Programming and Securing Service-oriented Wireless Sensor Networks

Hans-Joachim Hof, Bernhard Hurler, Anton Hergenröder, Christian Haas and Michel Conrad
Institute of Telematics, Universität Karlsruhe (TH), Karlsruhe, Germany
Email: [hof|hurler]@tm.uka.de, [anton.hergenroeder|christian.haas|michel.conrad]@ira.uka.de

Our demonstrator shows the implementation of a Service-oriented Architecture (SoA) for wireless sensor-actuator networks (WSAN). It demonstrates the feasibility of our service-oriented system in a real-world, resource-restricted WSAN based on off-the-shelf MICAz motes running the operation system TinyOS. In contrast to data-oriented approaches our service-oriented system does not only provide ”traditional” uni-directional data transfer (from sensor nodes to a base station), but also enables autonomous collaboration of sensor nodes. The nodes collaborate in the sense that the input of several sensors is used to trigger actuators, which in turn affect the sensor readings etc.

For demonstration purposes we built an *intelligent greenhouse* that autonomously adapts its ambience in order to cultivate plants according to their individual and collective needs (see Figure 1). E.g., the lighting of the greenhouse is adapted considering all plants' needs and the sunlight. For visualization we constructed a miniature version of the greenhouse with several plants. The greenhouse itself as well as the plants within are all equipped with various sensors and actuators in order to measure and modify the plants' ecosystem (i.e. light and soil humidity). We also simulate external influence on the ecosystem, such as the influence of the sun on the greenhouse's light control.

Protocol details of our service-oriented system can be observed via a couple of PDAs connected to the sensor nodes. These PDAs allow for inspecting and changing the internal state of sensor nodes. Hence, attendees of the demonstration can use these PDAs to interact with the WSAN.

We show two fundamental aspects of our Service-oriented Architecture in the demonstration:

- Service description and execution: The intelligent greenhouse application is composed of services. The services are described and executed by *Talassa* (Tasking Language for Service-oriented Sensor-Actuator Networks [1]).
- Secure lookup of available services: Services are stored in a distributed service directory, *SCAN* (Secure Content Addressable Network [2]). As this is a security critical component of our architecture, SCAN has been designed to provide secure service discovery.

Talassa is a description language for distributed WSAN applications based on services. An application consists of a number of atomic services, which perform either basic hardware interaction or influence the control flow of other services. A virtual machine on each sensor node executes any of the above mentioned service types and provides inter-service communication for the control flow services. *Talassa* allows the description of WSAN applications by composing atomic services to collaborating service sets, which can be altered or extended during runtime. For the *intelligent greenhouse* application we implemented a service set for each plant controlling the soil's humidity. A second service set controls the lighting for the greenhouse considering all plants' constraints (upper and lower acceptable lighting bounds). These services are altered and extended, when new plants are introduced.

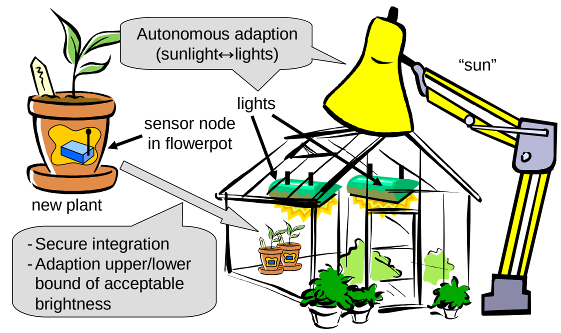

Fig. 1. Set-up of the demonstrator

SCAN is used for secure service discovery. SCAN uses a peer-to-peer (P2P) overlay network to store service descriptions under a service name. SCAN establishes and maintains security associations between overlay members. These associations allow for protection of integrity and confidentiality of service description records during the service discovery process. New nodes (e.g. a new plant in the greenhouse) get authenticated and authorized to join the overlay, and they get integrated into SCAN. The demonstrator shows the feasibility of P2P overlay networks on off-the-shelf sensor nodes.

The efficiency and scalability of both *Talassa* and *SCAN* in large sensor networks have been examined and proven by simulations. In this demonstration we show their feasibility on off-the-shelf hardware, their flexibility, and their practical use for distributed WSAN applications.

References

[1] B. Hurler, H.-J. Hof, and M. Zitterbart, *A General Architecture for Wireless Sensor Networks: First Steps*, 4th International Workshop on Smart Appliances and Wearable Computing, p. 442–444, Tokyo Japan, Mar 2004.

[2] H. -J. Hof and M. Zitterbart, *SCAN: A secure service directory for service-centric wireless sensor networks*, Computer Communications, vol. 28, no. 13, p. 1517–1522, ISSN 0140-3664, Elsevier, July 2005