International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

IMPLEMENTATION AND DESIGN OF MEMS BASED SELF ORGANIZING LOW COST WIRELESS SENSOR SECURITY NETWORK

Dr.E.N.Ganesh
Professor, Department of ECE
Saveetha Engineering College, Chennai, TN

***Abstract*— A very important benefit of continuing advances in CMOS IC technology is the ability to construct a wide variety of micro electrical-mechanical systems (MEMS) including sensors and RF components. These building blocks enable the fabrication of complete systems in a low cost module, which include sensing, signal processing, and wireless communications. Together with innovative and focused network design techniques that will make possible simple deployment and sustained low power operation, the small size and cost can be enabling for a very large number of law enforcement and security applications, including remote reconnaissance and security zones ranging from persons to borders. We outline how the application can be exploited in the network design to enable sustained low-power operation. In particular, extensive information processing at nodes, hierarchical decision making, and energy conserving routing and network topology management methods will be employed in the networks under development.**

Keywords— **Wireless sensors Networks, Micro electro Mechanical Systems, Radio Frequency.**

I. INTRODUCTION

Exponential growth in microprocessor performance and memory capacity has created a multi-billion part per year embedded processor market. These devices populate stand-alone products in diverse businesses including automotive, appliance, and manufacturing systems. Additionally, low cost micro electro-mechanical systems (MEMS) devices have been developed for sensing and actuation, enabling deployment of complete embedded systems when combined with recent advances in integrated communications technology. Consequently, in the near future, it will be possible to seamlessly join the existing information infrastructure with the physical world. We discuss such systems, with a focus on how the integrated nodes can cooperate in a security network. As illustrated in

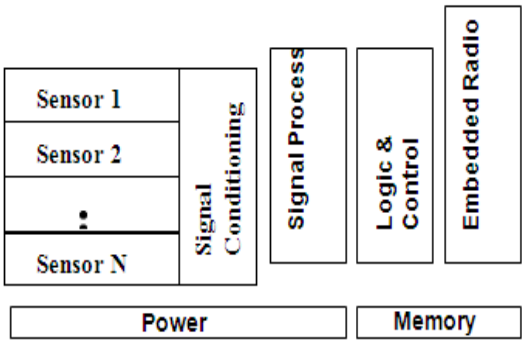

Figure 1. Basic architecture of WINS node

Figure 1, wireless integrated network sensor (WINS) nodes can include MEMS components such as sensors, RF components, and actuators, and CMOS building blocks such as interface pads, data fusion circuitry, specialized and general purpose signal processing engines, and microcontrollers. The more complicated but low duty cycle applications would for example be run in the general purpose processors, while frequently invoked operations would be run on specialized circuits to save power. The node may be powered by batteries, photocells, or power mains. It might alternatively scavenge power from vibrations, acoustic or millimeter wave energy through use of MEMS resonators or piezoelectric. The options increase as the size and power consumption diminish. Communications may be by wires, acoustic, infrared, visible light, or radio. The individual nodes may have modest capabilities, but may achieve large scale effects through coordinated activity in a network of hundred to tens of thousands of nodes. Examples of coordinated activities are beam forming for enhanced target detection, multi-hopped communications, distribution of timing and position information, and coordinated actuation to produce macro-scale effects from micro-devices. The distribution of intelligence throughout the network greatly promotes this scalability through massive reduction of control and data traffic. We are presently constructing a large number of prototype nodes, with the intended application of situational awareness. The present generation of nodes will

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

be modular in construction, with separate boards for processing, acoustic and seismic sensors, acoustic ranging actuator, the radio, and power supply. The nodes will be powered off 9 V batteries. For law enforcement and military applications, personnel cannot spend significant effort in precisely deploying and then bringing up the network. The expense in training and the potential exposure of personnel to danger both point to the need for completely autonomous operation. Therefore, the nodes will be capable of self-organizing into networks. Since the size of the network and the time of operation will not be known a priori, it is also important to devise a strategy which allows scalability in network size and conservation of energy reserves. In single processor systems with multiple sensor or communications ports, all elements have access to a common timing base, with all data paths fabricated with the same technology, enabling matching. Use of colocated sensors and centralized processing implies no communications cost. However, for a distributed sensor network, the timing, position, routing, processing scheduling, and communications must all be coordinated by passing control messages among nodes which cost power and which are subject to degradations due to node failure and jamming.

The solution lies in an integrated approach with aggressive power management at all levels:

i) spread spectrum communications for resistance to interference/jamming and to reduce detection in covert applications
ii) adaptive power control in communications to use minimal power
iii) link rate adjustment to extend communications range in adverse conditions
iv) multi-hop routing to minimize total power consumption, probability of message interception, and to enable flexible deployments
v) varying node alertness level to conserve power for essential tasks.
vi) cooperative algorithms designed for shared processing with close neighbors.
vii) distribution of data only to those nodes that need to know, increasing networking flexibilityand reducing communication duty cycle.
viii) distributed synchronization to prevent network self-interference and to preserve code lock.
ix) cooperative use of system resources to conserve power in critical nodes.
x) hardware optimized for low power operation.

It is the choice of protocols rather than the optimization of the hardware that leads to the largest power savings. With the proper choice of protocols, nodes may be in dormant states with high probability, executing tasks only when absolutely essential. Relatively high false alarm rates are tolerated in the low-power but frequently invoked operations; operations which lower the false alarm probability to the target level are costlier, but far less frequent. With these techniques, the cost of communicating can be reduced, enabling the nodes to engage in cooperative detection and communication tasks.

In the remainder of this paper, we describe some of the design choices that are available in creating such scalable low-energy networks. In section 2 we discuss the fundamental detection and communication tradeoffs, and some of the cooperative behaviors the network will support. In section 3 we discuss the life-cycle of the network, from boot-up through maturity to failure. Finally, in section 4 we present our conclusions.

II. FUNDAMENTAL DETECTION AND COMMUNICATION TRADEOFFS

Each detection device is inherently limited in range by the background noise and the attenuation of signals with distance. This is also true for the communications system. In this section we briefly outline some of the tradeoffs in designing a distributed system to provide both sensing and communications coverage

A. **Cooperation Detection and Estimation Problem.**

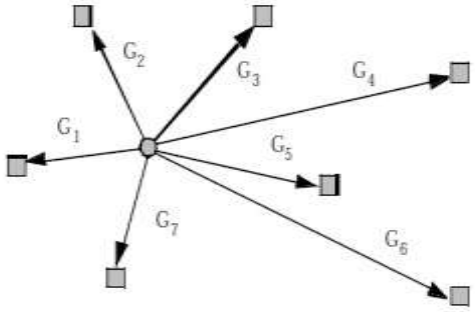

Figure 2. Propagation gains from target to sensor nodes

We may consider for example the problem of seismic detection. The Earth has a low-pass characteristic and additionally generates broadband seismic noise. Consequently, the seismic signature of any particular object gets distorted with range, and the signal-to-noise ratio (SNR) declines as the signal becomes attenuated. If the set of objects to be identified have well- defined seismic characteristics, it is possible to perform an adaptive deconvolution operation to remove the low-pass distortion based on each hypothesis, and then perform threshold tests to determine which hypothesis is most likely.Nevertheless, the higher frequencies will be less reliable, and clearly the closer sensors are to the source the more likely a reliable identification can be made. Thus, a distributed network of sensors will collect significantly different information than a system relying on a small number of highly sensitive elements at large range. A generic detection problem is

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

shown below in Figure 2, neglecting for the moment the dispersive nature of the signal propagation medium.

The simplest detection strategy is for individual nodes to make decisions on the presence or absence of the target based upon the received energy. Obviously nodes closer to the target will have a better detection probability. Suppose decision thresholds are set based upon a requirement for a particular false alarm probability. Then there will be some SNR above which detection probabilities will be acceptably high; with uniform signal propagation, we may draw detection circles around sensor, for a given source energy level. Having a slightly higher SNR will lead to an exponentially decreased probability of missed detection, so that in a certain sense the detection radius is hard. If the source lies within the detection radius of only one sensor, that sensor will be the only one communicating decisions. However, if the source lies within the detection regions of several sensors, it would be wasteful in communications resources for all to convey decisions. Rather, the sensor with highest SNR should decide (e.g., node 1 above), and inhibit the others from communicating. This can be assured by a protocol which demands that sensors wait an amount of time proportional to their decision uncertainty before passing a message. If no inhibition message has been received in that time, the sensor transmits its decision and inhibits the nearby sensors. In general, we do not need to make decisions based solely upon energy, but rather on a feature set in the data. In any case, decision thresholds and waiting times would be based upon the detection likelihoods.Now suppose that the source does not lie within the decision regions of any single sensor, but for example by performing maximal ratio combining several sensors could achieve an acceptable aggregate SNR (e.g., nodes 1,2,3,5,7). We now present a protocol that finds the minimum number of nodes required to produce a reliable decision. Nodes wait an amount of time based upon the SNR. If it is above the decision threshold, a decision is made and other nodes are inhibited. Otherwise, the node with highest SNR will be first to send out invitation signals to neighbors. The node with next highest SNR will be first to respond to the invitation by passing its data. The first node will fuse the data, and if the uncertainty is low enough, make a decision, and inhibit further activity. Otherwise, it will wait until more nodes respond to the invitation. The process stops when either a decision is made or the responses stop – indicating that the remaining nodes had SNRs below the necessary response level. A practical modification to this algorithm would be to send invitations to a pre-selected set of nodes that are likely to be within the fusion radius of the source, and for nodes to respond at discrete intervals (say measured in frames) based upon coarsely quantized SNR. We may alternatively solicit information within a predefined radius whose size depends on the SNR. Both approaches will limit latency at the expense of additional information transfer. The optimal algorithm and the practical variant are both examples of directed diffusion algorithms, in which activation and inhibition signals are used to control global network behavior (e.g., data fusion) based on local information. A very wide set of distributed computational behaviors can be synthesized in this fashion. More generally, we would wish to optimize the network resources (e.g., energy) used in making a decision and conveying it back to the end user.

When the signal wavefront exhibits coherence, then a beamforming approach can be used to both locate the target and improve the signal to noise ratio. Classically, complex weights will be applied to the outputs of a regular array of sensors to steer a main beam towards the target of interest, and nulls in the direction of interfering sources. This requires that the wavefront impinging on the array be coherent (i.e., that the phase relationships have meaning), and that the sensors have access to a common timing source. Production of beampatterns without grating lobes also requires careful design of the physical layout of the array elements. Remarkably however, both the source location and SNR enhancing functions of the array can be realized with a randomly distributed array, provided timing is supplied [1]. Since acoustic and seismic signals will be sampled at relatively low rates, the timing accuracy in a distributed network can easily be made sufficient for the task. On the other hand, lacking access to a common local oscillator makes coherent combining for such applications as radar a dubious proposition. Since clock accuracies are seldom better than parts per million, very complicated post-processing on the (oversampled) raw data would be required, to attempt to reconstruct the proper timing alignment. The inability to use phase information would change the problem from beamforming to data fusion, in that now the issue would be combining individual decisions, with weighting by the estimated probabilities of the outcomes. This non-coherent combining has a cost in the ability to locate targets (since we have only energy information), but at high SNR the detection performance is similar to coherent combining. Note that when there is a single target and a non-dispersive channel, maximal ratio combining produces the same results as coherent beamforming.

In beamforming and other cooperative detection strategies there is always the issue of how many nodes can and should be involved in making a decision. For example, consider a strong source located outside the convex hull of the sensor network. It would be undesirable for every node to become involved in beamforming to locate the target (due to the energy cost), but some clusters of nodes should act to form their own beams, so that the target can be located by triangulation. A directed diffusion process can act to achieve this aim as follows. We begin by observing that all nodes in a local region will detect similar signal strength. This condition can be recognized, and appropriate usage of inhibition/ activation signals will then cause one cluster of nodes within a predefined neighborhood to form a beam, with the vast majority of nodes uninvolved in the beamforming. This information can then be fused with that of the beams formed in adjoining neighborhoods.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

*B.*Cooperative Communication Problems

Low-power RF communications is an exercise in using more rather than less signal processing. The fundamental constraint is that circuits operating at high (RF) frequencies burn more power than those operating at low (baseband) frequencies. Therefore, techniques that can reduce the volume of data to be transmitted or the power at which it must be transmitted lead to large overall savings, even if some additional processing at baseband is required. Data reduction can be accomplished with local decision making. This can lead to orders of magnitude greater reductions in the network load than simply relying upon data compression. Secondly, diversity techniques must be exploited to reduce the average transmission power. With low cost nodes, a dense deployment will enable multiple transmission routes. The dense deployment together with multi- hopped communications will help to counteract the third or fourth power attenuation with distance typical of ground to ground communications, and closed loop power control can reduce transmission power to the minimum required for reliable transmission. Even considering the down- and up-conversion costs of a transceiver relaying messages, this will usually lead to a net power savings. Even more importantly, this will enable routing around obstacles caused by structures and terrain. For example, in urban operations a chain of sensors can be laid in buildings. In cluttered environments such as these, frequency diversity can also be of benefit.

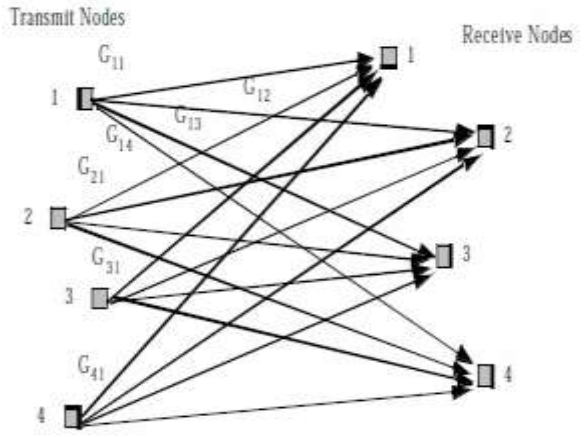

Figure 3. Cooperative communications

In the presence of fading, diversity techniques allow orders of magnitude reduction in power levels. Thus, a more sophisticated radio will use dramatically less power than a radio which has few degrees of control freedom. There will arise situations in which reliable links cannot be achieved at sufficiently high data rates, due to the inhomogeneities of both the node placement and the terrain. In this case, one possible solution is for nodes to form arrays for purposes of transmitting and receiving, as illustrated in figure 3.

The basic question we pose is how to select the collection of transmitter and receiver nodes, together with a coordinated transmission and reception strategy, so that the minimum network resources are consumed in achieving a desired information rate. The problem and the solution methods are very similar to the detection problems outlined previously. For example, if we consider a single transmitter and multiple receivers, the problem is exactly the same as multiple sensors and one source. With multiple transmitters, the problem is quite similar to classic multi-user detection problems, with the twist that we have control over what information flows from each transmitter.

The best situation would be coherent transmission and reception, in which the transmitting elements share a common phase reference, and the receivers likewise have a common phase reference. One way to attack this is as a classic beamforming problem, in that complex weights could be assigned to maximize the SNR during reception, which are close to being the optimal weights for transmission (details of different interference in the two arrays prevent this from being always true). An iterated least squares adaptation between the two arrays is often a successful approach. This may be a useful exercise for acoustic (ultrasound) communication, for which the phase jitter among nodes will be small. Additionally, space-time codes developed for radio applications may be directly applicable to this problem. They will serve to provide diversity over the link in the face of the variable path gains **Gik**, which while essentially fixed absent array mobility, are a priori unknown. However, there is likely scope for some innovation, since in contrast to the situation for mobile communications the variations in the path gains can likely be exploited – certain paths will have persistently higher capacity than others. This spatial variability of nodes adds a new dimension of complexity to the problem. In the presence of a peak energy constraint (the situation for distributed sensor networks), the capability to coherently send over **N** nodes and receive over **M** nodes can lead to an increase in the SNR by a factor of up to $\mathbf{N^2M}$, as can be deduced from the sizes of the main beams in transmission and reception, and the factor of **N** in increased radiated power. Whether this can be achieved in practice for randomly spaced elements is something that still needs to be investigated. In any case we expect the gains to be significantly diminished with large variations in the path losses, and when non-coherent transmission must be used.

As noted above, timing accuracy will be insufficient for coherent transmission at radio frequencies across the array, unless all elements are slaved to a common reference (e.g., GPS, optical beacons, etc.; this in itself is an interesting problem). There are then several ways in which to proceed with cooperative communication: a) single source, non-coherent combining in the receivers, b) single source, coherent combining in the receivers, c) multiple transmitters, single receiver, and d) multiple sources, non-coherent combining in multiple receivers. Each comes with different

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

power management issues and levels of robustness with respect to channel variations.

As for the cooperative detection problem, one issue is which collection of nodes should be involved in the cooperative communications. There are a number of subtle issues in how nodes can discover each other across a gap that is too large to permit reliable communications at the desired data rate, for single transmitters and receivers. One plausible scenario is that during network boot-up some slots are reserved for sending much lower data rate transmissions, particularly if the network knows approximately how many nodes there should be but has not discovered some sizable fraction of them. Having achieved a low-data rate link, the two subnetworks coordinate tests with different collections of nodes, with the final configuration depending on the cost/benefit of increased power consumption for higher data rate. The configuration may of course be time-varying, reflecting battery resources and network congestion. For example, we may begin with the highest- SNR link, and add progressively more links in order of the expected increase in the information rate as required, in much the same manner as was pursued for the data fusion problem.

III. NETWORK ARCHITECTURES

In this section we describe describe key aspects of WINS networking. Two such characteristics typical of WINS systems that distinguish them from packet radio and cellular networks are that the nodes are nonmobile and they have a lifetime limited by a finite energy supply. Therefore, one can expect a distinct deployment phase, which then evolves into an operational phase (although node additions/deletions are still allowed). This section concludes with a discussion of the network bootstrapping procedures. Minimization of energy consumption will be achieved not only by using low power electronics but also by turning off power- consuming resources whenever possible. Typical packet radio network protocols presume a two-state model for each transceiver: either it is transmitting or it is receiving (or attempting to receive). For a WINS network, a third state is added – OFF – and we design the protocol so that this is the most frequent state for the node to be in. This is a common technique used in radiopaging protocols.

This reflects the following important engineering principle for the WINS system design: the key communications and processing resources are capable of high enough bandwidths compared to the corresponding demands that it is unnecessary to manage them for high utilization. Rather, the key performance metric is energy conservation. Thus, the radio and sensor signal processors are "overprovisioned" so that they may operate at say 20% utilization. However, the system must only power up a resource when it performs a useful function. This maxim will be incorporated in the realtime operating system, and will also be the primary driver for communications protocol design.

Toward this end, a Time Division Multiple Access (TDMA) protocol will be used for normal operation. Nodes will be synchronized, and time slots assigned for anticipated transmissions to intended receivers. Nodes not assigned to either transmit or receive for any particular slot turn their transceivers off. Furthermore, a node that is assigned to receive in a given slot will only turn on its receiver long enough to determine whether a transmission is in fact present, otherwise it turns off for the remainder of the slot. Message transmissions will be variable length, with end-of-message detection allowing early receiver powerdown. It is possible that a preamble is transmitted to "wake up" a receiver from a relatively low power reception mode, however, our initial design approach presumes the receiver is completely off, with only the very low power clock running to awaken it for the next potential reception. Physical layer wake-up techniques are attractive for recovering synchronization or during network bootstrap. Paging and other wireless systems use addressing schemes wherein as soon as a receiving node determines from the address that it is not an intended recipient, it may turn off. Such schemes increase bandwidth utilization, which is not the primary consideration in our WINS design.

The WINS multiaccess protocol is selected to avoid self-interference. This differs from many of the early packet radio protocols, which were based on random access techniques. Random access results in wasted energy when packet "collisions" occur. However, a greater cost is caused by the need for each node to leave its receiver on continuously (unless it is transmitting), since there is no foreknowledge of when another node might begin transmitting. In a WINS network, the nodes are relatively closely spaced – a typical scenario might have them 100m apart or less. At such ranges, the energy consumed by the receiver is of the same order of magnitude as the transmitter. Thus it is paramount to turn the receiver off unless it actually has a reasonable chance of receiving something useful.

In addition to the energy conservation benefits, a TDMA protocol provides deterministic latency in message transport. (Here we refer to latency caused by medium access control; noise may arise and cause random errors at the physical layer, for which mitigating measures are needed.) This is the reason that synchronous protocols are used instead of random access for industrial control networks. Use of TDMA requires the overhead of synchronization, however, the synchronization messages serve a dual purpose of providing a heartbeat for the node. Again, this is a common technique used in industrial control. Many if not most WINS applications (e.g., security) require continuous confirmation that the system is operating properly.A further aspect of using a synchronous protocol is its inherent usefulness for the underlying WINS application. It is most likely that multiple WINS nodes are used to sense the same phenomena. Toward this end, to determine information about these phenomena it is necessary for them to be time-tagged, so that correlations may be made. Thus the WINS system must provide a time distribution service to support two functions: the application and network synchronization.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

It is noted that networking architectures have been offered that use a cluster approach, with synchronous operation within clusters but not between clusters. This is one benefit of the clustering approach – the advantages to wireless communications performance of synchronous operation are achieved, while global synchronization is not required. For a WINS system, there is a need *at the application level* for synchronization, so that proper perception may be deduced for phenomena (targets).

Since WINS will often be deployed in harsh radio environments, the use of frequency hopped spread spectrum techniques is likely. This entices us to use Code Division Multiple Access (CDMA), which provides the advantage of reducing the management of transmissions that would otherwise be in conflict. In fact, the TDMA scheduling problem is NP-complete without CDMA, while polynomial-time algorithms have been published for CDMA networks. However, CDMA causes another form of self-interference (assuming quasi-orthogonal codes), since some level of interfering energy is received in a node when another transmission using a different code occurs simultaneously. Based on our assumption that bandwidth is not scarce, and therefore we may create schedules that are less than optimal in terms of utilization, we choose to use CDMA only if the codes are orthogonal.

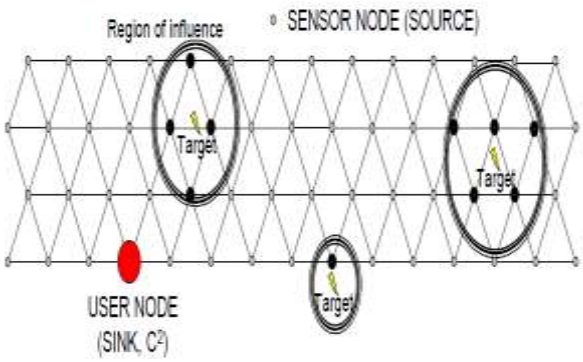

Figure 4. An example WINS network topology

The use of distributed control is an additional aid to low energy operation. Rather than each node transporting information to a central site which processes needed control (scheduling, routing, etc.), the exchanges are localized, thereby conserving overhead communications and hence energy. Distributed control is also required for self-organization capabilities; these are discussed further in the subsection describing network bootstrap procedures below. Network self-organization includes the ability to adapt to node additions and deletions as well as to traffic dynamics.

WINS distributed control extends beyond communications, and is incorporated in the sensing application as well. The network protocols are designed to support a user to issue commands, parameter changes, and download software via reliable broadcasts to the network. These actions instate the commander's intent, allowing the user to shepherd the complex adaptive system of intelligent nodes that perceive and respond directly with their environment.

The WINS network should be scalable, i.e., there should be no inherent limit to the number of nodes (although there may be a limit on density, since extreme densities can result in marginal benefit). A related goal is to allow but not require preprogamming of system parameters, such as the total (or maximum) number of nodes in the system. Similarly, protocol design should strive to not require that each node have a unique embedded serial number that is used for resolving conflicts. Uniqueness among nodes should be determined at network bootup; for example, each node's location may be used as its address. The nodes are presumed to be essentially homogeneous in their inherent capabilities, although wide disparities may arise (e.g., detection ranges) due to anomalies in a specific deployment (e.g., inhomogeneous terrain, or nonuniformity in the node locations). This architecture provides fault tolerance and graceful degradation when nodes die and/or the network becomes split into subnetworks. For a connected network, distributed control permits simultaneous but spatially distant activities to be prosecuted independently using only local interaction.

There are two extremes for WINS deployments: totally random placement of nodes (e.g., resulting from an unguided air drop), and careful manual emplacement according to an optimized spatial pattern (e.g., along the perimeter of a facility for security). A "random" spatial distribution of nodes may arise even though they are manually deployed, such as the need to place them on different machinery. Many WINS applications will call for a primarily 1- dimensional laydown of the nodes. For example, a security perimeter will be deployed as a string of nodes encircling the secured area; monitoring of road traffic will call for nodes paralleling the roadway, and nodes monitoring a river for pollutants will extend linearly along the river. To provide greater fault tolerance, the layout of nodes should be "fattened" to provide redundancy. Thus a deployment such as depicted in Figure 4 may be planned for a particular application; in this case, four rows of nodes are strung out to form a primarily 1-dimensional grid. Environmental conditions (such as rough terrain) and deployment method (e.g., delivery via ballistic munitions) can cause perturbations from the ideal topology, but the one-dimensional tendency could remain. Other factors can drive the need for different geometries. In particular, beamforming, which can be used for target location and identification, operates best if the target is within the convex hull of the sensor locations. Thus, one may choose to use multiple ranks of linear strings, so that a target is most "visible" to beamforming while it is between them. If there is a desire to track a target, then a more complete 2-dimensional covering is called for. Multi-story building applications may yield 3-dimensional geometries if between-floor radio linkage is possible.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 3, ISSN No. 2455-2143, Pages 120-128
Published Online January-February 2017 in IJEAST (http://www.ijeast.com)

The nodes are presumed to be spatially stationary; this is a critical distinction from most wireless networks, and greatly affects the choice of network protocol. A possible exception may be the user node, i.e., while the sensors themselves are fixed, a user may need the freedom to roam among them and be provided information in realtime. Sensor nodes will typically be laid on the ground, causing high propagation losses. On the other hand, a user node carried locally by a human will have an antenna that is relatively high off the ground. This implies that the user node will have a significantly higher radio range per milliwatt compared to the sensor nodes, greatly impacting the topology.All nodes will have radio transmission power control. The process of determining the proper transmit power level is part of the network bootstrap process (described briefly below). To conserve energy, the transmit power will be adjusted to the minimum possible level needed to reliably reach the intended neighboring node. Also, the nodes will typically communicate with the minimum number of neighbors needed to form a connected network. This provides the lowest energy-consuming system, since it requires less energy to transmit a message over many small hops than in one large hop, provided the small hops move the message sufficiently in the correct direction. A WINS network will generally consist of many nodes, which will be of two basic types: microsensor nodes and user nodes. A microsensor node is a "worker" node whose job is to inform the user about the environment. A "user node" is a generic designation for the end recipient of this information, and could be a device with a direct human interface, a controller (supervisory factory control and monitoring, fire control system, etc.), or a direct coupling to an end effector (actuator). A user node (as perceived by other nodes) could also be a relay node, which acts to link a remote user (or users) to the WINS network. In addition to being the recipient of the environmental information, a user provides command and control of the overall WINS network. Although both microsensor and user nodes engage in two-way communications, their traffic characteristics are very distinct. In addition, there are generally many more microsensor nodes than there are user nodes; in many moderate-sized applications, there may be only a single user node in the network.

Sensor nodes will push environmental information toward and accept commands from the user node(s). Sensor nodes will also engage in significant communications among themselves as they cooperate to improve the quality of the information produced. Figure 2 depicts how an environmental phenomenon will be sensed by a group of sensor nodes, which will create multicasting traffic. Each such node will need to query other nodes as to whether they also sensed the phenomenon, and this process may proceed dynamically until the set of nodes that sense the phenomenon is deduced, whereupon appropriate further communications within this multicast group would ensue. It is important to note that the sensing neighborhood of a node may be quite different from its radio neighborhood. Thus the networking protocol must provide an energy-efficient solution that maps the traffic demand (represented as a dynamic weighted directed hypergraph whose edges are defined by sensed environmental effects) onto the physical radio network (represented as a dynamic directed hypergraph whose edges may be created via transmission power control and nodes leaving their receivers off). Assuming bandwidth is relatively abundant alleviates this extremely complex problem. However, it is unreasonable to simply allocate a time slot for every possible type of message traffic and assume negligible energy is wasted for unused slots. For example, for a fully connected network of N nodes, there are $\mathbf{N}(2^{\mathbf{N}-1}-1)$ distinct multicast message types – a huge number. Therefore, there will be a need to establish some number of permanent virtual circuits for anticipated traffic (e.g., between nodes and the user(s)), but dynamically establish and disestablish additional communications as the need arises.

The ability for the system to self-organize will be critical to law enforcement applications. A broad spectrum of operational scenarios can be envisioned for WINS networks. Objectives range among surveillance, reconnaissance, and security. Scale ranges from large perimeter surveillance to personal security. Geometries may be 1-dimensional (e.g., a "trip-wire" line), 2-dimensional (e.g., regional coverage against possible aircraft landing), or 3- dimensional (e.g., multi-story buildings). The amount of foreknowledge and the time available for mission preparation will limit the ability to preprogram the system, to tune it for the particular application. Another critical parameter is the acceptable duration between initial deployment and when the system reaches fully operational status. Furthermore, the amount of training and level of competence required of the system user should be minimized. These various elements must be accommodated for the WINS network to be useful.

It was indicated previously that the nonmobile and finite lifetime nature of the WINS network implies there will be a distinct bootup phase. While radio resources are somewhat overprovisioned so that bandwidth is secondary to energy as a design metric, bandwidth is nevertheless not free. Therefore, it is worthwhile to expend one-time effort to establish communications links among the nodes that utilize spatial reuse. This aspect significantly alters the problem from that of earlier packet radio research. While node additions and deletions must be accommodated (including overseeding the system with new nodes), these events are expected to be relatively infrequent and tolerant of some latency in incorporating the changes in the network population.

The ability for each node and the network as a whole to self-organize will be essential to the success of the microsensor network. The efficiency of this organizational process can be heavily dependent on the particular deployment of the network and the degree and accuracy of information that is preprogrammed into the nodes. For example, if all nodes are powered up simultaneously, their attempts to find one

another will be subject to heavy contention. However, if this situation is foreseen, the nodes could be preprogrammed to awaken at slightly different times, one by one, so a much more organized startup process is used. The two extremes of "all at once" versus "one at a time" may be differentiated as "network bootup" versus "node entry," but clearly there will be intermediate cases. Our objective is to design a self-organization protocol that will always converge, even if the preprogrammed information is wrong, but will do so more efficiently with accurate prior knowledge embedded in the nodes.A top-level design has been developed for a generic node that specifies the procedural (software) flow from initial power-up through normal network operation. This provides the architectural basis describing the major components and their interfaces. These components comprise initialization routines, network discovery, network access, node type announcement, program/command injection/exchange, topology learning and position determination, neighborhood TDMA scheduling, subnetwork merging, traffic determination, routing, network TDMA scheduling, network time distribution, and dynamic circuit establishment/disestablishment. An elaboration of these techniques is presented in [2].

Another important question is what hierarchy of signal processing functionality should be imposed on the network in the interests of scalability to tens of thousands of nodes. It is clear that individual nodes must possess considerable signal processing ability in order to limit costly communications. However, other functions such as aggregation of messages to form summary reports may also be needed in order to avoid information overload on links near the terminal destination. Should every node have to support this function, or should special nodes be designated to do so? Likewise, certain nodes that have aggregated information may also have responsibility for requesting further data, so that final decisions can be made, thereby reducing the amount of traffic that must be passed upstream over congested links. The obvious problem with requiring every node to be capable of these functions is an increased signal processing hardware cost per node, but interestingly, there may be a savings in overall network power consumption by doing so, in that routing can be made more flexible, and indeed dynamic. Whether the cost of the nodes is therefore materially increased depends on what other functions they must perform and the architecture of the signal processing engine. Clearly there is also a reliability benefit from having a flat hierarchy, with functions taken up by nodes as needed. The high cost of communications as compared to signal processing leads to a different regime of tradeoffs than might ordinarily be considered in designing networks.

IV. CONCLUSION

Wireless integrated network sensor (WINS) technology will provide a bridge between the physical world and the exponentially growing information infrastructure. This technology will embed sensing and intelligence in existing products and into new products. We have described some of the cooperative network behaviors that can be enabled by this technology to make the whole much more than the sum of its individual parts. We are also pursuing research into classification algorithms that can be used in individual nodes and data fusion techniques to take advantage of the variety of sensors and the spatially separated sensing elements. As the environments in which the sensor networks may be used are highly varied, we anticipate pursuing a much expanded (and more easily automated) measurement program once our present generation of nodes has been fabricated and tested. While we have only lightly touched upon such topics in this paper, they are deep, interesting, and deserving of the attention of a large research community.

V. REFERENCES

[1] ASHTON, K. That 'Internet of Things' Thing. In the real world, things matter more than ideas. RFID Journal, 22 June 2009. Available from: http://www.rfi djournal.com/articles/view?4986

[2] BRÖRING, A. et al. New generation sensor web enablement. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652

[3] SENSEI. Integrating the physical with the digital world of the network of the future. Available from: http://www.sensei-project.eu/

[4] CHONG, C.-Y. and KUMAR, S. P. Sensor networks: Evolution, opportunities, and challenges. Proceedings of the IEEE 91(8), 2003, pp. 1247-1256.

[5] KUMAR, S. and SHEPHERD, D. Sensit: Sensor information technology for the warfi ghter. Proceedings of the 4th International Conference on Information Fusion (FUSION'01), 2001, pp. 3-9.

[6] COY, P. and GROSS, N. et al. 21 Ideas for the 21st Century. Business Week Online, 1999, pp. 78-167. Available from: http://www.businessweek.com/1999/99_35/2121_content.htm

[7] NI, L.M. China's national research project on wireless sensor networks. Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), 2008, p. 19.

[8] HATLER, M., GURGANIOUS, D. and CHI, C. Industrial wireless sensor networks. A market dynamics report. ON World, 2012.

[9] Figure courtesy of Silicon Labs and RTC Magazine: http://rtcmagazine.com/fi les/images/4151/ RTC1212_SilLabs_fi g1_medium.jpg

[10] Yole Development SA. MEMS technology: World's smallest barometric pressure sensor. Micro News, 2009,78:1.

[11] KAHN, J. M., KATZ, R. H. and PISTER, K. S. J. Mobile Networking for Smart Dust. ACM/IEEE

International Conference on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-19, 1999.

[12] ANG, R.J., TAN, Y.K. and PANDA, S.K. Energy harvesting for autonomous wind sensor in remote area. 33rd Annual IEEE Conference of Industrial Electronics Society (IECON'07), Taipei, Taiwan, 2007. [13] TANG, L. and GUY C. Radio frequency energy harvesting in wireless sensor networks. International conference on communications and mobile computing, 2009, pp. 644648.

[14] Courtesy of Shenyang Institute of Automation, Shenyang, China, 2014.

[15] FP7 EXALTED consortium, D3.3 – Final report on LTE-M algorithms and procedures, project report, July 2012. Available from: http://www.ict-exalted.eu/fileadmin/documents/EXALTED_WP3_D3.3_v1.0.pdf

[16]IEEE 802.15.4e-2012, IEEE Standard for local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer.

[17] IEEE Std 802.11™-2012, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifi cations, IEEE Computer Society, March 2012.

[18] UIMER, C. Wireless Sensor Networks. Georgia Institute of Technology, 2000. Available from: www. craigulmer.com/portfolio/unlocked/000919_sensorsimii/wireless_sensor_networks.ppt

[19] PISTER, K. and DOHERTY, L. TSMP: Time synchronized mesh protocol. [C]. Proceedings of the IASTED International Symposium, Distributed Sensor Networks (DSN 2008), 2008, pp. 391398. Available from: http://robotics.eecs.berkeley.edu/~pister/publications/2008/TSMP%20DSN08.pdf

[20] SHELBY, Z. and BORMANN C. 6LoWPAN: The wireless embedded Internet. New York, NY, USA: John Wiley & Sons Ltd, 2009. Available from: http://elektro.upi.edu/pustaka.elektro/Wireless%20 Sensor%20Network/6LoWPAN.pdf

[21] Sensinode. Available from: www.sensinode.com\\EN\\products\\software.html

[22] 6LoWPAN Sub1GHz Evaluation kit. Texas Instruments. Available from: www.ti.com/tool/CC-6lOWPAN-DK-868

[23] HUI, J., CULLER, D. and CHAKRABARTI, S. 6LoWPAN: Incorporating IEEE 802.15.4 into IP architecture. IPSO, Industrial Ethernet Book Issue 59, 1997. Available from: http:// www.iebmedia.com/index.php?id=7176&parentid=63&themeid=255&hft=59&showdetail= true&bb=1&PHPSESSID=a3tc6d9vhs5ab6svu8ahcb4c10

[24] BLILAT, A., BOUAYAD, A., CHAOUI, N. and EL GHAZI, M. Wireless sensor network: Security challenges. Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 6872. Available from: http://novintarjome.com/wp-content/uploads/2014/05/Wireless-Sensor-Network.pdf

[25] JAIN, A., KANT, K. and TRIPATHY, M. R. Security solutions for wireless sensor networks[C]. Proceedings of the 2012 Second International Conference on Advanced Computing and Communication Technologies (ACCT '12). IEEE Computer Society, 2012, pp. 430433.

[26] WANG, Y., ATTEBURY, G. and RAMAMURTHY, B. A survey of security issues in wireless sensor networks IEEE Communications Surveys and Tutorials 8, 2006, pp. 223.

[27] ALZAID, H. Security map for WSN. 2009. Available from:http://www.wsn-security.info/Security_ Map.htm

[28] MARTIN, T., HSIAO, M., HA, D. and KRISHNASWAMI, J. Denial-of-service attacks on batterypowered mobile computers. Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), IEEE, 2004, pp. 309318. Available from: http://www.ece.vt.edu/ tlmartin/power-secure/percom_martin_camera-fi nal.pdf

[29] FALK, R. and HOF, H.-J. Fighting insomnia, a secure wake-up scheme for wireless sensor networks. Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09), Athens/Glyfada, Greece, 18-23 June 2009, pp. 191196.

[30] LE X. H., SANKAR, R., KHALID, M., and SUNGYOUNG, L. Public key cryptography-based security scheme for wireless sensor networks in healthcare. Proceedings of the 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC '10). ACM, 2010.

[31]K. Yao, R. E. Hudson, C. W. Reed, D. Chen, and F. Lorenzelli, "Blind beamforming on a randomly distributed sensor array system," to appear, *IEEE J. Selected Areas in Communications*, Nov. 1998.

[32] G. J. Pottie, W. J. Kaiser, L. P. Clare, and H. O. Marcy, "Wireless integrated network sensors," submitted to *IEEE J. Selected Areas in Communications.*