Kyle Marshall

Faculty Mentor: Dr. Zourntos
Department of Electrical Engineering
Texas A&M University

ABSTRACT

Wireless sensor networks are an emerging technology with numerous applications in many different fields. A network consists of sensors called motes whose job is to collect requested data and send into the network. Each mote plays the dual role of router and data collector. An ever-changing environment could cause motes to come in any out of contact and the network must be able to reconfigure itself on the fly. The motes though must be small to be cost effective and this requires small power storage. Therefore all processes of the motes must be highly optimize to conserve processor cycles and power.

Any network, especially one that uses wireless channels, must be security conscious. Due to the heavily limited processing and power of the motes, typical security protocols and algorithms simply do not apply; therefore, new strategies and implementations are needed. The wireless sensor network must be able to withstand several types of security attacks. One of the most important is proving that data on the network is actually from a "friendly mote". This is referred to as sensor authentication.

Since power is a heavy concern on mote design, a properly designed hardware implemented security feature would fare better than a software implementation. Using a new state of the art analog to digital (A/D) converter design, we propose adding security hardware components to encode an authentication into the digital bit stream. This would prevent attackers from trying to include a false mote into the network and also would make falsifying data more difficult. This method could increase die size but would save precious processor cycles.