Survey of Security in Wireless Sensor Networks

SWITS 2011 – Andreas Larsson

A wireless sensor network is a network of small computers, sensor nodes, that can gather information via its sensors, do computations and communicate wirelessly with other sensor nodes. In general a wireless sensor network is an ad hoc network in which the nodes organize themselves without any preexisting infrastructure. Once in the area, the nodes that survived the deployment procedure communicate with the other nodes that happened to end up in its vicinity, and they set up an infrastructure.

Security is critical for many applications of sensor networks, just as for applications in other kinds of networks. Confidentiality and privacy is needed for sensitive, classified or proprietary information, e.g. medical data, sensitive information in civil security, industrial secrets or military information. It is important to be able to withstand attacks that aims to degrade the functionality of the network. Any kind of application can come under attack from someone that wants to disturb the network. For some applications it is critical to keep as much functionality as possible during an attack. Applications, e.g., that monitors restricted areas might have active attackers that have an interest in making the sensor network report erroneous information and the sensor network plays a critical role in maintaining security and/or safety of the facility.

Sensor networks are deployed in areas that is to be monitored. This usually implies that they are physically available for attackers. Furthermore, to feasibly deploy large number of nodes, they need to be inexpensive. Tamper-proof nodes are therefore often out of the question. The limitations in computing power, memory and battery makes many security algorithms inappropriate for use in sensor networks. This also limits the cryptography possibilities, especially for public key cryptography. Sensor networks often have very different traffic patterns than other networks. Information usually flows between the sensor nodes and the base station, or between nodes close to each other, but not between any pair of nodes in general. In addition, information is often aggregated on the way to decrease the total amount of needed traffic. The wireless medium makes it easy for an attacker to eavesdrop on the traffic, to jam communication or to inject messages into the network. This combination of circumstances that holds for many sensor networks opens up a set of security issues that needs to be considered. It also means that security protocols that are used in other networks, e.g. the Internet, are often not suitable at all for the sensor network setting.

We are working on a survey of security in wireless sensor networks. We aim to cover vulnerabilities and solutions for basic sensor network services and compenents as key management, encryption, authentication, integrity, intrusion/attack detection, routing, localization, aggregation, clock synchronization, clustering and power management.