Dealing with malicious behaviours in wireless sensor networks

Contact

Marin Bertier (marin.bertier@irisa.fr)
Anne-Marie Kermarrec (anne-marie.kermarrec@irisa.fr)

Research group

ASAP, INRIA Rennes / INRIA-Futurs, http://www.irisa.fr/asap. ASAP is a newly created research group, led by Anne-Marie Kermarrec, focusing on large-scale dynamic distributed systems. More specifically, we have a strong focus on peer to peer (P2P) and self-organizing systems ranging from abstractions and models to real implementations.
One of the main research axe of the ASAP research team focus on scalable algorithms for sensor networks. In this context, we have a strong collaboration with Rachid Guerraoui's group at EPFL (Lausanne, Switzerland) and the ARES research group at INRIA Rhone-Alpes. This proposal is funded through an INRIA ARC program, called Malisse for Malicious Sensors.

Context

Wireless sensor networks have recently received an increasing interest in many communities, way beyond the networking and signal processing areas. Wireless sensor networks provide a great infrastructure for many contemporary distributed applications. Many research groups are working for a few years on the design and implementations of distributed algorithms on such networks. More specifically, they are targeting data aggregation and how to make the aggregate traverse efficiently such a network. However, most of the proposed approaches rely on a simplifying assumption: they assume that the network is composed of reliable and well-behaved nodes, all collaborating with each other towards a common goal. We believe this is a paradox as sensor networks are precisely very often deployed in hostile environments.

The probability that some sensors are actually faulty is pretty high as well as the possibility of the presence of sensors exhibiting malicious behaviours. If the formers ones are sometimes considered, malicious behaviours are mostly ignored.

Objectives

We believe that for the sake of the credibility of wireless sensor networks and their applicability to a wide range of applications, they should be able to reliably support a number of key functionalities, even in the presence of malicious sensors. Obviously such algorithms need to be themselves adapted to sensor networks and more specifically should take into account sensors' reduced resources. The objective of this postdoctoral research is to consider the following basic functionalities in such a setting: (1) collection and aggregation of data observed in the sensor network and their routing to specific nodes; (2) generation and management of alerts when some of the observed measures reach a given threshold. Obviously, identifying the potential attacks in such a network is an important step of this research.

Expected outcomes should be both theoretical (algorithm design and proofs) and practical (simulation and implementation) in order to fully validate the proposed solutions.

Skills

We are seeking candidates with knowledge in distributed algorithms and networks, a solid theoretical background and programming skills.