Security in Wireless Sensor Networks

SWITS 2009 – Andreas Larsson

Security is important in many kinds of wireless sensor network applications, including:

- Sensor networks that monitor sensitive areas like harbors, airports and borders can have attackers that wants to avoid physical detection.
- Sensor networks that monitor structural integrity can have attackers that
- Sensor networks dealing with medical information can have attackers that wants to collect sensitive information.
- Any sensor network can have attackers that wants to disturb or sabotage the operation

In addition to the security concerns of wireless networks in general wireless sensor networks has a number of additional ones:

- The nodes in sensor networks are in general very limited in terms of battery, storage and computational power. Therefore strong cryptography and other general security tools are limited if at all available. An attacker can have much more powerful hardware than the nodes attacked.
- Sensor networks typically resides in unattended environments where an attacker can physically destroy nodes, add malicious nodes or in other ways tamper with the hardware of the network.
- Nodes in a sensor network dies of many different reasons. E.g. Battery can run out, nodes can break during deployment when they are thrown out from air or breaks during operation due to a harsh environment. It is hard to distinguish this from a malicious attack where nodes are deliberately destroyed

In a wireless sensor network the attacker can overwhelm the network or otherwise break designer assumptions of algorithms. To have long term security it is therefore important to have fault tolerance and/or self stabilization in conjunction with other security measures. If the network are not to withstand an attacker much more powerful than the nodes it should be able to get back to an operational state after an attacker has left the system.

We are looking into security with fault tolerance and self stabilization in mind. We have presented a secure and self-stabilizing clock synchronization algorithm and are working on secure and secure fault tolerant clustering.