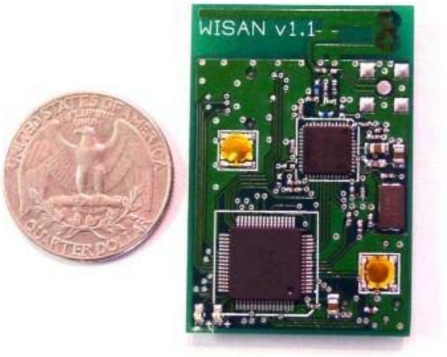
Project Description:

Sensor Networks

Application Scenario



A sensor network consists of many *sensor nodes*, which are typically small processors equipped with sensors and a radio interface. Sensor networks are mainly used for monitoring applications, such as environmental monitoring or military scenarios.

Sensor networks are sometimes created by scattering a large number of small inexpensive sensor nodes over a large area. Consider a sensor network that monitors temperature, oxygen levels and other factors that influence the fishing stocks in an archipelago. The sensor network may not be able to guarantee continuous connection back to the marine biologists, so local fishing boats are equipped with special mobile nodes that are only able to collect data from the small sensor nodes. Such mobile nodes are often called *data mule*s. In order to encrypt communication between the sensor nodes and the data mule, we need to establish a shared key between the two parties.

The sensor nodes have only very limited computational power and energy to spare for cryptographic purposes. On the other hand, there are no restrictions regarding the mules. Your task is to secure the data transmission between the node and the mule by choosing a suitable cryptography solution and key establishment mechanism that requires as little resources of the nodes as possible.

Project Definition

Design, evaluate and document a sensor node solution that addresses the issues presented by the scenario outlined above. Issues that *must* be addressed are:

- Risk analysis: What assets are at stake?
- Threat model: What assumptions do you make about the attacker(s), and what threats is your system supposed to protect against?
- Comparison: Examine a number of possible solutions with respect to the resources consumed. Important parameters in this investigation are the running time of the algorithms, the memory footprint of its implementation, power consumption and any special requirements on the processor hardware imposed by the proposed solution. The evaluation should consider as many of these parameters as possible.
- Security: Make sure that your system protects against the security issues raised in the threat model, and clearly document the threats that you do not protect against.