Next Generation Distributed Sensor Networks

S. S. Iyengar[1] , G. Seetharaman[4], R. Kannan[1], A. Durresi[1], S. Park[1] , B. Krishnamachari[2] , R. R. Brooks[3] and J. Morrison[4] 1st LT USAF
[1]Dept of Computer Science, Louisiana State University, Baton Rouge, LA70803-4020
[2]Dept of Computer Science, Univ of Southern California, Los Angeles
[3]Dept of Computer Science, Clemson University, NC
[4]AFIT ENG, Air Force Institute of Technology, WPAFB, OH

1. ABSTRACT

Distributed sensor networks operating through wireless communication offer a powerful means to sense, analyze and respond to dynamic environments spread over vast areas. Latest developments in micro electro mechanical sensors (MEMS) and related devices offer several technical and operational advantages making distributed sensor networks as a viable approach. Robustly packaged, inexpensive, energy aware and tamper proof sensors deployed in massively as an ad-hoc wireless sensor network add a whole new dimension to several high impact applications such as air port surveillance, traffic monitoring, environmental monitoring, surveillance against bio-terrorism, battle field damage assessment etc. In short they permit pervasive, persistent and high endurance monitoring of hostile environments. This paper is an introduction to some of the exciting information processing problems that are being solved to effectively harvest the benefits of current and emerging nano, micro, and macro sensors in distributed sensor networks.

2. BACKGROUND

Nano technology is one of the intensely researched areas at present. A number of nano and micro sensors are being introduced each month ranging from biological sensors to complex RF and optical sensors. The mass volume production and inexpensive fabrication of these sensors make them a viable candidate to propel the art of surveillance and monitoring of wide spread areas. Adding fuel to this idea is long-life batteries, energy aware CMOS circuit designs, and hybrid CMOS-MEMS integration techniques which are at the forefront of technology. An impressive array of packaging techniques exist and new ones are being steadily developed to help deploy these sensors in hostile conditions in large numbers.

Most hostile conditions and events of single occurrence do not permit redeployment or replenishing of the batteries in situ the sensors. Also, it is not possible to pre identify the network topology. It is required to have a systematic way of establishing a network among the sensors after they have been deployed, and gather information robustly in a maximally pervasive, persistent and enduring fashion. Sophisticated information processing tasks must factor this into account.

The September, 1999, edition of Business Week stated that the next generation of distributed sensor networks introduces important new technologies for the 21st century. Likewise, the February, 2003, edition of MIT's Technology Review identified sensor networks as one of the top ten emerging technologies. The July 2003 issue of the IEEE Proceeding is devoted to micro and nano sensors. The August 2004 issue of IEEE Computer Magazin gives an excellent introduction to the state of the art in wireless sensor networks.

The motivation for sensor systems is the intelligent gathering of sensor data, processing the data, and understanding and controlling the processes inherent to the system. Pervasive micro sensing and actuation has revolutionized the design and management of extremely complex physical systems. The revolutionary shift in paradigm is very similar to the invention of SIMD parallel computers in the late seventies. The focus at that time was: instead of building one very high performance computer, a well conceived network of very simple processors could be built and operated in single instruction multiple data mode to accomplish very high performance computing.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Next Generation Distributed Sensor Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Louisiana State University,Department of Computer Science,Baton Rouge,LA,70803**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

The Connection Machine, and MassPar machines built using this approach have demonstrated the merit of this approach. A similar revolution is taking place in surveillance and monitoring techniques based on large network of very simple sensors and extremely simple network topologies.

3. INTRODUCTION

Sensor networks can be viewed as a distributed autonomous system for information gathering, performing data-intensive tasks such as environment (habitat) monitoring, seismic monitoring, terrain surveillance, etc. Each node of the network must consist of three components:1) a variety of sensors to acquire information about the observed space; 2) a wireless communication system to help move the data to end user via the neighbors; 3) a computing / coordinating system to buffer the data, and perform higher level task related to forming and operating within an ad-hoc network. The computing part makes it capable of energy aware, adaptive operation, fault tolerant, and tamper proof.

Elements of a sensor network include the sink which sends queries and collects data from sensors, and the sensor which monitors phenomenon and reports to sink (Figure 1). Typically the outsider (sink) does not communicate invasively to an arbitrary element in the network; his query would be picked up by a nearest node in the boundary, or by one of a few pre-selected subset of nodes. Since communication with a distant sink takes more energy, a typical node should avoid communicating directly to the sink. Thus, there is an asymmetry: the sink can broadcast, but the nodes should not reply directly. There is an implicit tradeoff of involving latency for prudent use of power in favor of endurance.

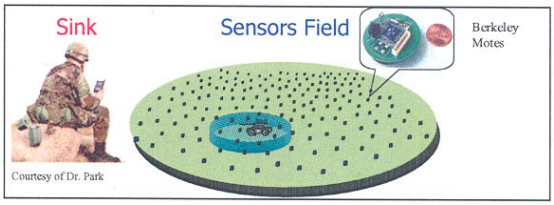

Figure 1: *Sink and Sensors*

Wireless sensor networks are usually a large number of sensor nodes that can be readily deployed in various types of unstructured environments. They rely on wireless channels for transmitting and receiving data from other nodes. Often, the deployment mechanisms do not permit control over the spatial manifest of the network topology. The sensors-nodes must have native capabilities to detect the nearest neighbors and help to develop an ad-hoc network through a set of well defined protocols.

Commercial off the shelf (OTS) components are available to provide the wireless communication aspects of the nodes, allowing the researchers to focus their effort on the sensor design, and analysis of sensed data. Thus, a typical node of a generic sensor network is envisioned as a hybrid structure made of custom designed sensors packaged with OTS (re)motes shown below. A typical sensor mote consists of sensing elements, battery (AA size), processor (less than 20MHz), memory (less than 1MB) and communicating equipment. Figure 2 is an example of a typical sensor node, also widely known as the mote.

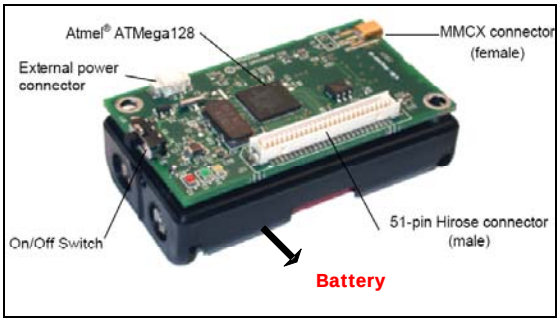

Figure 2: *Typical sensor node. Adapted from Courtesy Crossbow, Inc.*

Sensor network nodes may consist of many different sensor elements. A Sensorcraft [10] is being developed to accommodate a wide range of sensors in a single mobile platform. In this case, it is a small air craft designed carry advanced electromagnetic sensors based on RF-MEMS, FLIR cameras, and CMOS based cameras, an assured data link, onboard GPS and atomic precision time-reference circuitries. Another article from AFRL Horizons[11] depicts a heterogeneous network envisioned by AFRL with sensors operating in concert. Some nodes of the network remain at fixed positions, whereas other nodes (aircraft) remain in constant motion. Communications travels from aircraft to ground sensors, and vice versa. The network nodes also offer a wide range of sensing and communication capabilities, including distributed ground based sensor networks clustered together to act as a single sensor node. Some configurations will wait to be probed by a flyby sink, while others may risk

exposure to report critical events albeit with measured risk.

A challenge in distributed sensor networks is developing an efficient and effective method of extracting data from the network. Figure 3 shows an example of sensor network interaction in which a user submits a query to the network. In this example, the query is submitted to the network through a sink, and is then forwarded to the sensor nodes by local communications links. However, if the same node were to always host sink communications, then, that node will consume battery power faster than other less active nodes. Also, given a limited amount of memory per sensor node, an efficient method of handling communication buffer overflows must also be devised.

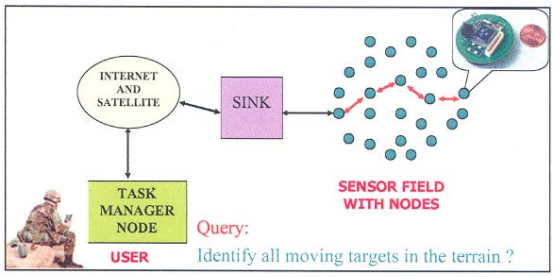

Figure 3: *Network of typical sensor nodes.*

A sensor network is an embedded system that should have the following properties:

- Self-Configuration - formation of networks without any human intervention
- Self-Healing - automatic deletion/addition of nodes without resetting the entire network
- Dynamic Routing - adapting routing schemes on the fly based on the network conditions like link quality, hop count, gradient, etc.
- Multi-Hop Communication - improving the scalability of the network by sending messages peer-to-peer to a base station.

Three common traffic methods to explore in a sensor network are many-to-one, one-to-many, and local communication. The many-to-one method has the sensor nodes sending data to a base station or aggregation point in the network. For the one-to-many method, a base station or single node under a specific condition multicasts or floods a query or control information to several sensor nodes or neighbors. For the local communication method, nodes exchange localized messages to locate and coordinate with each other. The local communication messages may be broadcast or unicast messages [1].

Sensor networks are usually used for either data gathering or an event detection. For data gathering, data should be gathered from the sensor nodes in periodic cycles. A challenge here is to guarantee the system lifetime. For example, communications should occur such that a single node is not burdened with all communications to the sink. For event detection, sensing should occur in real-time. Communication to the base station should be performed only upon the detection of a required event. For both data gathering and event detection networks, measurements from the sensors should be correlated in order to aggregate data. The sensors should also cluster to facilitate aggregation and protocol scalability.

4. HIGH IMPACT APPLICATION OF W-DSNS

Distributed sensor networks can be innovatively applied to a variety of domains (Figure 4). Military applications include surveillance, target tracking, and characteristics measurement of incoming targets.

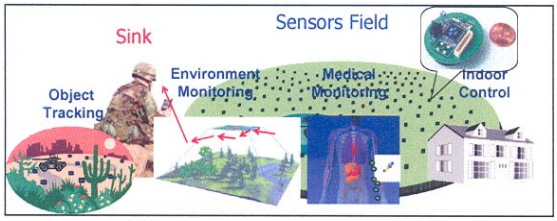

Figure 4: *Applications domains*

The advance of MEMS technology provides new opportunities for distributed sensor networks. MEMS are small, use little power, and are bulk produced. The Jammer Location System (JLOCS) [12] follows a network centered approach to detecting the jamming signals through a widespread set of GPS devices acting as jamming sensors. It is required that we know the self position of the sensors, swiftly determine the direction of arrival (maximum reception) and establish a precise baseline for triangulation. RF MEMS provide ability to generate high radio frequencies in order to super-heterodyne a jammed high frequency signal to much lower frequencies. At lower frequencies, the beat patterns between jammed signals and the jamming signals are efficiently measured and characterized to determine the jammer's location.

Another use of MEMS sensors is measuring sound and pressure activity to determine the location of a seismic or acoustical event. The Sniper Location System (SLOCS) (Figure 5) [13]

uses sensor nodes with numerous MEMS sensors each to measuring its self location, time-of-arrival, and angle of arrival of shock waves. At least two sensors per soldier is essential to measure phase difference and hence angle of arrival. The sniper location and projectile path may be determined from these measurements.

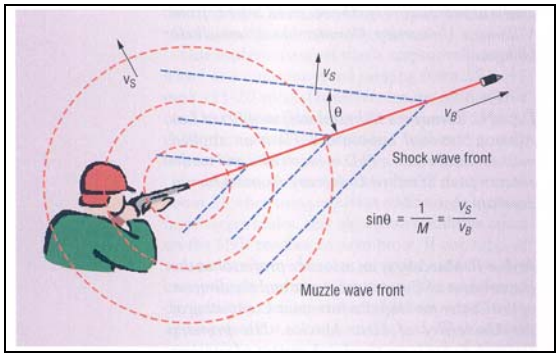

Figure 5: *Adopted from IEEE Computer Aug 2004.*

Interest is also growing in methods of employing stealthy and sacrificial nodes. This challenge addresses the conflicting interest of actively sensing while maintaining stealth (low observability). A sacrificial node may be chosen to emit the energy for active sensing, thus disclosing its location. However, the remaining sensor nodes maintain stealth as they collect the resulting measurements. One or more UAVs act as sacrificial nodes for networks to help acquire data from other stealth aircrafts. Atomic precision clock is necessary to coordinate the events. Current state of the art in modeling sensor nodes do not factor in the mobility and exposure (intentional risking of stealth). They do not focus on the time varying spatial configuration of the sensors, which may be manifesting as an elastic mesh, in a collective motion. Inclusion of such factors would be of vital value to problems focused by the micro UAV based SWARM sensing program, and the DARPA MANTIS program.

Another practical example we are studying deals with wide area video surveillance of busy places like airport corridors populated with steadily moving humans. Here the objective is to use inexpensive CMOS digital video cameras, with localized computing, and wireless communication capabilities. The wireless is chiefly needed for inexpensive and rapid deployment purpose only. The networked sensing is necessary to help construct high resolution images, and be able to human gestures. These requirements can not be accomplished by traditional approaches, where only a few cameras are used to image the corridor from a few strategically selected locations. Such systems are inevitably forced use wide angle lenses, and large depth of field of imaging, resulting in a low pixel count of any observed object. A super resolution imaging would track the subject as he/she moves in the field of view, and inverse compensate the motion, and fuse the video into a high resolution image. In this case, from information theoretic point of view, the motion must be extracted from sources other than video. A large network of extremely simple motion sensor, and/or line of sight optical sensors prove to be effective. Initial results are encouraging [14]. Once again, the choice of implementing this by a wireless sensor network is primarily driven by the economic and logistics constraints rewiring a building to deploy the sensors.

Another exciting application deals with early detection of onset of insidious viruses. The DSN approach to this problem would require a set of geo-sparse internet nodes equipped to communicate amongst themselves through a channel other than the Internet. These nodes form a graph. Each node is able to monitor localized traffic over a periodic interval and compute a local activity vector for each period. All nodes do so in a synchronized fashion. At the end of each period, each nodes communicates with its neighbors its qualitative assessment of the health (activity), and the traffic (port-wise) measure. Then, a discrete relaxation technique would help compute the health of a specific node, based on the perceived health of its neighbors (last frame), and their pair-wise dealings (packet statistics) over the last frame. This method is easy to implement. Analytical tools exist in Computer Vision and Artificial Intelligence to interpret relaxation based results.

For catastrophic events such as chemical or nuclear accidents/attacks, methods to rapidly deploy chemical and radiation sensor networks should also be developed. Sensor networks designed for these events should provide real-time monitoring information for response and rescue missions. Such systems could have been valuable for several incidents:

- Dec 3, 1984 - gas leaked from a tank of Methyl Isocyanate in Bhopal, India, leaving 4000 dead and thousands of people permanently disabled.
- March 20, 1995 - terrorist released sarin an organophosphate (OP) nerve gas in Tokyo

subway system killing 11 and injuring 5500 people.

Feb 6, 2001 - A leak of titanium-tetrachloride at the Tamworth heat treatment factory of Staffordshire, UK, resulted in more than 50 injuries.

5. KEY CHALLENGES: COORDINATED COMMUNICATION ALGORITHMS

There is still a great deal of research and development work to be done in distributed sensor networks. Before resource-constrained sensor networks can be deployed at large scale for long durations in harsh environments, a number of fundamental technical problems need to be solved, such as:

Self-Configuring Deployment and Coverage
Efficient Medium Access
Intelligent Self-Organizing Routing and Querying
Information Management and Distributed Control
Fault Tolerance and Robust Operation
Information Security and Attack-Countermeasures

Addressing these technical problems requires to cutting across all layers, from physical and link to network and application-level. Their solutions require the application of state-of-the-art sophisticated theoretical techniques from many disciplines: coding theory, game theory, distributed control, complexity theory and approximation algorithms, Bayesian inference, network security.

.

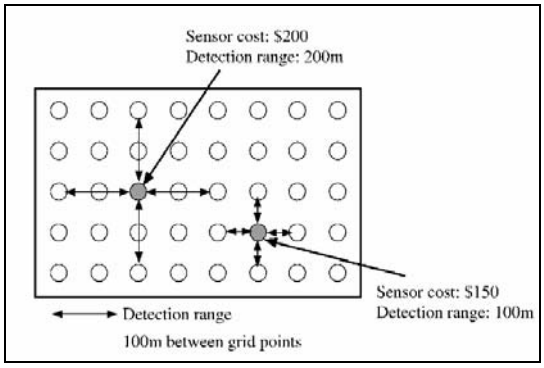

Figure 6: *An example from of a deployment and coverage problem in a two-dimensional sensor field.*

Recently, we have begun forging collaboration between LSU, faculty at Clemson (Brooks), and the University of Southern California (Krishnamachari) to tackle these challenges. At AFIT we are investigating MEMS enabled assured reference devices in JLOCS, SLOCS. Also, early warning virus onset-detectors using collaborative agents across the internet are also being investigated.

Some of our preliminary work is addressing the question of how heterogeneous sensors should be deployed to ensure coverage and connectivity goals are satisfied within cost constraints. Coding Theory techniques such as Identifying Codes are useful for addressing deployment and coverage problems such as is shown in Figure 6 [2].

Another area we are studying is the efficient access to the communication medium. To save energy, distributed algorithms (Figure 7) have been developed to coordinate sleep schedules of nodes to conserve energy while keeping communication delay within acceptable levels [3] [4].

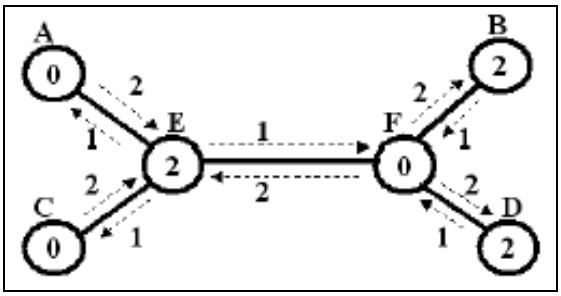

Figure 7: *Sample graph of algorithm to coordinate node communications for efficient medium access.*

Also, we have proposed Game Theoretic routing models for reliable path-length and energy-constrained routing with data aggregation [5]. In this model each node (player) will tend to link to the healthiest possible node (the network partition will be delayed). Each node shares the path length cost, with path lengths tending to be as small as possible. Smaller path lengths prevent too many nodes from taking part in a route, reducing overall energy consumption. The Nash Equilibrium of this routing game defines the optimal, Length-Energy-Constraint (LEC) path [5].

Because interoperability between different nodes in a large scale sensor system is inherently difficult, we have developed and evaluated a number of controller design methodologies for hierarchically controlling the behavior of distributed sensor; including Petri Net, finite state automata (FSA), and vector addition control (VAC) [6]. Also, we have developed a Bayesian interface technique to differentiate between

measurement errors and significant environmental anomalies based on localized evidence [7]. This technique can correct more than 90% of errors if the fault rate is less than 10%.

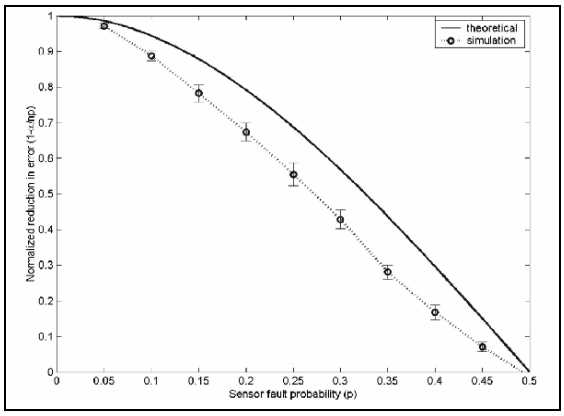

Figure 8: *Normalized reduction in average number of errors for the optimal threshold decision scheme.*

We have also worked on several routing techniques with in-network information fusion in order to aggregating information as much as possible (Figure 9) [8].

Scheme	Bits Used	Savings	Response Quality
No aggregation (NA)	221544	0%	Exact
Header Aggregation (HA)	117544	46.9 %	Exact
HA with Compression (HAC)	100648	54.6 %	Exact
Rectangular Aggregation (RA)	34984	84.2 %	Tight rect. approximation
Circular Aggregation (CA)	34984	84.2%	Tight circ. approximation
Stepwise Rect. Aggregation (SRA)	9240	95.8%	Tight rect. approximation

Figure 9: *Evaluation of several routing and aggregation schemes.*

We are also addressing network security requirements given the severe resource constraints, as traditional cryptographic techniques have unacceptable overhead. One recent development of new distribution protocol providing an efficient tradeoff between security and performance resulted in a 2-phase technique that provable outperforms state-of-the-art randomized techniques at new key [9].

Our next challenge addresses interoperability with Internet and Actor networks. In an Actor Network, an external user, such as a commander, orders actors to perform actions such as changing the environment or attacking targets (Figure 10).

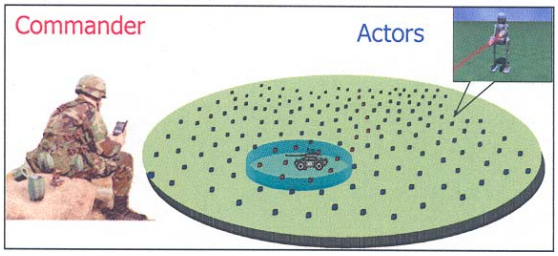

Figure 10: *Depiction of an interaction between a sensor network and an Actor network.*

The issues for interoperability between these networks include development of standard interfaces, authentication and security, and coordination. Due to different protocols at the sensor, actor network, and Internet, it is necessary to provide common and extensible interfaces. Hostile forces make critical the need to provide decentralized authentication methods over Internet or shared wireless media. Furthermore, all autonomous sensor and actor networks should collaborate with each other without human coordination. These are the challenges that the new technology and new ways of thinking have brought in the area of distributed sensor networks.

6. CONCLUSION

Current trends in MEMS and NEMS sensors indicate increased availability of inexpensive and massively deployable sensors to help monitor hostile environments through wireless sensor networks. Steady progress in power aware CMOS circuits, increased access to CMOS-MEMS hybridization, operational advantages of RF-MEMS antennas all make wireless sensor network a common place infrastructure of the near future. Recent research has been focused on both communication and protocols required to operate these sensor networks. We have presented a number of promising applications currently being studied, along with specific communication algorithms developed to perform the power aware routing. Security is an important factor which has not been covered here since it is covered by a number of papers in literature.

7. ACKNOWLEDGEMENT

The authors acknowledge the sources of Figure 2, Crossbow Inc, and that of Figure 5 the IEEE Computer magazine. Also, the research has been supported by various NSF and DARPA grants.

The coauthors' affiliation with The Air Force Institute of Technology does not in anyway imply that the material presented here is the official policy of the United States Air Force. The scientific views stated here are based on the collective scientific conclusions of the authors and not of their employers.

8. REFERENCES

[1] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," University of California at Berkeley, First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[2] K. Chakrabarty, S.S. Iyengar, H. Qi, E. Cho, "Grid Coverage for Surveillance and Target Location in Distributed Sensor Networks," IEEE Trans. of Computers, December 2002.

[3] V. Paruchuri, S. Basavaraju, A. Durresi, R. Kannan, and S.S. Iyengar, "Random Asynchronous Wakeup Protocol for Sensor Networks." To appear in Broadnets 2004.

[4] G. Lu, N. Sadagopan, and B. Krishnamachari, "Delay Efficient Sleep Scheduling in Wireless Sensor Networks," USC Tech Report 04-830, In submission to IEEE INFOCOM 2005.

[5] R. Kannan and S. S. Iyengar ``Game-Theoretic Models for Reliable Path-Length and Energy-Constrained Routing with Data Aggregation in Wireless Sensor Networks, " to appear in IEEE Trans. on Communications.

[6] R. Brooks, M. Zhu, J. Lamb, and S. S. Iyengar ``Aspect-Oriented Design of Sensor Networks, " Journal of Parallel and Distributed Computing, 2004.

[7] B. Krishnamachari, and S. S. Iyengar "Bayesian Algorithms for Fault-tolerant Event Region Detection in Wireless Sensor Networks," IEEE Transactions on Computers, March 2004.

[8] B. Krishnamachari, and S. S. Iyengar "Efficient and Fault-tolerant Feature Extraction in Sensor Networks," Workshop on Information Processing in Sensor Networks (IPSN) 2003.

[9] R. Kannan, L. Ray, A. Durresi, and S. S. Iyengar "Security-Performance Tradeoffs of Resilient Inheritance based Key Predistribution for Wireless Sensor Networks," In submission to IEEE Transactions on Computers.

[10] John M. Perdzock et.al. The Sensor Craft Challenge: Innovative concepts of high altitude and long endurance technologies for Sensor Craft. AFRL Horizons, June 2004. http://www.afrl.af.mil/techconn/index.htm. Reference document number. SN-03-12

[11] William Brown. Ron Kaehr, and Tamara Chelette. Finding and Tracking Targets: Continuous awareness of all targets and threats. AFRL Horizons, Feb. 2004. http://www.afrl.af.mil/techconn/index.htm. Reference document no. SN-03-08.

[12] GPS Jammer Detection and Location System. A SBIR/STTR Review. AFRL Horizons June 2004.

[13]Mikilos Maroti et.al. Shooter Localization in Urban Terrain. IEEE Computer. August 2004.

[14] Guna Seetharaman, Ha Le, S.S.Iyengar, and et.al. A Motion compensated super resolution imaging technique. IEEE Monograph of Multi Sensor Networks, (Eds) S. Poha et.al. John Wiely & Sons and IEEE Press. 2004.

[15] Clark Nguyen. Micro-Electro Mechanical Systems: Scaling Beyond the Electrical Domain. Proceedings of the DARPA-Tech 2004Conference. Section on MTO. http://www.darpa.mil/DARPAtech2004/proceedings.html