ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORT

Available Online at www.ijarcs.info

Case study: Wireless Sensor Networks Technology

Naveen Jain
Department of Electronics & communication
Geetanjali Institute of Technical Studies Udaipur.
naveenjain30@gmail.com

Pawan Shakdwipee
Department of Electronics & communication
Arya College of Engg. & IT Jaipur,
pawan21_uda@yahoo.co.in

Sunil Sharma
Department of Electronics & communication
Arya College of Engg. & IT Jaipur,
ersharma.sunil@gmail.com

***Abstracr*:** This paper present the history of research in sensor networks over the past decades, including two important programs of the Defense Advanced Research Projects Agency (DARPA), and the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SensIT) programs. Technology trends that impact the development of sensor networks are reviewed, and new applications such as infrastructure security, habitat monitoring. The paper concludes by presenting some recent case studies results in sensor network algorithms, including localized algorithms and directed diffusion, distributed tracking in wireless ad hoc networks, and distributed classification using local agents.

***Keywords*—** wireless sensor networks; enabling technologies; applications signal processing, micro sensors, net- work routing and control, querying and tasking, sensor networks, tracking and classification, wireless networks

I. INTRODUCTION

This paper provides a survey of WSNs technologies, main applications and standards, features in WSNs design with case study, and evolutions.Networked micro sensors technology is a key technology for the future. Cheap, smart devices with multiple onboard sensors, networked through wireless links and the Internet and deployed in large numbers, provide unprecedented port unities for instrumentings and controlling homes, cities, and the environment. Micro sensors provide the technology for a broad spectrum of systems in the defense arena, generating new capabilities..

Networked micro sensors relate to the general family of sensor networks that use multiple distributed sensors to col- lect information on entities of interest. Military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, distributed robotics, environment monitoring, and building and structures monitoring. The sensors in these applications may be small or large, and the networks may be wired or wireless. The sensor networks for various applications may be quite different, they share common technical issues. It presents a history of research in sensor networks, technology trends, new applications, research issues and hard problems and some examples of case study results.

II. SENSOR NETWORKS IN RESEARCH

The sensor networks requires technologies from three different research areas: sensing, communication, and computing.

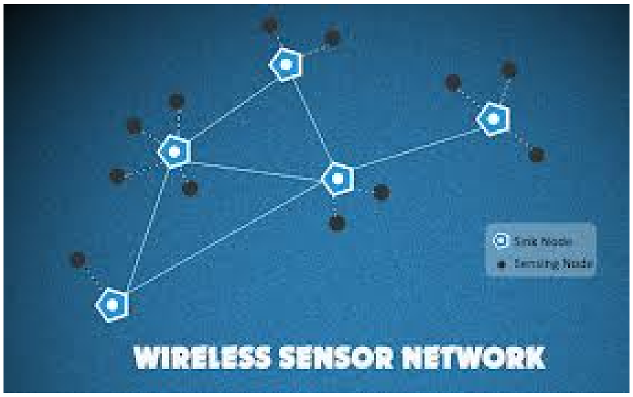


Figure 1. Interconnection of WSN

The combined and separate advancements in each of these areas have driven case study in sensor networks. Examples of early sensor networks include the radar net- works used in air traffic control. The national power grid, with its many sensors, can be viewed as one large sensor net- work. These systems were developed with specialized computers and communication capabilities, and before the term “sensor networks” came into news As with many technologies, defense applications have been a driver for research and development in sensor net- works. During the Cold War, the Sound Surveillance System (SOSUS), a system of acoustic sensors (hydrophones) on the ocean bottom, was deployed at strategic locations to detect and track quiet Soviet submarines. Over the years, other more sophisticated acoustic networks have been developed for submarine surveillance. SOSUS is now used by the National Oceanographic and Atmospheric Administration (NOAA) for monitoring events in the ocean, e.g., seismic and animal activity [3]. Also during the Cold War, networks of air defense radars were developed and deployed to defend the continental United States and Canada. This air defense system has evolved over the years to include aerostats as sensors and Airborne Warning and Control System (AWACS) planes, and is also used for drug interdiction.

These sensor networks generally adopt a hierarchical processing structure where processing occurs at consecutive levels until the information about events of interest reaches the user. In many cases, human operators play a key role in the system.

A. Distributed Sensor Networks Program at the Defense Advanced Research Projects Agency:

Modern research on sensor networks started around 1980 with the Distributed Sensor Networks (DSN) program at the Defense Advanced Research Projects Agency (DARPA). By this time, the Arpanet (predecessor of the Internet) had been operational for a number of years, with about 200 hosts at universities and research institutes. R. Kahn, who was coinventor of the TCP/IP protocols and played a key role in developing the Internet, was director of the Information Processing Techniques Office (IPTO) at DARPA. He wanted to know whether the Arpanet approach for communica- tion could be extended to sensor networks. The network was assumed to have many spatially distributed low-cost sensing nodes that collaborate with each other but operate autonomously, with information being routed to whichever node can best use the information.

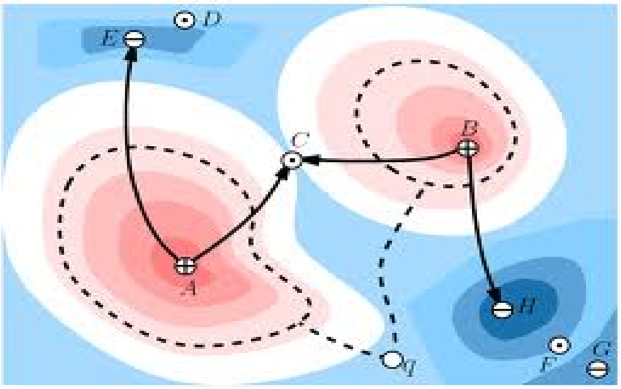


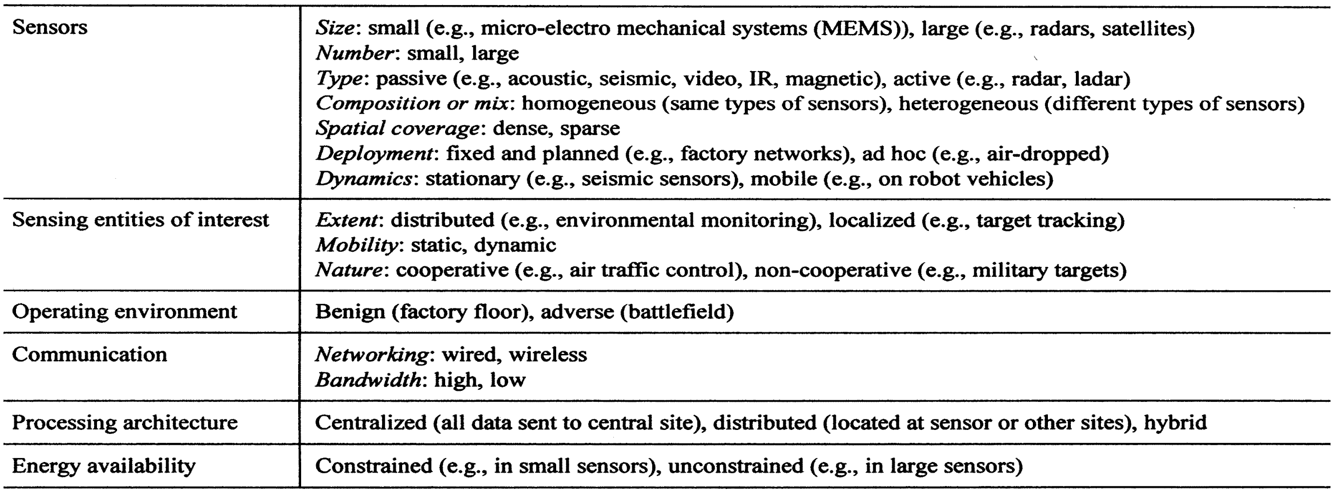
Figure 2 Distributed Sensor Networks

It was an ambitious program given the state of the art. This was the time before personal computers and workstations; processing was done mostly on minicomputers such as PDP-11 and VAX machines running Unix and VMS. Modems were operating at 300 to 9600 Bd, and Ethernet was just becoming popular.

Technology components for a DSN were identified in a Distributed Sensor Nets workshop in 1978. These included sensors (acoustic), communication (high-level proto- cols that link processes working on a common application in a resource-sharing network , processing techniques and algorithms (including self-location algorithms for sen- sors), and distributed software (dynamically modifiable dis- tributed systems and language design). Since DARPA was sponsoring much artificial intelligence (AI) research at the time, the workshop also included talks on the use of AI for understanding signals and assessing situations, as well as various distributed problem-solving techniques. Since very few technology components were available off the shelf, the resulting DSN program had to address distributed computing support, signal processing, tracking, and test beds. Distributed acoustic tracking was chosen as the target problem for demonstration.

Researchers at Carnegie Mellon University (CMU), Pittsburgh, PA, focused on providing a network operating system that allows flexible, transparent access to distributed resources needed for a fault-tolerant DSN. They developed and tracking performance through multiple observations, geometric and phenomenological diversity, extended detec- tion range, and faster response time. Also, the development cost is lower by exploiting commercial network technology and common network interfaces.An example of network-centric warfare is the Cooperative Engagement Capability (CEC) developed by the U.S. Navy. This system consists of multiple radars collecting data on air targets. Measurements are associated by a processing node "with reporting responsibility" and shared with other nodes that process all measurements of interest. Since all nodes have access to essentially the same information, a "common operating picture"

Table 1: Investigations of Sensor Networks



Sensors	***Size*: small (e.g., micro-electro mechanical systems (MEMS)), large (e.g., radars, satellites)** ***Number*: small, large** ***Type*: passive (e.g., acoustic, seismic, video, IR, magnetic), active (e.g., radar, ladar)** ***Composition or mix*: homogeneous (same types of sensors), heterogeneous (different types of sensors)** ***Spatial coverage*: dense, sparse** ***Deployment*: fixed and planned (e.g., factory networks), ad hoc (e.g., air-dropped)** ***Dynamics*: stationary (e.g., seismic sensors), mobile (e.g., on robot vehicles)**
Sensing entities of interest	***Extent*: distributed (e.g., environmental monitoring), localized (e.g., target tracking)** ***Mobility*: static, dynamic** ***Nature*: cooperative (e.g., air traffic control), non-cooperative (e.g., military targets)**
Operating environment	**Benign (factory floor), adverse (battlefield)**
Communication	***Networking*: wired, wireless** ***Bandwidth*: high, low**
Processing architecture	**Centralized (all data sent to central site), distributed (located at sensor or other sites), hybrid**
Energy availability	**Constrained (e.g., in small sensors), unconstrained (e.g., in large sensors)**

Essential for consistent military operations is obtained. Other military sensor networks in- clude acoustic sensor arrays for antisubmarine warfare such as the Fixed Distributed System (FDS) and the Advanced Deployable System (ADS), and unattended ground sensors (UGS) such as the Remote Battlefield Sensor System (REMBASS) and the Tactical Remote Sensor System (TRSS).

B. Sensor Network Research in the 21st Century:

Recent advances in computing and communication have caused a significant shift in sensor network research and brought it closer to achieving the original vision. Small and inexpensive sensors based upon microelectromechanical system (MEMS) technology, wireless networking, and inexpensive low-power processors allow the deployment of wireless ad hoc networks for various applications. Again, DARPA started a research program on sensor networks to leverage the latest technological advances.

The recently concluded DARPA Sensor Information Technology (SensIT) program pursued two key research and development thrusts. First, it developed new networking techniques. In the battlefield context, these sensor devices or nodes should be ready for rapid deployment, in an *ad hoc* fashion, and in highly dynamic environments. Today's networking techniques, developed for voice and data and relying on a fixed infrastructure will not suffice for battlefield use. Thus, the program developed new networking techniques suitable for highly dynamic *ad hoc* environments. The second thrust was networked information processing, i.e., how to extract useful, reliable, and timely information from the deployed sensor network. This implies leveraging the distributed computing environ- ment created by these sensors for signal and information processing in the network, and for dynamic and interactive querying and tasking the sensor network.

SensIT generated new capabilities relative to today's sensors. Current systems such as the Tactical Automated Security System (TASS) for perimeter security are dedicated rather than programmable. They use technologies based on transmit-only nodes and a long-range detection paradigm. SensIT networks have new capabilities. The networks are interactive and programmable with dynamic tasking and querying. A multitasking feature in the system allows multiple simultaneous users. Finally, since detection ranges are much shorter in a sensor system, the software and algorithms can exploit the proximity of devices to threats to drastically improve the accuracy of detection and tracking. The software and the overall system design supports low latency, energy-efficient operation, built-in autonomy and survivability, and low probability of detection of operation. As a result, a network of SensIT nodes can support detection, identification, and tracking of threats, as well as targeting and communication, both within the network and to outside the network, such as an overhead asset.

III. TECHNOLOGY TRENDS

Current sensor networks can exploit technologies not available 20 years ago and perform functions that were not even dreamed of at that time. Sensors, processors, and communication devices are all getting much smaller and cheaper. Commercial companies such as Ember, Crossbow, and Sensoria are now building and deploying small sensor nodes and systems. These companies provide a vision of how our daily lives will be enhanced through a network of small, embedded sensor nodes. In addition to products from these companies, commercial off-the-shelf personal digital assistants (PDAs) using Palm or Pocket PC operating systems contain significant computing power in a small package.

These can easily be "ruggedized" to become processing nodes in a sensor network. Some of these devices even have built-in sensing capabilities, such as cameras. These powerful processors can be hooked to MEMS devices and machines along with extensive databases and communication platforms to bring about a new era of technologically sophisticated sensor nets.

Wireless networks based upon IEEE 802.11 standards can now provide bandwidth approaching those of wired networks. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer. The organization has defined the IEEE 802.15 standard for personal area networks (PANs), with "personal net- works" defined to have a radius of 5 to 10 m. Networks of short-range sensors are the ideal technology to be employed in PANs. The IEEE encouragement of the development of technologies and algorithms for such short ranges ensures continued development of low-cost sensor nets. Further- more, increases in chip capacity and processor production capabilities have reduced the energy per bit requirement for both computing and communication. Sensing, computing, and communications can now be performed on a single chip, further reducing the cost and allowing deployment in ever larger numbers.

Looking into the future, we predict that advances in MEMS technology will produce sensors that are even more capable and versatile. For example, Dust Inc., Berkeley, CA, a company that sprung from the late 1990s Smart Dust research project at the University of California, Berkeley, is building MEMS sensors that can sense and communicate and yet are tiny enough to fit inside a cubic millimeter. A Smart Dust optical mote uses MEMS to aim submillimeter-sized mirrors for communications. Smart Dust sensors can be deployed using a 310 mm "wavelet" Shaped like a maple tree seed and dropped to float to the ground. A wireless network of these ubiquitous, low-cost, disposable micro sensors can provide close-in sensing capabilities in many novel applications.

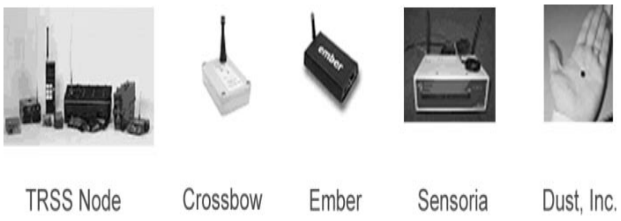


Figure 3. Three generations of sensor nodes.

Table compares three generations of sensor nodes; Fig. 3 shows their sizes.

IV. RECENT APPLICATIONS

The sensor networks was originally motivated by military applications. Examples of military sensor networks range from large-scale acoustic surveillance systems for ocean surveillance to small networks of unattended ground sensors for ground target detection. However, the availability of low-cost sensors and communication networks has resulted in the development of many other potential applica- tions, from infrastructure security to industrial sensing. The following are a few examples.

A. *Infrastructure Security:*

Sensor networks can be used for infrastructure security and counterterrorism applications. Critical buildings and facilities such as power plants and communication centers have to be protected from potential terrorists. Networks of video, acoustic, and other sensors can be deployed around these facilities. These sensors provide early detection of possible threats. Improved coverage and detection and a reduced false alarm rate can be achieved by fusing the data from multiple sensors.

Even though fixed sensors connected by a fixed communication network protect most facilities, wireless ad hoc networks can provide more flexibility and additional coverage when needed. Sensor networks can also be used to detect biological, chemical, and nuclear attacks. Examples of such networks can be found in, which also describes other uses of sensor networks.

B. *Environment and Habitat Monitoring:*

Environment and habitat monitoring is a natural candidate for applying sensor networks, since the variables to be monitored, e.g., temperature, are usually distributed over a large region. The recently started Center for Embedded Net- work Sensing (CENS), Los Angeles, CA, has a focus on environmental and habitat monitoring. Environmental sen- sors are used to study vegetation response to climatic trends and diseases, and acoustic and imaging sensors can identify, track, and measure the population of birds and other species. On a very large scale, the System for the Vigilance of the Amazon (SIVAM) provides environmental monitoring, drug trafficking monitoring, and air traffic control for the Amazon Basin. Sponsored by the government of Brazil, this large sensor network consists of different types of intercon- nected sensors including radar, imagery, and environmental sensors. The imagery sensors are space based, radars are lo- cated on aircraft, and environmental sensors are mostly on the ground. The communication network connecting the sen- sors operates at different speeds. For example, high-speed networks connect sensors on satellites and aircraft, while low-speed networks connect the ground-based sensors.

C. *Industrial Sensing:*

Several years ago, the IEEE and the National Institute for Standards and Technology (NIST) launched the P1451Smart Transducer Spectral sensors are one example of sensing in an industrial environment. From simple optical devices such as obtrudes and pH probes to true

a. *Ad Hoc Network Discovery:*

In the case of a mobile network, since the topology is always evolving, mechanisms should be provided for the dif- ferent fixed and mobile sensors to discover each other. Global knowledge generally is not needed, since each sensor node interacts only with its neighbors. In addition to knowledge of the topology, each sensor also needs to know its own lo- cation.

When self-location by GPS is not feasible or too expensive, other means of self-location, such as relative po- sitioning algorithms, have to be provided.

b. *Network Control and Routing:*

This requires research into issues such as network size or the number of links and nodes needed to provide adequate redundancy. Also, for networks on the ground, RF transmission degrades with distance much faster than in free space, which means that communication distance and energy must be well managed. Protocols must be internalized in design and not require operator intervention.

Alternative approaches to traditional Internet methods [such as Internet Protocols (IP)], including mobile IP, are needed. One of the benefits of not requiring IP addresses at each node is that one can deploy network devices in very large numbers. Also, in contrast to the case of IP, routes are built up from geo information, on an as-needed basis, and optimized for survivability and energy. This is a way to form connections on demand, for data-specific or application-specific purposes. IP is not likely to be a viable candidate in this context, since it needs to maintain routing tables for the global topology, and because updates in a dynamic sensor network environment incur heavy overhead in terms of time, memory, and energy.

c. Collaborative Signal and Information Processing:

Important technical issues include the degree of information sharing between nodes and how nodes fuse the information from other nodes. Processing data from more sensors generally results in better performance but also requires more communication resources (and, thus, energy). Similarly, less information is lost when communicating information at a lower level (e.g., raw signals), but requires more bandwidth.

Therefore, one needs to consider the multiple tradeoffs between performance and resource utilization in collaborative signal and information processing using micro sensors.

Again there is a tradeoff between performance and robustness. Simple fusion rules are robust but suboptimal while more sophisticated and higher performance fusion rules may be sensitive to the underlying models. In a networked environment, information may arrive at a node after traveling over multiple paths. The fusion algorithm should recognize the dependency in the information to be fused and avoid double counting. Keeping track of data pedigree is an approach used in networks with large and powerful sensor nodes, but this approach may not be practical for ad hoc networks with limited processing and communication resources.

These algorithms must be asynchronous, as the processor speeds and communication capabilities may vary or even disappear and reappear. Sensor nodes must determine results with progressively increasing accuracy, and so the processes can be terminated when enough precision is gained.

d. Querying:

These features render the database view more challenging, particularly for military applications given the low-latency, real-time, and high-reliability requirements of the battlefield. An example of a human-network interface is a handheld unit that accepts speech input. The users should be able to command access to information, e.g., operational priority and type of target, while hiding details about individual sensors.

Mobile platforms can carry sensors and query devices. As a result, seamless internetworking between mobile and fixed devices in the absence of any infrastructure is a critical and unique requirement for sensor networks. For example, an air- borne querying device could initiate a query, and then tell the ground sensor network that it will be flying over a specific location after a minute, where the response to the query should be exfiltrated.

e. Security:

Since the sensor network may operate in a hostile environment, security should be built into the design and not as an afterthought. Network techniques are needed to provide low-latency, survivable, and secure networks. Low probability of detection communication is needed for net- works because sensors are being envisioned for use behind enemy lines. For the same reasons, the network should be protected again intrusion and spoofing.

Case Studies Results:

The following are examples of some recent research results.

A. Localized Algorithms and Directed Diffusion:

As discussed previously, even though centralized algorithms that collect data from multiple sensor nodes can potentially provide the best performance, they are undesirable because of high communication cost and lack of robustness and reliability. In localized (or distributed) algorithms, the sensor nodes only communicate with sensors within a neighborhood. Localized algorithms are attractive because they are robust to network changes and node failures. The communication cost also scales well with increasing network size.

For instance, simulation and experimental results of directed diffusion in representative sensor networks indicate that multicast protocols (such as omniscient multicast, which is an IP-based multicast routing technique) re- quires less than half the energy required for flooding, and diffusion requires only 60% of the energy needed for even multicast. These savings are achieved by eliminating paths spent delivering redundant data, and from in-network aggregation such as through intermediate nodes suppressing duplicate location estimates.

B. Distributed Tracking in Wireless Ad Hoc Networks:

Tracking mobile targets is an important application of sensor networks for both military and defense systems. Even though target tracking has been widely studied for sensor networks with large nodes and distributed tracking algorithms are available, tracking in ad hoc networks with micro sensors poses different challenges due to communication, processing and energy constraints.

In particular, the sensors should collaborate and share data to exploit the benefits of sensor data fusion, but this should be done without sending data requests to and collecting data from all sensors, thus overloading the network and using up the energy supply.

C. Distributed Classification in Sensor Networks Using Mobile Agents:

In a traditional sensor network, data is collected by individual sensors and sent to (possibly multiple) fusion nodes for processing. Because the bandwidth of a wireless sensor network is typically lower than that of a wired network, a sensor network's communications requirements may exceed their capacities.

Mobile agents have been proposed as a solution to this dilemma. In a mobile-agent-based DSN, data stay at each local site or sensor, while the integration or fusion code is moved to the data. Communication bandwidth requirement may be reduced if the agent is smaller in size than the data.

V. CONCLUSION

When the concept of DSNs was first introduced more than two decades ago, it was more a vision than a technology ready to be exploited. The early researchers in DSN were severely handicapped by the state of the art in sensors, computers, and communication networks. Even though the benefits of sensor networks were quickly recognized, their application was mostly limited to large military systems. Technological advances in the past decade have completely changed the situation. MEMS technology, more reliable wireless communication, and low-cost manufacturing have resulted in small, inexpensive, and powerful sensors with embedded processing and wireless networking capability. Such wireless sensor networks can be used in many new applications, ranging from environmental monitoring to in- dustrial sensing, as well as traditional military applications. In fact, the applications are only limited by our imagination. Networks of small, possibly microscopic sensors embedded in the fabric of society: in buildings and machinery, and even on people, performing automated continual and discrete monitoring, could drastically enhance our understanding of our physical environment.

VI. REFERENCES

[1]. R. Rashid, D. Julin, D. Orr, R. Sanzi, R. Baron, A. Forin, D. Golub, and M. Jones, "Mach: A system software kernel," in 34th Computer Society Int. Conf. (COMPCON), San Francisco, CA, 1989.

[2]. C. Myers, A. Oppenheim, R. Davis, and W. Dove, "Knowledge- based speech analysis and enhancement," presented at the Int. Conf. Acoustics, Speech and Signal Processing, San Diego, CA, 1984.

[3]. C. Y. Chong, S. Mori, and K. C. Chang, "Distributed multitarget mul- tisensor tracking," in Multitarget Multisensor Tracking: Advanced Applications, Y. Bar-Shalom, Ed. Norwood, MA: Artech House, 1990, pp. 247–295.

[4]. "Distributed tracking in distributed sensor networks," pre- sentedat the Amer. Control Conf., Seattle, WA, 1986.

[5]. R. T. Lacoss, "Distributed mixed sensor aircraft tracking," presented at the Amer. Control Conf., Minneapolis, MN, 1987.

[6]. "Distributed sensor networks," MIT Lincoln Laboratory, Lexington, MA, Rep. No. ESD-TR-88-175, 1986.

[7]. V. R. Lesser and D. D. Corkill, "The distributed vehicle monitoringtestbed: A tool for investigating distributed problem solving net- works," AI Mag., vol. 4, no. 3, pp. 15–33, Fall 1983.

[8]. D. S. Alberts, J. J. Garska, and F. P. Stein. (1999) Network Centric Warfare: Developing and Leveraging Information Superiority [On- line]:

[9]. (1995) The cooperative engagement capability. [Online] Available: http://techdigest.jhuapl.edu/td1604/APLteam.pdf