NEST Hardware Limitations

A report based on the August 20, 2003 field experiment on
"A Line in the Sand"
by
The Ohio State University

August 27, 2003

We address here the question of specific hardware limitations somewhat broadly in that we interpret hardware to include various platform aspects of the NEST smart dust sensor networks. We also provide recommendations on how each limitation can be addressed.

- **Magnetometer –** OSU has observed that the magnetometers present on the MICA sensor boards become desensitized over time. One remedy is to include the set/reset circuitry needed to demagnetize them on an integrated sensor board. Alternatively, one could get better magnetometers that come equipped with such circuitry.

- **Micropower Impulse Radar (MIR) Interference –** The MIR units tend to interfere with each other at close range. These sensors should implement some form of dithering on the RF pulse and/or the timing of the pulses to prevent this kind of interference. An alternative strategy is to place the sensors with a minimum separation between each other. OSU has had success with separation greater than 8 ft. We believe that shorter separations are possible, although no extensive or documented testing of shorter separations has been performed.

- **MIR/Magnetometer Interference –** OSU observed non-deterministic interference between the MIRs and the magnetometers. In particular, we found that motes with magnetometer sensors which were executing the magnetometer signal chain only would not deterministically detect presence of metallic objects when an MIR sensor was mounted on them. We also found that motes with MIR sensors which were executing with MIR signal chain only suffered from eventual false negatives in the detection of moving objects. We have not as yet fully explained these observations.

- **Antennas –** OSU encountered many problems with our antennas. Graduate students did not have access to the tools (crimping equipment, etc.) or have the experience to assemble antennas that require careful placement and soldering of small parts. In the final analysis, OSU decided to remove all antennas that used the MMCX connectors and replace them with antennas soldered directly to the MICA2 boards. However, even these antennas would occasionally be bent and break off, requiring desoldering of the remnants and resoldering of a new antenna – a process that sometimes permanently damaged the MICA2 boards.

- **Ground Absorption –** Both the radio transmission range and the micropower impulse radar (MIR) detection range are severely affected by ground absorption effects. OSU obtained acceptable performance by placing the MIR sensors 3” or more above ground. OSU also tuned the power level of radio transmission carefully to satisfy two sided constrains: on one hand, to compensate for ground absorption and on the other hand to avoid excessive interference between motes that are not logical neighbors.

- **Communications and Routing –** Communications and routing in dense multi-hop mesh networks remains an unsolved problem in practice. OSU’s experience in this area indicates that there are complex interactions and interference ranges that exceed far beyond the useful transmission capability of the radios. Approaches to circumvent this problem include power level management, reduced communications, *in situ* aggregation, and reliable communication schemes. To address the problem of *reliable and scalable routing* well, much more significant work is needed in gathering and analyzing traffic and fault data.

- **Byzantine Behavior –** Occasionally, some motes exhibited Byzantine behavior. Note the Byzantine behavior can be caused by low batteries (as we encountered innumerable times) so Byzantine behavior is not just an academic concern. Byzantine behavior is also sometimes caused by incorrect wireless programming of the motes, even though it would appear that the mote had successfully completed its task in a wireless download. As another example, sensor board debonding was observed to cause continuous false alarm at a rates of 50+ incorrect detections *per second*. To handle these kinds of problems, OSU built a regulator service that would cap the maximum number of messages a sensor could transmit. In the general case, attention needs to be given to analyzing and handling Byzantine behavior. For example, if multiple sensors conclude that another sensor has become Byzantine, they may choose to suppress the Byzantine node’s communications.

- **Sensor Board Debonding –** Our sensors currently are implemented using multiple separate circuit boards that are friction-fit connected. In addition, these MICA2 form-factor boards provide mounting holes that can be used with standoffs to “bolt” the boards together. Both false positives and false negatives should be expected when debonding occurs. However, Ohio State’s experience indicates that even these bolts are not sufficient to keep the boards from becoming loose (“debonding”). In the future, hardware better engineered for positive lock mounting *or* a single integrated sensor/computer/communicator board should be used to address sensor board debonding.

- **Network Reprogramming –** A *secure*, *reliable*, and *multi-hop* network reprogramming model and implementation is required for research efficacy and eventual in-network re-tasking. In the current implementation of XNP, security is completely unsupported. In this case, we would like security to include two-way authentication and data confidentiality. Security is required for the usual reasons of avoiding unintended or unauthorized reprogramming of the motes. Reliability, while present in XNP in the form of packet retransmissions, is not robust. Many motes required hand reprogramming even though no “official” errors were reported. The exact sources of these problems remain unknown but the use of improved cyclic redundancy check (CRC) and forward error correction (FEC) algorithms is likely to reduce the problems. Finally, one significant weakness of XNP is that it only works over a single hop in a broadcast transmit and unicast retransmit manner.

- **Event Loss or Interference in TinyOS –** OSU observed certain events getting lost/not occurring in TinyOS. It is not yet clear whether this is due to bugs (*e.g.* port mapper problem in TinyOS) or something else like failing to check the return status of a call (*e.g.* FAIL vs. SUCCESS). There is role for stabilization to play in the face of event losses, etc. Self-stabilizing code can return the system to a known good state in the presence of state corruption. Another TinyOS lesson that we learned was to keep event handlers as short as possible and make judicious use of tasks and atomic blocks. For example, our initial TimeSync and MIR code event handlers were too long and caused many problems with one event overwriting the state of the previous event. Unfortunately, we are not aware of a tool that can determine whether a program can be executed successfully on the mote.

- **Overheating –** During the August experiments and demonstrations at MacDill AFB in Tampa, FL, OSU discovered that many sensors displayed reduced performance when exposed to heat for extended periods of time. In particular, both the magnetometer *and* MIR sensors that were sitting on the sand near the tree line demonstrated significantly reduced sensitivity. OSU found that power-cycling the sensors and recollecting the MIR sensors to a cooler (shady) area often fixed the problem. In addition, the batteries became extremely hot and in some cases were too hot to handle with bare hands. We feel that at these heat levels, there is some danger of battery explosion.

Minor Issues:

- **Batteries** – OSU encountered some minor mechanical problems with the batteries. We discovered that certain Duracell batteries are designed in such a way that when used with the MICA2 battery holders, the positive terminal of the battery *fails* to touch the metal contact and therefore doesn’t complete the circuit.

- **Rain** – While our sensors continued to work in the presence of drizzling rain, our enclosures were not *highly* robust to the heavy rain. In one case, a mote “burned up” or “smoked” and no longer worked after being subject to some rainwater. This would have been avoided had our enclosures been sealed.

- **Relay –** OSU used a 900MHz spread spectrum set of radios with longer range than the Chipcon radios to connect the base stations to the monitoring station. While functional, this configuration was not ideal and we encountered many small hardware/connectivity problems.

- **Operator error –** Human error (*e.g.* downloading the wrong programs by accident). Hard to avoid!