sensor Networks

Sicherheit in Sensornetzwerken

Stefan Fischer, University of Lübeck,
Martina Zitterbart, Karlsruhe Institute of Technology

Designing and implementing sensor network solutions open up completely new challenges for communication system developers. Such networks literally merge with the real world in which they can sense and control physical phenomena. Therefore, one of the most important issues to be solved is that of security. Services such as confidentiality, integrity, authenticity and access control, but especially privacy and trust are inherently important for the practical use of sensor networks.

However, it is much more difficult than in traditional communication systems to provide these security services, as sensor networks or more specifically sensor network nodes are equipped with much fewer resources, for instance regarding computing power or memory. Conventional procedures which work well in traditional networks can usually only be used in a limited way if at all.

This issue of it – “Security in Sensor Networks” will therefore extensively cope with this issue. It features a total of five articles, organized in three thematic blocks which cover important areas of the subject.

The first block deals with basic procedures for the establishment of traditional security services, such as confidentiality, integrity and authenticity. It contains the contribution “Security Solutions for Uplink- and Downlink-Traffic in Wireless Sensor Networks” authored by Jens-Matthias Bohli, Alban Hessler, Osman Ugus, and Dirk Westhoff which concentrates specifically on selected security and dependability solutions which are able to assure an acceptable security level while at the same time minimizing energy and memory usage.

The second block discusses attacks against sensor networks and possible counter measures. Because of the exposure of sensor nodes to the real world, additional ways of attack against these networks open up, compared to conventional networks. In their article “Attacker Models for Wireless Sensor Networks”, Zinaida Benenson, Erik-Oliver Blass, and Felix C. Freiling classify such attacks and describe how attackers can be modeled formally. On the basis of such models, further steps can be taken, such as the creation of intrusion detection systems. The design and implementation of such systems is described by Christoph Krauss in his article “Detecting Compromised Nodes in Wireless Sensor Networks: Misbehavior-based Detection vs. Attestation-based Detection”.

The third block, finally, addresses the issue of security in sensor network applications. The paper “Security Design for Industrial Sensor Networks” co-authored by Rainer Falk and Hans-Joachim Hof deals with the use of sensor networks in industrial applications such as process automation or machine monitoring. The second article, called “Security in Border Control and Area Monitoring” and co-authored by Daniela Krüger, Christian Haas, Peter Rothniel, Denise Dudek, and Dennis Pfisterer discusses the security requirements of applications operating in the area of real estate and border control.

Finally, we would like to thank all contributors to this special and also the anonymous reviewers who dedicated their time and efforts to improving the whole issue.

Prof. Dr. Stefan Fischer

Prof. Dr. Martina Zitterbart
Prof. Dr. Stefan Fischer is a full professor for computer science and director of the Institute of Telematics. After his PhD in 1996 (University of Mannheim, Germany) and being a postdoc researcher at the University of Montreal, he joined the International University in Germany as an Assistant Professor, in 1998. In 2001 he became an Associate Professor at the TU Braunschweig, and finally he joined the University of Lübeck in 2004. His current research concentrates on massively distributed systems such as sensor networks. He has published over 100 reviewed scientific articles and 6 books.

Prof. Dr. Martina Zitterbart is full professor in computer science at the Karlsruhe Institute of Technology (KIT), Germany. She is director of the Institute of Telematics. She received her doctoral degree form the University of Karlsruhe in 1990 and was Visiting Scientist at the IBM T. J. Watson Research Center, Yorktown-Height, NY, USA in 1991/92. From 1995–2001 she was full professor at the TU Braunschweig. Her current research interests include Future Internet, sensor networks, Internet of energy as well as architectures, algorithms and protocols for communication systems in general. In 2002 Martina Zitterbart received the Alcatel SEL research award on technical communication.