

SCATTERABLE SENSOR NETWORKS FOR NETWORK CENTRIC WARFARE APPLICATIONS

Kenneth E. Viall
United States Army

ABSTRACT

This paper investigates the utility of realistic, time and scale-constrained sensor networks in cooperation with semi-autonomous robots as envisioned in future Network-Centric Warfare. The particular application chosen is a networked minefield based roughly on the United States Military Family of Scatterable Mines (FASCAM) with similar emplacement and planning techniques. Algorithms for sensor network operation and sensor network control are provided. Simulation results for sleep and wake cycles and energy consumption indicate that sleep logic based on hop distance from a minefield event provide the best energy savings.

INTRODUCTION

THE Department of Defense has been investigating the concept of Network-Centric Warfare (NCW) as a means of leveraging the power of networked systems to move time-sensitive and relevant information quickly in a battlefield and achieve more rapid and decisive victories [1]. Relevant information traverses the notionally ubiquitous and secure network to link sensors, shooters, and decision-making entities and improve overall performance. The vision of NCW motivates the Defense Advanced Research Projects Agency (DARPA) and other military research organizations to investigate and fund research grants supporting the leading technology in areas related to networked communications, robotics, and sensor networks. Similarly, theoretical researchers in these fields seek to understand and model different environments to validate the utility or performance of particular ideas. This paper provides a concrete example of a potential military application of sensor network employment and interaction with semi-autonomous robots as a bridge between theory and practical application.

This paper is organized as follows. This introduction is followed by an outline of the motivation and general related sensor net applications, with specific differences in

assumptions valid for certain military environments. The paper then reviews more military focused related research in intelligent minefields and Unmanned Aerial Vehicle (UAV) interaction with sensor networks. Next, a notional extension of military remotely delivered mines to a sensor net emplacement is introduced, with discussion of some recent sensor network protocols for localization, routing, and data coding useful for a military sensor net emplacement. The next section provides an overview of a simulation of a portion of the proposed system with some analysis of message complexity and energy usage. Finally, future simulations and research directions are outlined.

MOTIVATION AND BACKGROUND

General Sensor Network Applications

Sensor networks have been studied and proposed for a number of applications [2-4]. A representative sample is presented in figure 1, comparing the scale subjectively measured in numbers of sensor nodes to an estimate of the length of time the sensor network might expect to operate

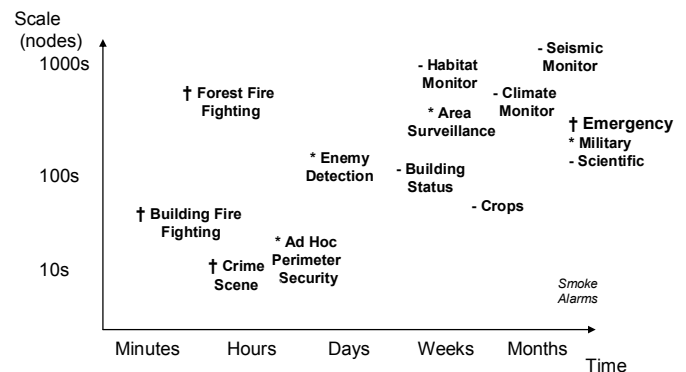


Fig. 1. Sensor Net Scale compared to Operational Time for Notional Applications

to serve some useful purpose.

Scientific applications for long period observation of climate, habitat, or seismic activity could be optimized for low energy operation over long periods with sophisticated techniques for extracting data from a widespread network. At the other extreme, immediate delivery of sensor nodes could assist in emergency response such as fire fighting and would only be expected to operate for a very short

This paper is based on material supported in part by the Department of Defense Information Assurance Scholarship partnership between the National Defense University and Texas A&M University. Opinions expressed are those of the author and do not represent the official position of the Department of Defense.*

time. For emergency applications, the design considerations of energy conservation might be less important than providing rapid and reliable communications.

Military applications might stress security and reliability for their intended purpose with moderate energy conservation. For example, long term area surveillance might be such a strategic requirement that it would be important enough to preclude using a sensor network as the only method of observation of the area. Short range enemy detection in a local area when a friendly force has established a defensive position could be valuable but not particularly challenging to design if it always operated in close proximity to friendly forces allowing constant oversight and replacement of power sources.

On Demand Sensor Networks

A long range employment of a tactical sensor network to a remote location which other sensor methods can not reliably cover due to weather or terrain provides a dual challenge. First, the sensor net must capture and protect relevant data reliably for a stated period of operation. Second, the network should securely provide the data to an authenticated friendly entity, human or robotic, that would interact with the sensor net within a shorter time window than might be required in a number of scientific applications.

Recent simulations conducted to validate concepts related to NCW included Future Combat Systems that linked sensor networks with ground vehicles and extended network coverage using a number of networked UAVs [5]. Sensor networks should be considered in the broader scheme of NCW as augmentation to other sensors in extreme weather or terrain. For example, a sensor network detecting large vehicle movements across a desert coupled with a communications gateway could provide cues to friendly aircraft to rapidly investigate the report.

On a medium scale under shorter time constraints, a sensor network could be employed in advance of a moving force to observe key road intersections and provide a more detailed data set for analysis to a scout robot which could relay commands and data to the actual military force. Design differences from civilian applications generally include a much shorter expected operating time, less concern for scalability, and greater requirement for security of the system.

RELATED WORK

Intelligent Minefields

The closest examples to on-demand sensor network employment in current military ground operations are the

artillery or air delivery of relatively simple mechanical mines with self-deactivation limits. These mines can be emplaced with particular density and coverage area to impede enemy personnel or vehicle movement for short periods of time in support of military objectives. Recent United States Government policy on mines committed the country to a number of requirements for all mines by 2010 [6]. First, the U.S. will only use mines including a reliable self destruct mechanism timed currently between 4 hours and 15 days. Second, a secondary self deactivation method will ensure batteries expire within 90 days to meet international treaty requirements of safety for eventual humanitarian demining after 120 days. In addition to describing absolute design parameters that the government must achieve, the policy mentions future concepts including more intelligent mine fields with remote control, selective activation, and focused temporary deactivation in specific areas to allow friendly force movement.

One example of an intelligent minefield demonstrated next generation mines with a number of sensors and network capability as a proof of concept [7],[8]. The mines provide a self healing capability by cooperatively detecting holes in their topology which might indicate a successful enemy breach of a portion of the area [8]. Mines would then execute a series of physical hops using an onboard propulsion mechanism while the explosive charge was temporarily deactivated to attempt to close the breach. This experiment differs from this paper in the method of mine emplacement and lack of interaction with an external entity.

Robotic Interaction with Military Sensor Nets

Numerous examples of robotic minefield clearing exist in the literature but since these applications focus on the opposite problem from minefield sensor interaction, this area will not be addressed in this paper. General robotic sensor net interactions have been studied for some commercial applications but few specifically for military purposes. Categories of interaction related to movement include navigation of the robot using the sensor field and UAV operations to deploy a sensor net [9]. Other categories of research include methods for extracting information from the sensor network. One project proposes an ad hoc election of a gateway sensor node for communication with a UAV to save power while providing the benefit of the sensor network for harvesting [10].

ON-DEMAND SENSOR NET PROPOSAL

Given recent changes in mine policy, the current military Family of Scatterable Mines (FASCAM) must evolve to meet the requirements of next generation mines in a

network-centric environment. FASCAM minefields are emplaced by firing a number of shells from a ground-based artillery system or dropping equivalent shells from an Air Force aircraft [11]. A secondary explosion ejects the mines from the shell a fixed distance from the planned point of impact and the mines fall dispersed over an area determined by the trajectory of the original shell and aim point. FASCAM planners determine the number of shells to employ to achieve a certain density of mines over hundreds of meters.

FAS-SENET Proposal Overview

One proposed extension could create a Family of Scatterable Sensor Networks, named FAS-SENET for the remainder of this paper, using the same ballistic parameters and forms as the current anti-personnel and anti-vehicle mines in the FASCAM system (Fig 2.). While a large scale employment of sensors for area surveillance could be infeasible for artillery delivery methods, medium scale networks for enemy detection would certainly be consistent with current use of FASCAM.

The FAS-SENET could retain the capabilities of the current FASCAM minefield, or become a sensor only device. It would be useful to retain the capability to self destruct to prevent tampering with a small explosive charge. The sensor function of the system could be extended beyond the personnel trip wire or magnetic vehicle detection to include sound or visual detection.

This paper assumes a minimum sound detection capable of detecting a local explosion. Sensor CPU, memory,

Global features of the system should include the ability to track the total number of detections by type, along with time and real or relative locations within the capabilities of the localization algorithms. Node destruction or loss of contact should also be reported. Estimated line of bearing to the most likely avenue of enemy approach could be derived in the sensor network based on the distribution of detections.

Local nodes should maintain an operational alertness level between a sleeping or suspended state and a fully alert state. Nodes should supplement a personnel or vehicle detection with other sensory data including sound or vibration which might indicate tampering. Nodes should deactivate when scheduled or earlier if disturbed.

Support Robot Overview

A sensor net may have limited utility if the data is not retrieved. A sensor enabled minefield could still fulfill its original military purpose at least as well as previous dumb minefields. However, intelligent control of minefields implies an eventual interface to a human or relay through robotic devices including UAVs.

The robot role in this system is to navigate to the sensor net and control the net while in close proximity. Details of semi-autonomous robot operation are not covered in this paper. Without loss of generality, the robot could be a UAV that achieves an overhead position and circles for extended periods of time or a remotely controlled ground vehicle that is placed in proximity to the sensor network and then allowed to execute local protocols to link to the sensor field. A ground based system will be assumed in this project.

Upon establishment of adequate communication with the sensor field, the robot can extract data, reprogram the operation of the sensor field, or deactivate the sensor field. The robot can be assumed to have other communications systems capable of connecting periodically to a base control station in order to relay information or transfer control to friendly forces that move into the vicinity of the sensor field before deactivation.

System Design Considerations

A proposed system design is shown in figure 3. Upon initial deployment of the sensor field each node performs individual activation, then after a random delay joins in network activation [12],[13]. The sensor net will operate independently with maximum use of sleep cycles to conserve energy until a trigger event occurs. Default behavior on event detection will be to flood the network with an alert that wakes other sensor nodes in anticipation of correlated events. Numerous events can occur during this period. Data collection can be cataloged into critical

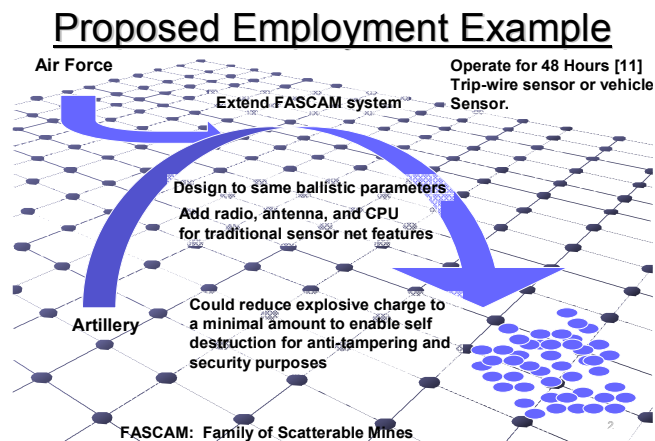


Fig. 2. Notional Deployment of an On Demand Sensor Net [11]

radio, and antenna forms must be capable of withstanding the shock of deployment. For purposes of the paper they will be assumed to enable the types of algorithms and protocols described in current literature on sensor network research.

aggregated information (“how many detections in the network, how many lost nodes”) but other techniques such as distributed erasure codes could be used to archive

System Design Flow

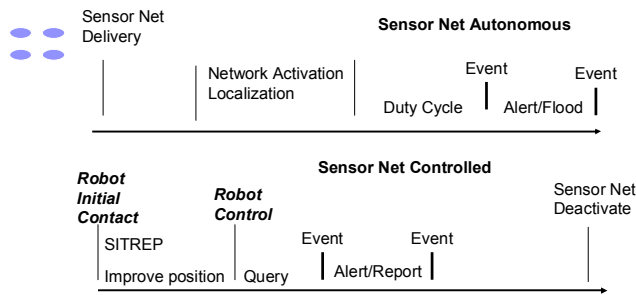


Fig. 3. FAS-SENET transitions before and after Robot Arrival

information about all events over a period of time for possible retrieval and analysis [14].

Upon initial contact by the robot, an initial situation report (SITREP) can be exchanged to provide a summary of events detected and time of last event, and local neighbor’s location to aid in establishing better connectivity to the sensor network. The robot should have a global positioning satellite (GPS) capability and may translate sensor network reported locations to real coordinates to perform incremental movements and achieve redundant connections.

With sufficient connectivity, the robot could begin to query the network systematically to retrieve archived event data which may be encoded. Commands to sensor nodes and subsequent communications can utilize stateless routing techniques instead of broadcast, reserving broadcast for future alerts [15],[16]. Table I provides a summary of design areas and potential protocols from the literature as solutions.

Sensor Node Algorithms

Some parameters must be loaded into sensor nodes prior to employment. A variable deactivation time should be common to the network and for this project can be set at 48 hours. Encryption keys and other parameters should be available.

Sleep mode can be interrupted by sensor events or receive events. Wake mode duration will depend on a linear time factor of the hop distance from the event and will be evaluated in later sections. Pseudo-code for sensor operation with annotations is shown in Table II.

TABLE I
FAS-SENET POTENTIAL IMPLEMENTATIONS

Area	Requirement	Possible Application
Localization and Topology Discovery	Prefer a geographic embedding, or the ability to translate when GPS position is injected	GLS [12] UDG [13]
Network or Source Coding	Improve network flow or prepare network for better reaction to future query	Distributed Erasure Codes[14]
Routing	Broadcast alert data, Periodic network refresh. Link to robot and report	AODV[15] GPSR[16]

Robot Algorithms

Robots can be remotely tele-operated but must have

TABLE II
FAS-SENET SENSOR ALGORITHM PSEUDO-CODE

Code Logic	Notes
Delay random period; Initialize; While (not deactivate time) Sleep until (timer or interrupt);	General Sensor initialization and loop
If (tamper detected) Wake, Multicast send “tamper”, self-destruct	Attempt to send an alert, self destruct
If (detect event) Wake, Multicast send “alert” Process event data If (receive “tamper” from neighbor) Mark neighbor on suspect “grey list” If (detect explosion after “tamper”) mark neighbor on “black list”	Broadcast alert data, Flag neighbors as suspected or confirmed destroyed based on correlated report and detections
If (Receive “Robot message”) Unicast response Update parameters	Use GPSR for direct connection

some semi-autonomous capability to execute linkup tasks to overcome the possibility of periodic loss of connectivity to the controlling station. Common encryption keys must be loaded before robot deployment.

The SITREP situation report with immediate, high value information provides information of immediate tactical value to the linked robot. Nothing prevents any number of authenticated robots in a network-centric environment from receiving a SITREP while one designated robot performs data retrieval and control of the sensor net.

The DIGEST is a more detailed history of events with timestamps that could be encoded in a decentralized fashion to provide high probability of retrieval if too many sensor nodes are not destroyed quickly. This information may already have contributed to in-network estimates of enemy direction of approach. Correlation of this information with other network-centric sensors after collection and transmission to a command and control facility by the robot could have additional operational value. Pseudo code for the robot sensor net logic is shown in Table III.

SIMULATION

Design of Sleep-wake Duty Cycles

While the overall FAS-SENET model provides a number

TABLE III
FAS-SENET ROBOT SENSOR ALGORITHM PSEUDO-CODE

Area	Notes
Navigate to safe distance from sensor field expected location; Begin broadcasting beacon; While (no answer & not at sensor field) Move incrementally;	General robot initialization and position improvement
If (first response) Query for location of neighbors and deactivate time, get SITREP; Move incrementally to establish redundant connectivity;	Improve network flow, reduce energy drain on single sensor
While (not deactivate time) Query sensor net for DIGEST information;	Broadcast alert data, Periodic network refresh.
If (Receive "Alert") Record and update; Update parameters;	Sensors link to robot and report

of potential research topics, the sleep-wake duty cycle provides an initial topic to examine in simulation. Simulation tools for sensor nets can be used to focus on different aspects of systems, from the physical communications protocol and energy efficiency to higher concepts such as the performance of routing and security implementations.

From the list of available network simulators, the J-Sim [5] and VisualSense [17] systems provide complementary capabilities operating on a common Java runtime environment. J-Sim operates with component based architecture and models sensor nodes with CPU, battery,

and radio components. While it is similar to NS-2 in the TCL scripts used to construct a simulation (Java TCL in this case), it is not as thoroughly documented. Protocols common to sensor network experiments including AODV and GPSR are available, as well as directed diffusion and localization. While a few small example simulations of GPSR for a small number of sensor nodes were performed, it remains future work to build a full model of an intelligent minefield, perhaps as an extension of the NCW simulation.

VisualSense extends the Ptolomy Project simulation system [16] and provides for composite actors which can be linked visually to interact with each other in the simulation. To explore the basic operation of the minefield sensor network, the small world and evader pursuer models were combined and extended to 100 sensor nodes placed randomly in a 200x200 meter area with a mobile robot opposed by an enemy vehicle. The relative starting positions of the actors could be adjusted with the mouse but the sensor nodes would reinitialize to different random positions every iteration.

Figure 4 shows an example run with random node placement. Dark nodes near the composite actor representing the enemy tank have detected the tank and flood the sensor network with alert messages. White nodes represent stragglers that failed to receive the initial alert broadcast. Over a number of simulations, approximately

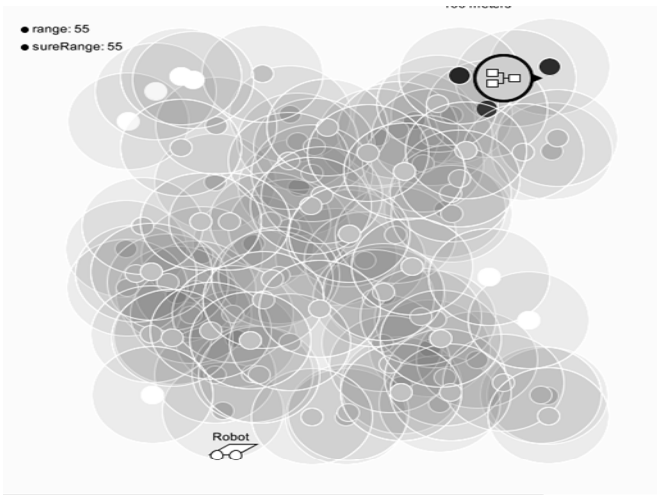


Fig. 4. VisualSense Simulation of a random Event Detection Propagation

six percent of sensors placed near the edge of the minefield failed to receive alert broadcasts.

Results

Figure 5 shows the average distribution of distance in hops from a detection event for 5 simulation runs. If the network is sufficiently dense, one would expect the

minefield to detect enemy contact close to the perimeter of the field. Communications cost close to the center of the field could be higher than the cost at the perimeter for end to end routing such as GPSR, which could contribute to node death earlier than desired if the system were required to operate for a long period of time. Under the time

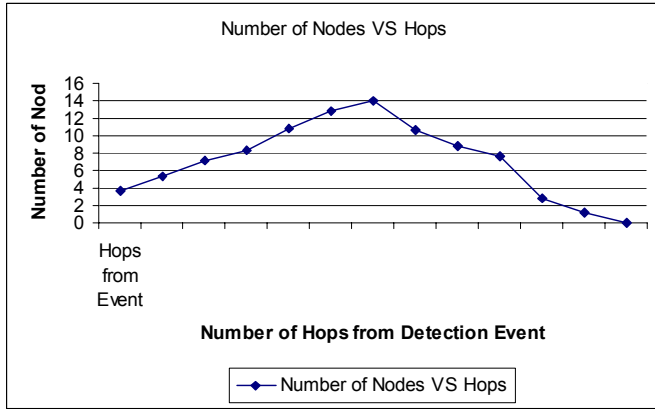


Fig. 5. Distribution of Hop distance from Alert Events for 100 nodes

assumptions specific to this application and the use of message flooding each node should retransmit an alert message once and energy consumption is balanced relative to event detection.

To estimate other relative energy consumption, the following assumptions were made for a power model. Average energy consumption for an alert node is normalized as one unit. Sleeping nodes are assumed to maintain the capability to wake on alert and are assumed to consume 0.5 units of energy, less than the normal alert consumption. Message passing can consume 10 units per message, represented the expected increased energy expenditure of wireless transmission.

The hop distance from a node sending an event alert broadcast was used to construct a function to determine the length of time the receiving sensor should remain awake. Two algorithms were constructed and simulated (eq. (1)). The sleep time S_i for each node is calculated based on local information of a few tunable parameters and the hop distance from the event. A constant factor C is set to achieve a maximum period of alertness. In the linear model, nodes reduce their sleep time as a linear function of their hop distance from the event H_i .

$$\begin{aligned} S_i &= C - \alpha H_i \\ S_i &= \beta + \frac{C}{H_i} \end{aligned} \quad (1)$$

The parameters α, β (representing a linear rate and minimum alert period, respectively) and C could be tuned based on models of enemy vehicle movement and tactics to

influence the performance of the intelligent minefield. Setting C to 20, α, β to 1 and 5 for the simulation, the total energy consumption at each hop distance over the five simulations are compared for the linear and multiplicative sleep models in Figure 6.

While the results indicate greater energy consumption for sensor nodes in the middle of the network, hop based sleep logic provides an improvement of %30 percent for the linear model and %50 percent in the multiplicative

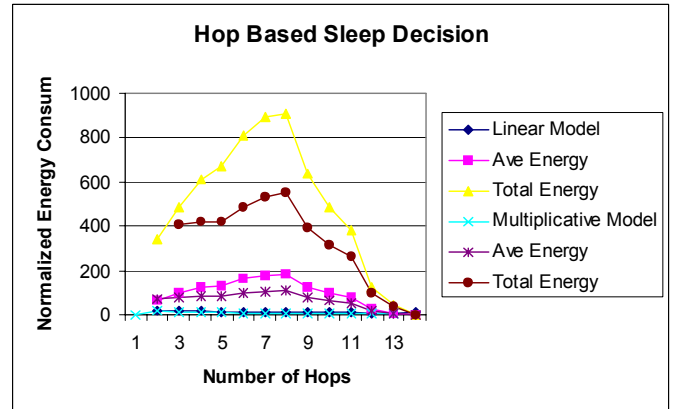


Fig. 6. Energy Consumption based on Sleep Decisions model compared to a benchmark default behavior of a fixed sleep period upon each alert cycle.

Analysis

Hop-based sleep logic provides some energy efficiency for nodes farther from detection events. Conversely, the longer alert time at leading edge nodes make use of node energy in an area that might be more likely to be disrupted by enemy advances. The small scale and bounded operational time of a military sensor network application allow for more limited complexity in the selection of schemes for message passing and alert/sleep cycles than might otherwise be considered for civilian sensor network applications.

While the algorithms chosen for this experiment were adequate to demonstrate the concept, they could be made more power efficient or selective in message broadcasts. The problem of orphan clusters must also be addressed. The orphan clusters initially represent small numbers of mines that activate outside of the reach of the majority of the sensor net. Robotic intervention with a more capable antenna at a higher elevation could help reconnect otherwise orphaned segments. Otherwise, orphans could work individually or in concert with a few neighbors with the same algorithmic control logic as the main network, and self destruct or deactivate in the same time window.

FUTURE RESEARCH DIRECTIONS

A number of potential extensions can improve the concept of FAS-SENET presented in this paper. Robot recovery of friendly minefields can be implemented using geographic routing information translated from the localization in the sensor network, and a greedy forwarding technique to partition the mines and retrieve them in according to some pattern. RFID tags on friendly equipment and soldiers could allow intelligent minefields to temporarily deactivate and prevent friendly casualties, but care must be taken to prevent an adversary from compromising the security of such a scheme. In addition, in network processing could be designed to extend localization to estimate enemy direction of advance or other patterns, and to archive data efficiently for later retrieval and analysis [18].

CONCLUSION

Military Applications of Ad Hoc Sensor networks must conform to different design constraints such as security, reliability, and assured operation for particular purposes. Considerations of energy consumption should be considered but balanced against the operational purpose of the network. A FAS-SENET system could offer a feasible ground forces employed sensor net capability consistent with current United States mine policy. As an illustrative example, this project provides a model application that could stimulate thought on realistic military uses for emerging research in sensor networks.

REFERENCES

- [1] A. Gartska, Network Centric Warfare, Department of Defense, 2001.
- [2] A. Hac. *Wireless Sensor Network Designs*. John Wiley and Sons, Ltd. West Sussex, England, 2003.
- [3] D. Estrin. "Next Century Challenges: Scalable Coordination in Sensor Networks". In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*.
- [4] J. M. Kahn, R. H. Katz, K.S. Pister, "Next Century Challenges: Mobile Networking for 'Smart Dust'". In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*.
- [5] University of Illinois at Urbana-Champaign, "Future Combat System Simulation Demonstration", available online at <http://lion.cs.uiuc.edu/demo/demo.html>
- [6] United States Government, Department of State. "Landmine Policy Whitepaper." February 27, 2004. Available online at <http://www.state.gov/t/pm/rls/fs/30047.htm>
- [7] W. Merrill, L. Girod, B. Schiffer, D. McIntire, G. Rava, K. Sohrabi, F. Newberg, J. Elson, W. Kaiser. "Dynamic Networking and Smart Sensing Enable Next-Generation Landmines," *IEEE Pervasive Computing*, vol. 03, no. 4, pp. 84-90, October-December, 2004.
- [8] G. Rolander, J. Rogers, I. Batteh. "Self-healing minefield". Science Applications International Corp. *Proceedings of SPIE -- Volume 5441 Battle space Digitization and Network-Centric Systems IV*, Raja Suresh, Editor, July 2004, pp. 13-24
- [9] P. Corke. "Autonomous Deployment and Repair of a Sensor Network using an Unmanned Aerial Vehicle". *Proceedings of IEEE Conference on Robotics and Automation*, New Orleans, 2004.
- [10] W. Su. "An Adaptive and Fault-Tolerant Scheme for Gateway Assignment in Sensor Networks. *Proceedings of 2003 IEEE Military Communications Conference*, 2003.
- [11] J. Pike, "Family of Scatterable Mines – FASCAM," GlobalSecurity.Org, available online from <http://www.globalsecurity.org/military/systems/munitions/fascam.htm>
- [12] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in *Proceedings of the 6th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking*, Boston, Massachusetts, USA, August 2000.
- [13] F. Kuhn, t. Moscibroda, R. Wattenhofer. "Unit Disk Graph Approximation," In *Proceedings of the 2004 Joint Workshop on Foundations of Mobile Computing*, 2004.
- [14] A. Dimakis, V. Prabhakaran, K. Ramchandran. "Ubiquitous Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes," *Symposium on Information Processing in Sensor Networks (IPSN'05)*, April, 2005.
- [15] C. Perkins. "Ad Hoc on Demand Distance Vector Routing (AODV)" *MILCOM '97 panel on Ad Hoc Networks*, November 1997.
- [16] B. Karp, H. Kung. "Greedy Perimeter Stateless Routing for Wireless Networks". *Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 243-254, Boston, MA, August, 2000.
- [17] P. Baldwin, S. Kohli, EA Lee, X. Liu, Y. Zhao, "Modeling Sensor Networks in Ptolomy II," *Proceedings of Information Processing in Sensor Networks*, 2004.
- [18] P. Venkitasubramaniam, S. Adireddy, L. Tong. "Sensor Networks With Mobile Access: Optimal Random Access and Coding" *IEEE Journal on Selected Areas of Communications*, Vol 22 No. 6, August 2004.