Security Analysis of Sensor Networks

Roland Gémesi and László Zömbik

The development of wireless communication technologies and advances in embedded systems made it possible to build systems that interact with their physical environment and connect observations into a networked system. The growing level of integration and the decreasing cost of required units envision systems that contain a huge number of small units scattered in the environment.

In distributed sensor networks, sensors with integrated CPU, memory, battery and wireless communication units make it possible to distribute the common sensing and computing task. Units of sensor networks are usually heavily resource constrained, so the amount of computing, storage and communication tasks should be minimized. Since the nodes are very small and battery powered devices, operation of the participants is usually unreliable.

The large number of unreliable components call for a self organizing and fault tolerant architecture. Self organizing systems raise serious questions from the security point of view. The cooperation of nodes cannot be assumed, since malicious parties can easily get access to the wireless communication channels.

There are several solutions to achieve security in traditional networks, although those are usually not suitable for sensor networks. The security mechanisms designed especially for sensor networks have not been analysed exhaustively. Existing techniques for the analysis of security protocols usually cannot be used, sensor networks require a different approach.

An analysis technique is process algebra, which can be effectively used to model complex behaviour of distributed systems. The CSP (Communicating Sequential Processes) process algebra give the possibility to formalize systems that are composed from communicating distinct entities. With its help, several properties of distributed systems can be modelled and analysed. Security requirements of sensor networks can also be investigated in this framework.

In the presentation sensor networks and their security threats will be introduced. Fundamentals of the CSP process algebra will be shown to understand its modelling and analysis potential. Focusing on the security properties of distributed sensor networks, several modelling techniques will be presented. The presentation points out that the CSP process algebra can be a very effective framework to model and analyse distributed networks, such as sensor networks. Within this framework, analysis of proposed security protocols will be performed.