IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Sensor Usage and Training with Realtime Application

Sasikumar M[*1], Narendran M[2]

[*1]Final Year, Tagore Institute of Engineering and Technology, Salem, Tamilnadu, India
[2]Assistant Professor, Tagore Institute of Engineering and Technology, Salem, Tamilnadu, India
jmjsasi@gmail.com

Abstract

In this paper shows the basic concept on sensor networks, which has been made feasible by the convergence of micro electro-mechanical system, wireless communication and digital electronic. At first the sensing charge and the potential sensor network applications are shown. The communication structural design for sensor network also delineated. The algorithm and protocols of the sensor network are discussed. Then open research issues of sensor network are investigated and work with trained sensor network with trained sink. A massive deployment of sensor nodes to produce globally meaning full information from data collected by individual sensor nodes.

Keywords: Include at least 5 keywords or phrases

Introduction

Recent process in micro-electro-mechanical system(MEMS),wireless communications and digital electronics have facilitate the maturity of low cost, low pore multifunctional sensor nodes that are small in size and communicate untethered in short distance. There minuscule sensor node, which consist of sensing data processing and communicating components, influence the idea of sensor network based on mutual effort of node. Sensor network. Symbolize a considerable expansion over conventional sensors, which are arranged in the following two ways.

- Sensor can be spotted outlying from the authentic incident
- More than a few sensors that perform only sensing can be organized.
- They broadcast time series of the sensed incident to the inner node, where the calculations are done and data are merged.

A sensor network is poised of a large number of sensor nodes, which are compactly organize either inside the incident or very near to it. The position of the nodes head not be pre- determined. A unique feature of sensor network is the co-operative efforts of sensor nodes.

Some of the application areas of sensor networks are military, health, security etc…

Application

Sensor network consist of different types of sensor they are low sampling rate magnetic, thermal, seismic, infrared, visual radar, and acoustic. Which are able to visible avoid a verity of ambient, stipulation that include the following.

- Temperature,
- Humidity,
- Lighting condition,
- Vehicular movement,
- Pressure,
- Soil makeup,
- Noise level,
- Presence and absence of certain kinds of objects
- Mechanical stress level
- Character

Sensor nodes are used for incessant sensing, event id, location, and above all functions. These process of sensing through a wireless communication may used for many application they are

- Military
- Society
- Health
- Home application
- Commercial

Some of the influencing factors of sensor network design.

A) Military

Some of the systems like (C4ISRT) play a major role in military such as, command, control, communication, intelligence, reconnaissance, computing and targeting. It also play a characteristic of sensing techniques. Some sensor networks are based on dense position of discarding and low cost sensor nodes, thus, the discarding of some nodes does not affect a military operation. It makes a sensor network concept a better approach for battlefield.

Some of the special application that sensor network performs in military such as

- Updating neighbor forces, equipment and function
- Battlefield path
- Targeting
- Damage assessment
- War detection

Updating Neighbor, Equipment And- Function: commandos can dynamically monitor the status of neighboring forces, their condition and their equipment status by the use of sensor networks. The gathering information is passed to the upper level of commandos or leaders.

Battlefield Path: The routes and straits are visible clearly covered with sensor networks and all the activities are closely watched through the sensor survey line.

Targeting: Through the sensing nodes we, can easily target the object.

Damage Assessment: To access the damage after the attack. The sensors are used to gather the damages.

War Detection: Suppose our neighboring country planned to biological and chemical attack the sensor can easily detect the chemical or biological warning.

Atmospheric application:

Some atmospheric application of sensor networks includes tracking the action of animals, birds, insects and also it monitor the environmental condition. Some of the main applications are,

- Monitoring the soil condition
- Weather conditioning
- Fire detection in forest
- Agricultural
- Oceanographic
- Inundation detection etc…

Monitoring The Soil Condition: It maintain the mineral wealth detail. Present in the soil. That may used for agricultural purpose and also used to find the density of the soil that may help to avoid the soil errousition.

Inundation Detection: To detect the inundation (or) flood some ALERT systems are organized in us about more than 90 ALERT system .were founded with sensor to protect our environment (or) surrounding.

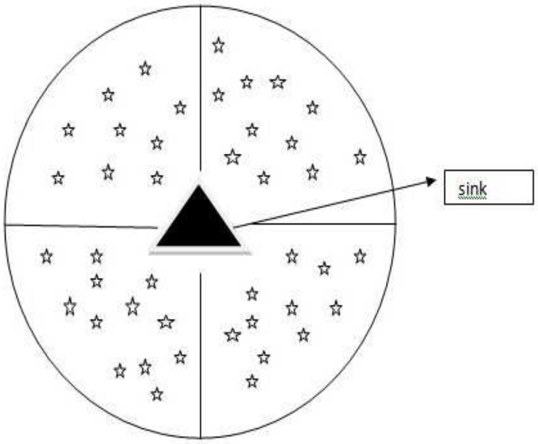
Fire Detection In Forest: Sensor node can be easily relay the exact origin of the fire to the end user before the fire is spread and also the sensor are well equipped with effective power scavenging method.

Maintaining Physical Condition: To maintain the physical fitness sensor network provides an interface for the disabled, some applications are monitoring patient health condition, diagnostics drug therapy.

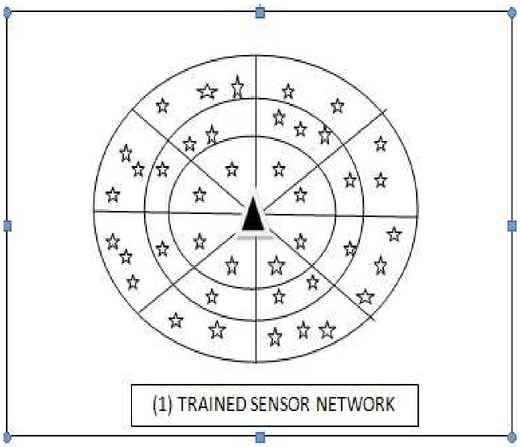
Monitoring Patient Health Condition: The physical data about a patient are collected by the sensor network and can be stored for a long period.

Training a wireless sensor network:

In this work, we assumed that the wireless sensor networks consist of sink and a set of sensors that randomly circulated in its broad case range as shown in diagram(1).



(a) SINK NODE



(1) TRAINED SENSOR NETWORK

To reduce the difficulty, we assume that the sink is placed in center although this is not really necessary.

The task of giving sensor with rude grain location awareness. Where the set of sensors deployed, in an area is separated in to cluster. As a result of training, we force to organize system on to the sensor networks. In such a way each sensor belongs to exactly on one cluster. The organized system divides the sensor network in to equiangular packs. In turns, these packs are divided into sectors by means of coronas centered at the sink and whose radii are determined to optimize the cluster and sensor begin one to one.

B) Securing Wireless sensor Network

The task of securing wireless sensor network is complicated by the fact that the sensors are mass-produced unspecified device.

Wireless sensor network are sufficiently different from ad-hoc network that security designed specifically. Thus it was recently noted that the ultra-lightweight protocol imposed by the inflexible energy limitation may leave not much room for advanced encryption schemes. As a result protection against over hearing in military application and privacy protection in personal system needs to be inherently built in to the concept if sensor network models and protocols. Reliability is expected as a result of large number of sensors deployed for specific operation.

C) Our Hand-Out

We view our hand-outs at several levels:

- First we propose a dynamic coordinate system for a extraordinarily deployed collection of large sensor nodes. It yields at no extra cost.
- A clustering scheme: If they have same coordinates the node to be in same cluster. It shows the virtual infrastructure.
- Then we move on to show that training of the sensor nodes through this process nodes learn their coordinates. It can be performed by a protocol that is at the same time light weight and secure. Indeed we mapped a way of making the training protocol secure by wing a parameterized variant of frequency hopping.
- Next we show that a trained wireless sensor network routing and data function can be act by very simple and energy-efficient protocols.
- Finally we show how to design to coordinate system such as to minimize the power consumption in collecting and routing data.

  The reminder of this paper is developed as is follows.

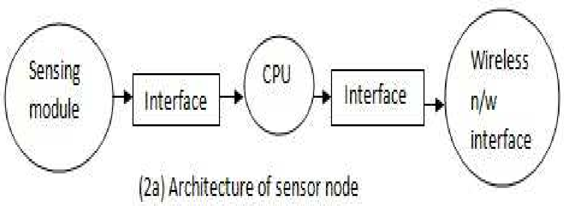
The Model of Sensor Nodes

We assume that the sensor node to be a device that process on the basic three capabilities. Sensor, computation and wireless communication as illustrate in figure (2a).

The sensory function is necessary to acquire data from the environment. The computational function is necessary for the process control information. For aggregating data and to managing both sensory and communicational activity. Finally the wireless communication function is necessary to sending (receiving) aggregated data and control information to (from) other sensors or the link.

We consider that individual sensor nodes operate subject to following fundamental constraints.

- Sensor nodes are anonymous they do not have fabrication time identities.
- Sensor nodes are tiny, commodity devices that are mass produced in an environment where testing is luxury.
- Each sensor as a non-renewable energy budget. When the power supply is exhausted, the sensor is expired.
- In order to save energy, each sensor node is in sleep mode most of the time, waking up at random points in time for short intervals for their process.
- Each sensor has a some special transmission range, perhaps a few meters. This shows that the messages. Passed by a sensor can reach only the sensor in its proximate time.
- Individual sensor nodes must work unattended.



(2a) Architecture of sensor node

At any point in time, a sensor will be engaged in performing one of a finite set of possible operation, in other words will be as sleep.

The basic operations of sensing are,

Data Fussion: To collect raw measurement.

Aggrication: To drive target data from raw measurement.

Routing: To communicate raw measurement, target data and control data.

We consider that each operation performed by sensor consumer small amount of energy and sleeping performances by sensor consumes no energy.

It is efficient mentioning that while the energy budget can supply short-term application, sensor detected to work over years may need to scavenge energy from the specific environment for temperature, light, kinetic, magnetic field, vibration etc.

A) Protocol Implementation

The node's of genetic material play a key role in driving the functionality of different node protocols. To describe this we consider protocol implementation for security solution for the sensor network.

We assume that at pre-deployment time the sensor nodes are passed, in a secure environment with the following

Pseudo Random Number: one of public domain algorithm available.

Secret Seeds: to be used as a parameter for the random number generator.

Initial Time: at this time all the sensor nodes are synchronous to the sink node.

It I important to note that immediately after deployment all the clocks am synchronous. In time however, clocks will drift and re-synchronization will be become necessary. We consider the synchronization is always done to the master clock running at the sink. Our main aim is a light weight re-synchronization protocol.

Classical frequency hopping mechanism have as a mean of computing jamming both hostile and non hostile of implementing frequency diversity. These mechanisms offered little cryptographic value.

Cryptographic technique such as encryption that are used to address security problems in all the physical in the network. The key idea of our proposed security solution is that by extending classical frequency happing techniques using cryptography, security problems in the physical layer, as well as the network layers can be uniformly addressed in a unified frame work. We call this frame work as randomized frequency hopping.

We are new at the status to show the genetic material is used in support of secure communications in sensor networks. For this process it is useful to image three sequence of random number as follows.

- An infinite sequence of t1, t2… ti.. of time lengths.
- Fsf
- Sdsd

Through the genetic material these sequence can be generated locally by each sensor nodes so that no need to be communication after deployment.

We assume that time is ruled in to epochs. During the ith time epoch, of length ti, a frequency set ni will be subjected to hopping patten and to the sequence of adhslfuifhflsfdsdjj. Thus for a long sensor node is synchronous to the sink, it show the current time epoch. The hopping patterns appear as the product of an unknown random process to an outside observer, however successive epoch length. Hopping set and to the hopping Patten appearance. These techniques are used to show the hopping sequence by monitoring transmission, and the choice of frequency parameter is to determine the magnitude of the challenge to an adversary.

B) Tamper-Resistant

The most obvious tamper resistance strategies are hardware based and involves some special hardware circuits, with in the sensor node. To protect sensitive data, with special coatings (or) tampers seals. However hardware solution to the tampering problem increases the cost and hardware complexity of sensor nodes. The additional hardware is very likely to consume valuable energy and also the seals with coating used for the protection. Thus the tamper-resistant (or) seals are used in present day sensors.

The potential of physical tampering attack and function of unattended, are mostly used in

Wireless sensor network. ie) post deployment tamper detection also the physical tampering may compromise only node attacked or the entire network our preference to endow individual sensor nodes with temper resistance does not require more sophisticated hardware .

In order to set the stage of our solution as, by the tampering thread model assume that the adversary is, Force to open an individual sensor nodes in suit; or Physically removing to sensor nodes from the deployment area.

We proposed against the first thread by blanking out the memory, triggered by a simple switch. We proposed against the second thread by relying on local data, that the sensor can collect. After that we set specified frequency for the hopping during its wake time. This allows the individual sensor nodes to collect an array of signal Strength from the sensor in their locale. It is important to recall the array of signal strength is the only data available to the sensor nodes. It establishes the neighborhood of the nodes. For this specification the array will be referred as the nodes neighborhood signature array i.e.) (NSA, for short). If the nodes is removed from the array the changes in the signals recessives when compared to NSA and erase its own memory to prevent the tampering agent from gaining access to information secrete to the sensor networks. These sort of tampering attempts involves the removal of several sensor nodes will also defected the set of removed nodes will notice changes in its NSA and can alert the others.

Structure of Wireless Sensor Network

We provide a massive deployment of sensor nodes perhaps in the thousands or even ten thousands. The sensor nodes are aggregated in to computational and communication infrastructure, called a wireless sensor networks. Whose aim is to produce globally meaningful information from data collected by individual sensor nodes? However, the deployment of massive sensor nodes in a sensor networks. Joint with anonymity of individual sensor, with limited power budget and in many applications pose daunting challenges to the design to protocol for sensor network, for a thing, the design of ultra-light weight communication protocol to the design of getting at the individual sensor node level. The direction is to perform the process of local data processing at the sensor level, to avoiding the transmission of raw data through the sensor network, are the important measure. It is known as the cost of energy to transmit 1kb of data to a distance of 100meter at 3J, using the same amount of energy, a general-purpose processor with the modest specification of 100millions watt executes 300millions instruction.

For the reason of scalability a consequence of sensor network must be multiple-hop and it is assumed that no sensor nodes knows the topology of the network.

Our contribution on the design of ultra-light weight organization and communication protocols for a class of wireless sensor network consisting of a single sink node and for the transmission range of the sink. A large number of sensor nodes randomly deployed.

A basic problem to solve in wireless sensor networks is to balance the utility of activity in the network against the cost.

Interfacing the sensor network is converted to outside world (ex: internet etc) through a gateway node. The gate way node may or may not be collected with the sensor nodes in the deployment asked as show in figure 1.we calculate to interface with the outside world may be achieved by a helicopter or aircraft over flying the sensor network, and collecting the set of information . for such communication between individual sensor nodes by radios through, the reporting nodes are communicated with the external way that is shown in the below structure 2. Reporting nodes are communicating with the external gateway by laser.

One can easily have a mobile sink, or collection of mobile sinks for fault tolerance, assume the role of the gateway in the network. In case the sink is collocated with the sensor network, it can also be in charge of performing any necessary training and maintenance operations.

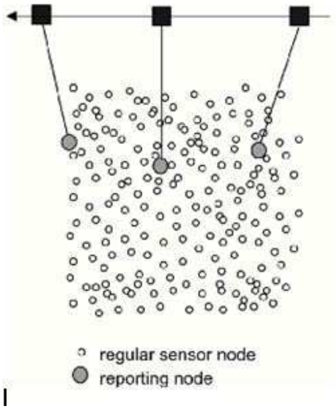


Figure 2. A sensor network with a mobile external gateway.

A somewhat complementary view, illustrated in figure3 is to have a sink node collocated with the sensor nodes play the role of the gateway. In this case, the sink node has a full range of computational capabilities, can send long-range directional broadcasts to all sensors, can receive messages from nearby sensors, and has a steady power supply. However, since the sink is a single point of failure in this model, we envision that in practice multiple (backup) sink nodes will exist in the network.

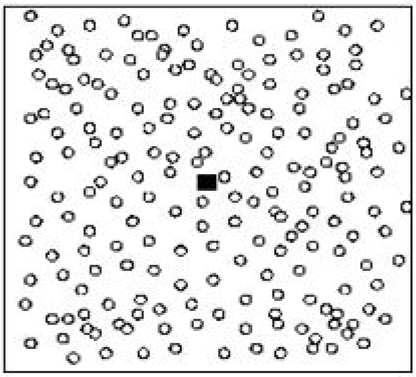
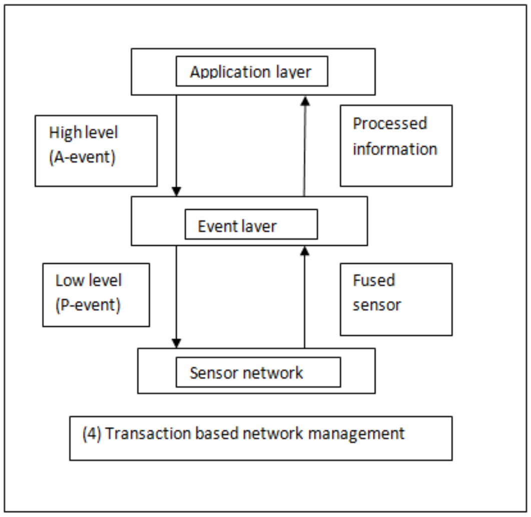


Figure 3. A sensor network with a central sink node.

Performance Model for Wireless Sensor Network

We take the view that the sensor network performs the tasks mandated by an end-user (perhaps a point of command and control) that is remote from the network itself. Assuming the sensor network model depicted in figure 3, the sink node serves as the interface between the end user and the network. We characterize the work activity in the network in terms of an event model. Under the event model, the utility of the sen- sor network is measured by the time period during which it guarantees a specific Quality of Service (QoS) for detection and notification of event types of interest to the application.



Based on this work model, we propose a hierarchical multi- level network management approach, as illustrated in figure4. The hierarchy involves the following layers:

- Application layer: high-level consumers of information produced by the sensor network;
- Event layer: provides the interface between the sensor net- work and the application layer.

We now discuss each layer in detail. Referring to figure4, the application layer issues high-level requests, of a coarse semantic granularity defined in terms of application-level abstractions, referred to as Application events (A-events, for short) to be performed by the sensor network. The A-event is a task that takes the form of a tuple consisting of a high-level action, along with a desired level of QoS. As an example, the A-event (Fire, p) requires that the occurrence of fire be detected in the area of interest with probability at least p. Here, of course, p specifies the requested QoS.

The event layer provides the interface between the application layer and the sensor network. This layer receives A-events, i.e., high-level tasks and QoS requests from the application layer, considers the current state of the sensor network and its capabilities including the remaining energy bud- get both globally and within the individual clusters, and then negotiates a contract with the application layer before com- mitting the network. Due to this negotiation, the network will not squander resources needlessly by attempting to carry out an A-eventthat it does not currently have the resources to provide. Also a set of A-events queueing for service in the event layer will be prioritized in order to get the greatest benefits from the sensor network. After a contract has been agreed upon, the event layer translates the corresponding A-event into individual tasks, termed primitive events (P-events, for short), assigned to individual clusters. The clusters must then perform these tasks at the QOS level required and send the data back to the sink for further consolidation and analysis in the event layer. The polished information from this effort is provided to the application layer for proper dissemination. To continue our example, assume that the event layer determines that the A-event (Fire, p) is feasible for the sensor network. Assuming that the occurrence of fire is predicated on high temperature, low humidity and the presence of smoke, the event layer will then translate (Fire, p) into the following (P-events):

- (Temperature, t0, q): detect with probability larger than q whether the temperature reading is higher than thresh- old t0.
- (Smoke, q┐): detect with probability larger than q┐ that there is smoke.
- (Humidity, h0, q┐ ┐): detect with probability higher than q┐ ┐ whether the humidity is lower than threshold h0.

On the other hand, if the A-event (Fire, p) is infeasible for the sensor network, the event layer will negotiate with the application layer for a new task, for example, (Fire,p ┐) with p┐ <p .

Training a Wireless Sensor Network

It was recognized that some applications require sensory data with some location awareness, encouraging the development of communication protocols that are location aware and per- haps location dependent. The practical deployment of many sensor networks will result in sensors initially unaware of their location: they must be trained in this vital information. Further, due to limitations in form factor, cost per unit and energy budget, individual sensor nodes are not expected to be GPS-enabled. Moreover, many probable application environments limit satellite access.

The localization problem is for individual sensor nodes to determine, as closely, as possible their geographic coordinates in the area of deployment. Prominent solutions to the localization problem are based on multi alteration [7–9, 12, 16, 29, and 33]. Most of these solutions assume the existence of several anchor nodes that are aware of their location (perhaps by endowing them with GPS-like devices). Sensor nodes receiving location messages from at least three sources can approximate their own locations. For a good survey of localization protocols for wireless sensor networks we refer to [25].

In some other applications, exact geographic location is not necessary: all that the individual sensor node need is coarse-grain location awareness. There is an obvious trade- off: coarse-grain location awareness is lightweight but the resulting accuracy is only a rough approximation of the ex- act geographic coordinates. Figure 5 illustrates a possible way of inducing such a coarse-grain location awareness by an over flying aircraft or helicopter. All that the individual sensor nodes need is to determine their approximate distance to three different positions of the training agent. We omit the details.

Our approach is different: we obtain this coarse-grain location awareness by the training protocol that imposes a

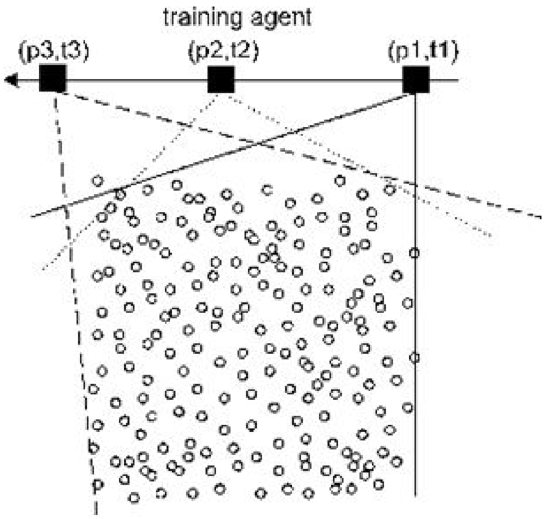


Figure 5. Acquiring coarse-grain location awareness.

Coordinate system onto the sensor network. An interesting by-product of our training protocol is that it provides a partitioning into clusters and a structured topology with natural communication paths. The resulting topology will make it simple to avoid collisions between transmissions of nodes in different clusters, between different paths and also between nodes on the same path. This is in contrast with the majority of papers that assume routing along spanning trees with frequent collisions.

Clustering was proposed in large-scale networks as a means of achieving scalability through a hierarchical approach. For example, at the medium access layer, clustering helps increase system capacity by promoting the spatial reuse of the wireless channel; at the network layer, clustering helps reducing the size of routing tables and striking a balance between reactive and proactive routing. It is intuitively clear that wireless sensor networks benefit a great deal from clustering; indeed, separating concerns about inter-cluster management and the intra-cluster management can substantially decrease, and load balance the management overhead. Given the importance of clustering, a number of clustering protocols for wireless sensor networks have been proposed in the recent literature [5,11,15]. However, virtually all clustering proto- cols for wireless sensor networks assume tacitly or explicitly that individual sensor nodes have identities. As it turns out, our clustering protocol has the following desirable features:

- lightweight as a by-product of training;
- organizes anonymous asynchronous nodes;
- a cluster is the locus of all nodes having the same coordinates; and
- Individual nodes need not know the identity of other nodes in their cluster.

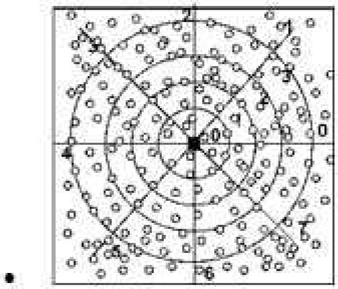


Figure 6. A trained sensor network.

In the remainder of this work we assume a wireless sensor network that consists of a sink and a set of sensors randomly deployed in its broadcast range as illustrated in figure 3. For simplicity, we assume that the sink node is centrally placed, although this is not really necessary. The task of training refers to imposing a coordinate system onto the sensor net- work in such a way that each sensor belongs to exactly one sector. The coordinate system divides the sensor network area in to equiangular wedges. In turn, these wedges are divided into sectors by means of concentric circles or coronas centered at the sink and whose radii are determined to optimize the transmission efficiency of sensors-to-sink transmission as will be discussed later. Sensors in a given sector map to a cluster, the mapping between clusters and sectors is one-to-one. Referring to figure6, the task of training a sensor network involves establishing:

Coronas: The deployment area is covered by k coronas determined by k concentric circles of radii r1 <r2 < · · ·<rk centered at the sink node.

Wedges: The deployment area is ruled into a number of angular wedges centered at the sink node.

As illustrated in figure6, at the end of the training period each sensor node has acquired two coordinates: the identity of the corona in which it lies, as well as the identity of the wedge to which it belongs. Importantly, the locus of all the sensor nodes that have the same coordinates determines a cluster.

Routing and Data Fusion in a Trained Sensor Network

The main goal of this section is to show that once a wireless sensor network has been trained, both routing and data fusion become easy and straightforward.

A) **Routing**:

The routing problem in sensor networks differs rather substantially from routing in other types of wireless networks. For one thing, individual sensor nodes do not have unique identifiers; thus, standard addressing methods do not work directly. For another, the stringent energy limitations present in sensor network render the vast majority of conventional routing protocols impractical. Given the importance of routing, it is not surprising to see that a number of routing protocols specifically designed for wireless sensor networks were proposed in the literature. For example, in [21] Intanagonwiwat et al. describe directed dif- fusion and a companion routing protocol based on interest tables at the expense of maintaining a cache of information indexed by interest area at each node.

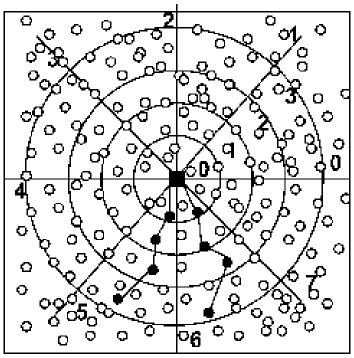


Figure 7. Illustrating communication paths to the sink.

Shah and Rabaey [34] responds to client requests by selecting paths that maximize the longevity of the network rather than minimize total power consumed by a path with path options established by local flooding. The protocols of Kulik et al. [24] are based on a push-pull system where the nodes send metadata first using routing that is optimal for point-to-point communication, but does not benefit from established predefined paths. Other routing protocols include rumor routing [6], and multi-path routing [14], among others. As we are about to demonstrate, our training protocol provides a novel solution to the routing problem by yielding energy efficient paths based routing.

Recall that sensor networks are multi-hop. Thus, in order for the sensing information to be conveyed to the sink node, routing is necessary. Our cluster structure allows a very simple routing process as described below. The idea is that the information is routed within its own wedge along a virtual path joining the outermost sector to the sink, as illustrated in figure7. The collection of all the virtual paths (one per wedge) defines a tree. In this tree, each internal node, except for the root, has exactly one child, largely eliminating MAC level contention in sending sensor information to the sink.

Recently, a number of MAC layer protocols for wire- less sensor networks have been proposed in the literature [36,41,43]. It’s worthwhile to note that in our routing scheme by appropriately staggering transmissions in neighboring wedges, collision and, therefore, the need for retransmissions is completely eliminated. Thus, our training protocol implies an efficient MAC protocol as well.

B) **Data Fusion**:

Once sensory data was collected by a multitude of sensor nodes, the next important task is to consolidate the data in order to minimize the amount of traffic to the sink node. We place the presentation in the context of our work model. To be more specific, we assume that the cluster identified by (I, j) – that is, the set of sensor nodes located in sector Ai, j, where i is the corona identifier, and j is the wedge identifier, are to perform a certain task T. A number of sensors in sectors A1,j,A2,j,...,A i−1,j are selected to act as routers of the data collected by the sensors in Ai, j to the sink. Collectively, these sensors are the support sensors of task T.

It is, perhaps, of interest to describe the process by which the sensors associated with T are selected. To begin, during a time interval of length the sink will issue a call for work specifying the identity j of the wedge in which the task is to be performed, as well as the identity i of the corona in which data is to be collected. The sensor nodes in wedge j that happen to wake up during the interval and that have an appropriate energy level stay awake and will participate in the task either as either data collectors or as routers depending on their respective position within the wedge. It is intuitively clear that by knowing the number of sensors, the density of deployment and the expected value of sleep periods, one can fine tune in such a way that a suitable number of routers will be awake in wedge j in support of T. Likewise, we can select the set D of data collecting sensors in Ai, j. Let S denote the set of support sensors for T. It is appropriate to recall that a by-product of the call for work is that all the sensors in S are synchronized. In order to make the task secure the sensors in S will share a secret key that allows them access to a set of time epochs, a set of frequencies to be used in each time epoch, and a hopping sequence to be used within each epoch. For details we refer the reader to the description of the randomized frequency hopping security framework proposed in section 2.

Assume that the results of the data collection specific to task T can be partitioned into 2m (m   0), disjoint groups. Thus, each sensor performing data collection will encode its data in a string of m bits.

Since, typically, D contains a large number of sensors, it is important to fuse individual results into a final result that will be sent to the sink node. We now outline two possible solutions to the data fusion problem. Using the algorithm of Nakano and Olariu [26] that does not require sensors to have identities, the sensors in D acquire temporary identities ranging from 1 to |D|. Using their newly acquired identities, individual data values are being transmitted to the sensor whose identity is 1 who will perform data fusion and will send the final result to the sink node as discussed in section 7. The advantage of this data fusion scheme is that there is no data loss and all the collected values will be correctly fused. There are, however, many disadvantages. For one thing, the initialization algorithm of [26] requires every sensor in D to expend an amount of energy proportional with log |D|. For another, the final result of the data collection is concentrated in a single sensor (i.e., the sensor with temporary identity 1), who is a single point of failure.

We now propose a much simpler data fusion scheme that involves some data loss but that is fault tolerant and does not require the sensors in D to have unique identities. The idea is that the sensors in D transmit the data collected bit by bit starting, say, left to right as follows: a value of 0 is not trans- mitted, while a 1 will be transmitted. The sensors in Ai−1,j that have been elected as routers in support of transaction T pick up the values transmitted. The following disambiguation scheme is used:

- No bit is received – in this case a 0 is recorded;
- A bit of 1 is received – in this case a 1 is recorded;
- A collision is recorded – in this case a 1 is recorded.

It is clear that as a result of this disambiguation scheme, every sensor in Ai−1,j that is in support of T stores the logical OR of the values stored by sensors in D. Note also that while there was loss of information in the process of fusing data, no further loss can occur in traversing the path from Ai−1,j to the sink: this is because all routers in Ai−1,j transmit the same bit string.

C) **An Example**:

For an example of data fusion consider a sensor network that is tasked to monitor and report the temperature in cluster Ai, j. Referring to table 1, for the application at hand temperatures below 111 F are considered to be non-critical and if such a temperature is reported no specific action is to be taken. By contrast, temperatures above 111 F are considered to be critical and they trigger a further monitoring action. The encoding featured in table 1 is specifically designed to reflects the relative importance of various temperature ranges. For example, the temperature ranges in the non-critical zone are twice as large as those in the critical zone. Also, notice that the left- most bit differentiates critical from non-critical temperatures. Thus, if the sink node receives a reported temperature whose leftmost bit is a 1, then further action is initiated; if, on the other hand, the leftmost bit is 0, then no special action is necessary.

a) Trading energy for lossless data aggregation/reporting.

Let us see how our data fusion works in this context. Referring to figure8(a) assume that a group of three sensors d0, d1, andd2 in Ai, j have collected data and are about o transmit it to the sensors s0 and s1 in Ai−1,j. The values collected are encoded, respectively, as 0110, 0101 and 0110. Thus, none of the values indicates acritical situation. After transmission and disambiguation, the sensors in Ai−1,j will store 0111 which is the logical OR of the values transmitted. Notice that although the data fusion process involves loss of information, we do not loose critical information. This is because the logical OR of non-critical temperatures must remain non-critical. Conversely, if the logical OR indicates a critical temperature, one of the fused temperatures must have been critical and thus action must be initiated. It is also interesting to note that when the sensors in Ai−1,j transmit to those in Ai−2,j no further loss of information occurs. There is an interesting interplay between the amount of loss in data aggregation (fusion) and the amount of energy expended to effect it. As we are about to show, if we are willing to expend slightly more energy, lossless data aggregation can be achieved. The corresponding tradeoff is interesting in its own right being characteristic of choices that present themselves in the design of protocols for wireless sensor networks. For illustration purposes, assume that it is necessary to determine the maximum of the bit codes stored by the sensors in Ai, j. To solve this problem, all the sensors in Ai, j that have collected relevant information engage in the following protocol that is guaranteed to aggregate the values into the maximum. Assume that each sensor stores an n-bit code for the range. Starting with the highest significant bit to the lowest:

1. Sensors in Ai, j that have a 0 in position p listen for two time slots; if in any of these slots a 1 or a collision message is received, they terminate their participation in the protocol.

2. Sensors that have a 1 in position d transmit in the first time slot and sleep in the second.

3. Sensors in Ai−1,j do the following: 3.1. Any sensor that has received a 1 or a collision in the first slot, echoes a 1 in the second.

3.2. Any sensor that has not received a transmission in the first slot sleeps in the second slot.

Figure 8(b) illustrates how the maximum of the values collected by sensors d0, d1, andd2 in Ai, j is correctly communicated to the support sensors s0, ands1 in Ai−1,j. In this case, we assume d0, andd1 are not in direct communication range of each other. Note that s0 receives a collision corresponding to the third most significant bit; consequently it echoes a 1, thereby enabling d1 to terminate the protocol. Similarly, s1 receives a collision, and echoes a 1 for the same bit position (not shown in the figure). It is easy to confirm that by exploit- ing the associatively of the maximum, the simple protocol that we just outlined correctly forwards to the sink the maximum of the values stored by sensors in Ai, j.

b) Our lightweight training protocol:

Our proposed model for a sensor network assumes that after deployment the sensor nodes must be trained before they can be operational in the network. Recall that sensor nodes do not have identities and are initially unaware of their location. It follows that untrained nodes are not addressable and can- not be targeted to do work in the network. The main goal of this section is to present, in full detail, our lightweight highly scalable training protocol for wireless sensor networks. The key advantage of this protocol is that each node participating in the training incurs an energy cost that is logarithmic in the number of clusters and wedges defined by the protocol. Being energy efficient, this training can be repeated on a scheduled or ad-hoc basis providing robustness and dynamic reorganization. After deployment nodes sleep until wakened by their individual timers. Thus, each node sleeps for a random period of time, wakes up briefly and if it hears no messages of interest, selects a random number x and returns to sleep x time units. Clocks are not synchronized but over any time interval [t, t+ t]a percentage directly proportional to t of the nodes are expected to wake up briefly. During this time interval the sink continuously repeats a call to training specifying the current time and a rendezvous time. Thus, in a probabilistic sense a certain percentage of nodes will be selected for training. The time interval t can be adjusted to control the percentage of nodes that are selected. Using the synchronization protocol we describe in section 5.1 the selected sensors nodes reset their clocks and set their timer appropriately before returning to sleep.

c) The Synchronization Protocol:

It is natural to assume that, just prior to deployment, the sensor nodes are synchronized. However, due to natural clock drift, re-synchronization is necessary. Re-synchronization is done with respect to the master clock running at the sink. Suppose that the sink dwells τ micro-seconds on each frequency in the hopping sequence. For the purpose of showing how synchronization is effected, assume that time is ruled into epochs as discussed before. For every i (i 1), we letli stand for └ ti/τ┘ ; thus, epoch ti involves a hopping sequence of length li. We can think of the epoch ti as being partitioned into li slots, each slots using its own frequency selected by virtue of the hopping sequence out of the set ni of frequencies associated with epoch ti. It is clear that determining the epoch and the position of the sink in the hopping sequence corresponding to the epoch is sufficient for synchronization. Our synchronization protocol is predicated on the assumption that clock drift is bounded. Specifically, assume that whenever a sensor node wakes up during its local time epoch ti the master clock is in one of the time epochs ti−1, ti, orti+1. Using its genetic information, the sensor node knows the last frequencies λi−1, λi and λi+1 on which the sink will dwell in the time epochs ti−1, ti, andti+1, respectively. Its strategy, therefore, is to tune in, cyclically, to these frequencies, spending τ/3 time units on each of them. It is clear that, eventually, the sensor node meets the sink node on one of these s frequencies. Assume, without loss of generality, that the node meets the sink on frequency λ in some (unknown) slot s of one of the epoch's ti−1, ti, orti+1. To verify the synchronization the node will attempt to meet the sink in slots s+1, s +2 and s +3 at the start of the next epoch. If a match is found, the node declares itself synchronized. Otherwise, the node will repeat the above process. We note that even if the sensor node declares itself synchronized with the sink, there is a slight chance that, it is not. The fact that the node has not synchronized will be discovered quickly and it will again attempt to synchronize. There are ways in which we can make the synchronization protocol deterministic. For example, the hopping sequence can be designed in such a way that the last frequency in each epoch is unique and it is not used elsewhere in the epoch. How- ever, this entails less flexibility in the design of the hopping sequence and constitutes, in fact, an instance of a differential security service where the level of security is tailored to suit the application or the power budget available.

Conclusion Remark

In this work we have proposed a virtual infrastructure a dynamic coordinate system –for a massively-deployed collection of anonymous sensor nodes. This coordinate system provides, at no extra cost, an interesting clustering scheme according to which two nodes are in the same cluster only if they have the same coordinates. Notice that this clustering scheme works for anonymous sensor nodes. As a corollary, sensor nodes do not know the identity of the other nodes in the same cluster. Our second contribution was to show that training the sensor nodes – the process of learning their coordinates – can be performed by a protocol that is at the same time lightweight and secure. Being energy efficient, this training can be repeated on either a scheduled or ad-hoc basis to pro- vide robustness and dynamic reorganization. We also showed that in a trained wireless sensor network the tasks of routing and data fusion can be performed by very simple and energy-efficient protocols. Finally, we showed how to design the co- ordinate system such as to minimize the power expended in collecting and routing data. In this paper we addressed the problem of training a sensor network in a two-dimensional plane. In practice, however, the network training problem manifests itself in three dimensions, for example, because of irregularities in a rugged deployment terrain. To extend our work we have developed solutions for the three-dimensional training problem where the majority of the nodes are assumed to reside in one logical base plane, while the remaining nodes are dispersed over other parallel planes. The goal was to mimic the case of minor terrain ir- regularities. However, training a sensor network of nodes arbitrarily dispersed in a three-dimensional space remains an open problem.

References

[1] J. Agre and L. Clare, An integrated architecture for cooperative sensing networks, IEEE Computer 33(5) (2000) 106–108.

[2] F. Akyildiz, W. Su, Y. Sankarasubramanian and E. Cayirci, Wireless sensor networks: A survey, Computer Networks 38(4) (2002) 393–422.

[3] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (Wiley, New York, 2001).

[4] R. Anderson and M. Kuhn, Tamper resistance – a cautionary note, in: Proc. 2nd USENIX Workshop on Electronic Commerce, Berkeley, CA (1996), pp. 1–11. IEEE Wireless Communications 9(1) (2002) 40– 48.

[5] S. Bandyopadhyay and E. Coyle, An efficient hierarchical clustering algorithm for wireless sensor networks, in: Proc. INFOCOM'2003, San Francisco, CA (April 2003).

[6] D. Braginsky and D. Estrin, Rumor routing algorithm for sensor net- works, in: Proc. Internat. Conf. on Distributed Computing Systems (ICDCS-22) (November 2001).

[7] N. Bulusu, J. Heidemann and D. Estrin, GPS-less low cost outdoor lo- calization for very small devices, IEEE Personal Communications 7(5) (2000) 28–34.

[8] N. Bulusu, J. Heidemann and D. Estrin, Scalable coordination for wireless sensor networks: self-configuration localization systems, in: Proc. 6th Internat. Sympos. on Communication Theory and Applica- tions (ISCTA-2001) (July 2001).

[9] S. Capkun, M. Hamdi and J.-P. Hubeaux, GPS-free positioning in mo- bile ad-hoc networks, Cluster Computing 5(2) (2002) 157–167.

[10] D.W. Carman, P.S. Kruus and B.J. Matt, Constraints and approaches for distributed sensor network security, Technical Report 00-010, NAI Labs (2000).

[11] D. Coore, R. Nagpal and R. Weiss, Paradigms for structure in an amor- phous computer, MIT Artificial Intelligence Laboratory Technical Re- port AI-1616 (October 1997).

[12] L. Doherty, H.S.J. Pister and L.E. Ghaoui, Convex position estimation in wireless sensor networks, in: Proc. INFOCOM'2001, Anchorage, AK (April 2001).

[13] A. Ephremides, J. Wieselthier and D. Baker, A design concept for re- liable mobile radio networks with frequency hopping signaling, Pro- ceedings of the IEEE 75(1) (1987) 56–73.

[14] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, Highly resilient, energy-efficient multipath routing in wireless sensor networks, ACM Mobile Computing and Communications Review 5(4) (2001).

[15] S. Ghiasi, A. Srivastava, X. Yang and M. Sarrafzadeh, Optimal energy- aware clustering in sensor networks, Sensors 2 (2002) 258–269.

[16] L. Girod, V. Bychkovskiy, J. Elson and D. Estrin, Locating tiny sensors in time and space: A case study, in: Proc. International Conference on Computer Design (ICCD 2002), Freiburg, Germany (September 2002).

[17] R.G. Graham, D.E. Knuth and O. Patashnik, Concrete Mathematics (Addison-Wesley, New York, 1989).

[18] G.D. Abowd, J.P.G. Sterbenz, Final report on the inter- agency workshop on research issues for smart environ- ments, IEEE Personal Communications (October 2000) 36–40.

[19] J. Agre, L. Clare, An integrated architecture for cooper- ative sensing networks, IEEE Computer Magazine (May 2000) 106–108.

[20] I.F. Akyildiz, W. Su, A power aware enhanced routing (PAER) protocol for sensor networks, Georgia Tech Technical Report, January 2002, submitted for publica- tion.

[21] A. Bakre, B.R. Badrinath, I-TCP: indirect TCP for mobile hosts, Proceedings of the 15th International Conference on Distributed Computing Systems, Vancouver, BC, May 1995, pp. 136–143.

[22] P. Bauer, M. Sichitiu, R. Istepanian, K. Premaratne, The mobile patient: wireless distributed sensor networks for patient monitoring and care, Proceedings 2000 IEEE EMBS International Conference on Information Technol- ogy Applications in Biomedicine, 2000, pp. 17–21.

[23] M. Bhardwaj, T. Garnett, A.P. Chandrakasan, Upper bounds on the lifetime of sensor networks, IEEE Interna- tional Conference on Communications ICC'01, Helsinki, Finland, June 2001.

[24] P. Bonnet, J. Gehrke, P. Seshadri, Querying the physical world, IEEE Personal Communications (October 2000) 10–15.

[25] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, Scalable coordination for wireless sensor networks: self-configuring localization systems, International Symposium on Com- munication Theory and Applications (ISCTA 2001), Ambleside, UK, July 2001.

[26] B.G. Celler et al., An instrumentation system for the remote monitoring of changes in functional health status of the elderly, International Conference IEEE-EMBS, New York, 1994, pp. 908–909.