REPORT DOCUMENTATION PAGE

AFRL-SR-AR-TR-02-

0264

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
22-07-2002	Final Technical Report	June 2000-Deecember 2001

4. TITLE AND SUBTITLE

Instrumentation for Wireless Agent Networks and Sensor Webs

5a. CONTRACT NUMBER

5b. GRANT NUMBER
F49620-00-1-0212

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

George Cybenko, Dorothy and Walter Gramm Professor of Engineering

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Thayer School of Engineering   Hanover NH 03755
Dartmouth College

8. PERFORMING ORGANIZATION REPORT NUMBER

536237 Final Tech. Report

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Office of Scientific Research   801 N. Randolph St.
Arlington, VA 22203-1977

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR-NM

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY ST

Distribution unlimited

DISTRIBUTION STATEMENT A:
Approved for Public Release -
Distribution Unlimited

20020909 114

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Instrumentation for three types of wirelessly networked systems was requested and acquired in this project in order to extend the experimental capabilities of several existing and proposed defense research efforts. The three types of networks and the work they enabled are:

- 50 IEEE 802.11 wirelessly networked PC's - to support fundamental scalability studies of ad hoc wireless networks and larger-scale performance experiments of mobile agent systems;
- 50 IEEE 802.11 wirelessly networked palm or handheld PC's - for scalability studies of end-user performance, ad hoc networking and collaborative mission-oriented agent systems using smaller, lighter and limited-functionality computing devices;
- COT's components - for 100 wirelessly networked, lightweight computing and sensory devices to begin experimentation with the networking paradigms for and capabilities of wirelessly connected commodity sensors that can self-organize into a "smart sensor web."

Miscellaneous supporting equipment, supplies and development software were also requested and acquired.

15. SUBJECT TERMS

Wireless networks, IEEE 802.11, command and control, remote sensing, sensor grids.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					George Cybenko
a. REPORT	b. ABSTRACT	c. THIS PAGE	None	4	19b. TELEPHONE NUMBER (include area code)
Unclassified	Unclassified	Unclassified			603 646-3843

FINAL TECHNICAL REPORT OF AFOSR GRANT F49620-00-1-0212

Title: Instrumentation for Wireless Agent Networks and Sensor Webs

PI: Professor George Cybenko, Dartmouth College, Hanover NH 03755

This grant supported the acquisition of equipment suitable for experimental studies of various types of wireless networks. Of particular interest are the wireless sensor platforms, shown below, for experimenting with a variety of routing, power consumption, sensor types and markup languages in a real experimental laboratory setting. The basic element is a single module.

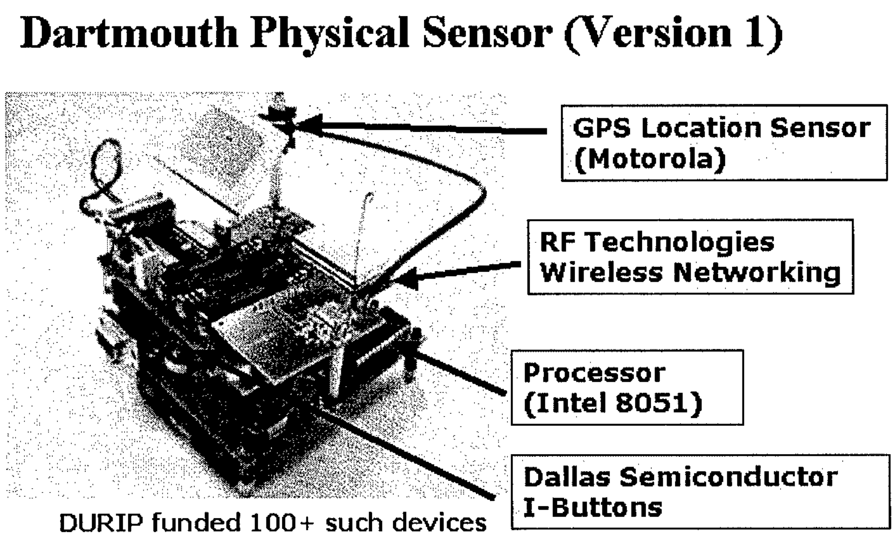

Figure 1: Dartmouth Physical Sensor Module, first version

As depicted above, all modules are identical, containing the same hardware and software features. Which of these features are utilized depends on the Module's current state: Module or Hub. Regardless of current state value, each Module consists of a microprocessor and integrated circuitry for controlling the functionality of the module. The main purpose of the Module is to collect and store weather data using the iButton Weather Station tools, developed by Dallas Semiconductors [1]. Because the modules can potentially be placed anywhere, some sort of positioning equipment is required. For this, a standard GPS receiver is employed.

Once the Module has collected a sufficient amount of data, the Module relinquishes the information via wireless transmission. This is accomplished with an RF transmitter and receiver (transceiver). (See Figure 2).

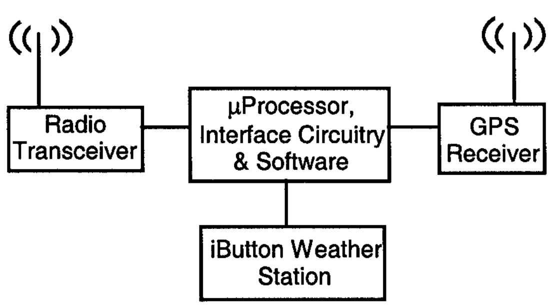

Figure 2.

The span of the network may at times be larger than the transmission range of a single module. Therefore, in order for each module to remain in contact with each other, transmissions will need to "hop" from one module to another, until the message reaches its intended receiver. Thus, each module must behave as a *Router* and requires the proper software and hardware to do so.

Each module is equipped with intelligence for self system monitoring. For example, a simple scheme is used to monitor memory storage space. As the collected weather data fills the on board memory allocation, the Module is responsible for detecting potential overflows and disposing of the data properly. The Module can erase the data, transmit it to Home, or transmit it to another Module with available memory space.

Another issue of importance is the self monitoring of a Module's position. If a Module is moving, it must be aware of the distance and directional relationship to its surrounding Modules. This idea adds several beneficial features. First, it prevents a Module from traveling too far out of transmission range. Second, if a Module is leaving one cell range and entering another, it must recognize this and update its Hub transmission path (i.e. Cellular Mobility).

An effective way to implement this *Neighborhood Monitoring* scheme is through the use of software *Agents*. Once a Module begins moving, it can generate and send an agent over the network to determine which other Modules are nearby. Once the task is completed, the agent will return to the original Module with the necessary information. This technique eliminates the need for constant RF polling by the Module to find out who its neighbors are, thereby reducing processor power consumption and network bandwidth.

This Neighborhood Monitoring method can also be used to optimize the positioning of the mobile Module. By spacing the Modules effectively, data may be collected more efficiently.

A unique name or address is used to identify each Module. A simple addressing solution would be to use an individual static IP address for each Module. However, by using a dynamic addressing scheme, more information about the Module can be collected. If the IP address is composed of its GPS coordinates and a timestamp, each Module will have a unique identifying label since no two modules can be in the same place at the same time. This IP addressing scheme gives instant information about the Module (position and time). Following this idea, as the Module moves, it will need to continuously update its IP address with the new location coordinates and time. Without proper handling, this idea could lead to an unstable network.

To maintain the dynamic IP addresses, each Module is responsible for sending its new IP address to its local Hub. The Hub contains a *Mapping Table* to map the dynamic address with a static address previously assigned to each Module by the network administrator. This helps prevent an administrator/user from worrying about the changing addresses.

The Hub is in actuality a Module, but is given a higher status, granting it permission to use extended features. The Hub is responsible for the communication link between Home and the individual Modules in its cell range. The Hub is also responsible for maintaining the mapping table for the Module identification information. Based on the topology of the network (number and relative distance of modules), the number of Hubs will be selected. A Module can be promoted or demoted between Hub status and Module status at any time. If a Module is demoted from Hub status, it must transfer all unsent data packets and the Mapping Table to the nearest Hub, or new replacement Hub. Dynamically allocated Hubs within a network adds to the robustness of the communication scheme. It allows the network to expand or contract seamlessly.

The Hub is also responsible for controlling the network bandwidth. Through the use of filters, the Hub is equipped with the capability of filtering out superfluous or redundant data packets received. If a Module is continually sending similar data packets, the Hub may refuse to forward the packets Home. Network congestion can be a serious problem so it is important to utilize a protocol to minimize radio transmissions.

The Home terminal is maintained and controlled by a user. It can be either a desktop computer workstation, or a laptop terminal. A Home is equipped with an adequate RF transceiver package and proper software utilities for communication and control of the wireless Modules. The user is able to communicate with any individual Module using a Web Browser and an IP addressing identification scheme.

This work has had impact on several DOD and DOD-related research projects. Those projects are listed below.

AFOSR 1997 MURI – The ActComm Project: Transportable Agents for Wireless Networks

PI:	George Cybenko
Co-PI's:	D. Kotz, D. Rus, H.T. Kung, T. Basar, P.R. Kumar, K. Vastola, K. Whitebread, E. Entin
Prime:	Dartmouth
Subs:	Harvard, RPI, University of Illinois at Urbana-Champaign, ALPHATECH Inc., Lockheed Martin ATL
Duration:	June 1997 to May 2002
Agency:	AFOSR
Contact:	Dr. Robert Herklotz, AFOSR-NM

AFOSR-IF Workshop on Infospheric Science

PI:	David Kotz
Co-PI's:	None
Prime:	Dartmouth
Subs:	None
Duration:	May 2001 to December 2002
Agency:	AFOSR
Contact:	Dr. Robert Herklotz, AFOSR-NM

DARPA CoABS Program – Resource Control for Large-Scale Agent Systems

PI:	David Kotz
Co-PI's:	D. Rus, R. Gray, G. Cybenko
Prime:	Dartmouth
Subs:	None
Duration:	May 1998 to October 2002
Agency:	DARPA via Rome Labs
Contact:	Dr. Dylan Schmorrow, DARPA

DARPA TASK Program - Agent-Based Systems Engineering

PI:	G.Cybenko
Co-PI's:	D. Rus
Prime:	Dartmouth
Subs:	None
Duration:	AUgust 2000 to October 2004
Agency:	DARPA via Rome Labs
Contact:	Dr. Gary Koob, DARPA

Next-Generation Agent-Based Distributed Simulation

PI:	Linda Wilson
Co-PIs:	G. Cybenko, D. Lynch, B. Szymanski, B. Cushman-Roisin
Prime:	Dartmouth
Subs:	RPI
Duration:	October 1998 to September 2002
Agency:	National Science Foundation
Contact:	Dr. Richard Hilderbrandt, rhilderb@nsf.gov

Investigative Research for Infrastructure Assurance

PI:	G. Cybenko
Co-PIs:	R. Gray, S. McGrath
Prime:	Dartmouth
Subs:	Stanford, Michigan, Mitretek, Tulsa, Sandia, Harvard
Duration:	October 2000 to January 2002
Agency:	National Institute of Justice
Contact:	Dr. John Hoyt, NIJ, Department of Justice