TU Clausthal

Diplomanden- und Doktorandenseminar
des Instituts für Informatik

Sichere Datenkommunikation mit ressourcen-beschränkten eingebetteten Systemen über schmalbandige funkbasierte IPv6-Netzwerke

Daniel Fischer, TU Clausthal

Ein seit einigen Jahren bestehender und stetig wachsender Trend ist die Vernetzung verschiedenster Geräte mit dem Internet, um sie so aus der Ferne beobachten und/oder steuern zu können. Mit der flächendeckenden Ablösung von IPv4 durch IPv6 ist es möglich und wird von Forschern auch so erwartet, dass weltweit Milliarden von unterschiedlichsten Geräten eigene IPv6-Adressen bekommen und so das Internet der Dinge (Internet of Things, IoT) formen. Mit der Einführung des IEEE-802.15.4-Standards, der auch die Basis von Zigbee darstellt, gibt es seit einigen Jahren auch einen wohl definierten Standard für schmalbandige Funkübertragungen (~100kBit/s) mit sehr geringem Energieverbrauch (so genannte LoWPANs, Low-Power-Personal-Area-Networks), der die drahtlose Vernetzung kleinster batteriebetriebener eingebetteter Systeme wie beispielsweise einfacher Temperatursensoren ermöglicht. Zur Einbettung solcher Geräte in IPv6-Netzwerke wie dem (zukünftigen) Internet wurden unter dem Begriff 6LoWPAN (IPv6-over-Low-Power-Personal- Area-Networks) verschiedene Techniken entwickelt. Die Anwendungs-gebiete sind sehr vielfältig: Gebäude- und Industrieautomatisierung, Smart-Metering und Smart-Grid, Umweltüberwachung, etc. Ein bisher noch wenig beachteter aber sehr wichtiger Aspekt ist dabei das Thema Sicherheit.

Das übergeordnete Ziel dieser Arbeit war die Implementierung einer vollständigen und gesicherten Funkstrecke zur Übertragung von Daten. Dazu wurde zunächst das für IoTAnwendungen weit verbreitete Open-Source Betriebssystem namens Contiki-OS, welches bereits einen IPv6- und 6LoWPAN-Stack enthält, studiert und auf zwei typische und repräsentative Hardware-Systeme für Anwendungen aus dem IoT-Bereich portiert. Die verwendeten Systeme haben strenge Ressourcenbeschränkungen hinsichtlich RAM (wenige kB), ROM (wenige hundert kB), Rechenleistung (wenige MHz) sowie der verfügbaren Energie (Batteriebetrieb), weshalb eine effiziente Nutzung dieser Ressourcen für zum Einsatz kommende Protokolle unabdingbar ist. Anschließend wurden verschiedene Sicherheitsprotokolle (IEEE-802.15.4-Security, IPSec, DTLS) analysiert und beispielhaft auf den verwendeten Systemen implementiert respektive bestehende Implementierungen portiert und hinsichtlich ihres Ressourcenverbrauchs und allgemeiner Aspekte (Ende-zu-Ende-Sicherheit, Konfigurationsaufwand, etc.) evaluiert.

Montag, den 28.10.2013
13 Uhr c.t. in Raum 210, IfI, Am Regenbogen 15

Technische Universität Clausthal • Institut für Informatik • Julius-Albert-Straße 4 • 38678 Clausthal-Zellerfeld
Tel +49.(0)5323.72.7100 • Fax +49.(0)5323.72.7139 • http://www.in.tu-clausthal.de • info@in.tu-clausthal.de