

Networked Embedded Systems: From Sensor Webs to Cyber-Physical Systems

Shankar Sastry

University of California at Berkeley - Berkeley, CA, USA

Abstract. There has been a great deal of excitement in recent years concerning the evolution of sensor webs of smart dust. There has been a very substantive active world wide in this area and in particular at Berkeley there have now been over six generation of "motes" for these sensor webs, and at least three new start ups have arisen to commercialize these developments. I will survey these developments and where they have brought us in a very important new class of computing involving an integration of communication and computing. I will describe how the technology push is matched by the applications pull on numerous different applications.

Throughout the talk, I will highlight the efforts of my group and that of my colleagues especially Culler, Pister, Wagner and Brewer in "closing the loop" around these networked embedded systems. We believe that this closing the loop brings into sharp focus the real time constraints and issues inherent in the use of networked embedded systems. Further, the most important new directions in sensor webs involve this new direction beyond simply sensing and monitoring the physical environment and infrastructure. In particular, I will describe the range of methods and algorithms needed to track multiple targets in a sensor web and to be able to pursue them. The culmination of this project was a 557 node demonstration that we conducted at the Richmond Field Station in August 2005. Some areas of future development in sensor networks involve the use of high bandwidth sensors (such as camera motes) and mobile sensor webs. I will give a preview of some of the most exciting opportunities in this regard.

Finally, with our increase dependency on computing and communication to instrument physical infrastructures, such as electric power, water, gas, etc. we find that they are not high confidence: that is they are complex systems which may not be correct by construction, or fault tolerant and are vulnerable to information attack of networked embedded systems. Such systems are being referred to as high confidence cyber physical systems. To address this grand challenge societal problem of building high confidence cyber physical systems, I will give a snap shot of the kinds of techniques with, privacy and policy work, in the area of secure network embedded systems.