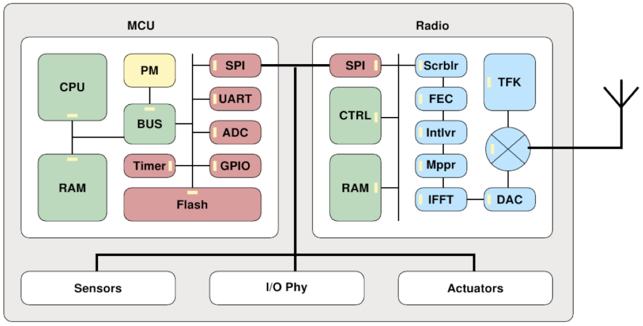
Federal University of Santa Catarina
Software/Hardware Integration Lab
http://www.lisha.ufsc.br/

SW-SoC - Energy-aware SoC for Secure WSN

SoCs for Wireless Sensor Networks



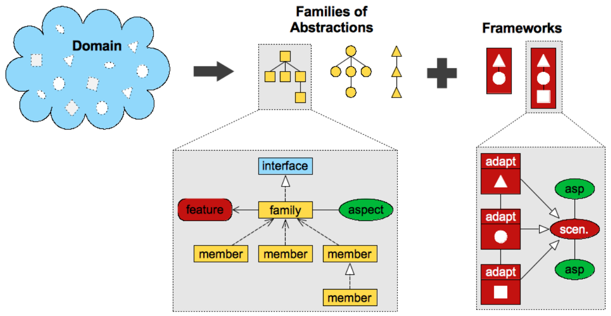
A wireless sensor network (WSN) is a communication network that comprises many autonomous computing devices. These devices equip with sensors, and cooperate to monitor physical, chemical and environmental properties in many strategic applications that require monitoring and control. As examples, one can cite weather and environment monitoring, oil's physical/chemical parameters monitoring, tracking and surveillance systems, precision farming applications, bio-medicine, military and aerospace applications, and so on. In a typical application, one can find many of these small devices spread on the observed environment, in order to gather relevant data.

Considering the design of these autonomous computing devices, the key technological elements are (a) communication protocols at MAC level; (b) strategies to manage energy consumption, specially for battery-powered devices; and (c) integration of device's components (e.g. processor, memory, sensors, and radio) into a single chip (System-on-Chip).

Towards Trustful Wireless Sensor Networks

The vision shared by the authors of this project is that there is a need to assure consumption of only the data that satisfy trust, security and privacy requirements for a given application. It is also desirable that this set of security requirements is defined around each application's needs and operation context. In order to target the envisioned scenario, two effort fronts were defined: (a) to build an infrastructure to implement the trust, security and privacy requirements for data collection from sensor networks; [1] and (b) to conceive a methodology to manage application requirements, device configurations, and context information. By the end of the project, the joint operation of the two research efforts shall make it possible to deploy a security solution tailored to match each application's requirements.

The ADESD Methodology



It is worth to mention that, depending on the application, different requirements will affect the wireless sensor system. In other words, depending on application requirements, one or more blocks may be removed from the device in order to optimize it for that given application. To allow this adaptability, the Application-Driven Embedded System Design (ADESD) will be used in the context of this project. [2]

The SW-SoC project

After adequately engineering the security domain, a tailorable secure communication framework shall be conceived. In order to tailor this framework to match scenarios of application requirements and contextual information, however, a consistent mapping methodology must be defined. This is where the ADESD methodology comes into play. ADESD's concepts of scenario adapters and configurable features will be extensively explored to build the tailorable secure communication framework. Finally, scenario adapters can be switched on and off, or configurable features' values changed, in order to adapt the system to applications's requirements to changes in the context. In the resultant system, energy-efficiency will be either addressed as an application requirement or as a context restriction, affecting the decision process during the adaptation phase.

1. REFERENCES

[1] A. A. Fröhlich, R. Steiner, and L. M. Rufino, "A Trustful Infrastructure for the Internet of Things based on EPOSMote," in *9th IEEE International Conference on Dependable, Autonomic and Secure Computing*, Sydney, Australia, Dec. 2011, pp. 63–68. [Online]. Available: http://www.lisha.ufsc.br/pub/Frohlich_DASC_2011.pdf

[2] A. A. Fröhlich, "Application-Oriented Operating Systems," Ph.D. dissertation, Technical University, Berlin, 2001, ph.D. Thesis.