Literature Survey on Wireless Sensor Networks

Pavlos Papageorgiou
pavlos@eng.umd.edu

July 16, 2003

Contents

1 Literature Survey

1.1 Surveys

A survey on sensor networks [1]
I.F. Akyildiz, Weilian Su, Sankarasubramaniam, E. Cayirci
IEEE Communications, Aug 2002

The authors present a communication architecture for sensor networks and proceed to survey the current research pertaining to all layers of the protocol stack: Physical, Data Link, Network, Transport and Application layers.

A sensor network is defined as being composed of a large number of nodes which are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes collects data and its purpose is to route this information back to a sink. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined. Cooperation among nodes is the dominant feature of this type of network, where groups of nodes cooperate to disseminate the information gathered in their vicinity to the user.

Major differences between sensor and ad-hoc networks:

- Number of nodes can be orders of magnitude higher.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failure.
- Frequent topology changes.
- Broadcast communication paradigm.
- Limited power, processing and power capabilities.
- Possible absence of unique global identification per node.

The authors point out that none of the studies surveyed has a fully integrated view of all the factors driving the design of sensor networks and proceeds to present its own communication architecture and design factors to be used as a guideline and as a tool to compare various protocols. After surveying the literature, this is our impression as well and we include it in the open research issues that can be explored for future work. The design factors listed by the authors:

- Fault Tolerance: Individual nodes are prone to unexpected failure with a much higher probability than other types of networks. The network should sustain information dissemination in spite of failures.
- Scalability: Number in the order of hundreds or thousands. Protocols should be able to scale to such high degree and take advantage of the high density of such networks.
- Production Costs: The cost of a single node must be low, much less than $1.
- Hardware Constraints: A sensor node is comprised of many subunits (sensing, processing, communication, power, location finding system, power scavenging and mobilizer). All these units combined together must consume extremely low power and be contained within an extremely small volume.
- Sensor Network Topology: Must be maintained even with very high node densities.

- Environment: Nodes are operating in inaccessible locations either because of hostile environment or because they are embedded in a structure.
- Transmission Media: RF, Infrared and Optical.
- Power Consumption: Power conservation and power management are primary design factors.

Physical Layer

Briefly discusses how the choice of a modulation scheme affects the power requirements. The authors consider that this is a largely unexplored area. Open research issues: Design of simple and low power modulation schemes, strategies to overcome signal propagation effects and implementing the hardware in very small volume.

Data Link Layer

Data Link Layer: Responsible for creating the network infrastructure (hop by hop communication and self organizing ability) and efficiently sharing communication resources among sensor nodes.

Authors argue that novel protocols need to be devised because current solutions used in other wireless networks are not suitable because sensor networks exhibit unique resource constraints and application requirements. Cellular systems have fixed infrastructure and the main goal of MAC is to provide QoS and bandwidth efficiency through dedicated resource assignment. Bluetooth and the Mobile Ad hoc NETwork, although close to sensor networks, have orders of magnitude fewer nodes and much higher transmission power.

Sensor networks on the other hand need to cope with more frequent topological changes (not so much because of mobility, but mainly because of nodes failing, going to sleep, being blocked by environment interference, etc) and have as primary goal to prolong network lifetime by power conservation.

The protocols that the authors surveyed are:

- SMACS and EAR [19]:

  In this model sensor nodes are mostly stationary and there exists a number of higher energy mobile nodes. SMACS achieves network startup and link-layer organization for the sensor nodes by combining neighborhood discovery and channel assignment phases so that by the time nodes hear all their neighbors the have formed a connected network. This is achieved without the presence of global or local master nodes.

  Uses fixed allocation of duplex time slots at fixed frequency. Exploits large available bandwidth compared to sensor data rate. Conserver power by random wake up during setup and after time slot allocation by turning radio off while idle. EAR enables seamless connection of the mobile nodes and is transparent to SMACS.

- CSMA-Based Medium Access [35]:

  The MAC protocol must be able to support variable but highly correlated and dominantly periodic traffic. This does not fit traditional CSMA-based schemes which assume stochastically distributed traffic mainly for point-to-point flows. This scheme uses constant listening periods for energy efficiency and introduces random delays for robustness. In order to achieve fairness, an adaptive rate control scheme is used.

- Hybrid TDMA/FDMA CSMA-Based Medium Access [39]:

  In this scheme hybrid TDMA-FDMA is shown to be more energy efficient than TDMA or FDMA. This work emphasizes that energy efficient protocols for sensor networks cannot be designed unless physical layer and hardware issues are taken into account. Protocols throughout the protocol stack should be aware of the physical layer and hardware and not treat them as ”black boxes”.

Network Layer

- Small Minimum Energy Communication Network: Creates a subgraph of the sensor network that contains the minimum energy path.
- Flooding: Broadcasts data to all neighbor nodes. Simplest routing protocol with serious deficiencies such as implosion, overlap and resource blindness.
- Gossiping: Sends data to one randomly selected neighbor. Avoids implosion problem but message propagation takes longer time.
- SPIN: Whenever a node has available data, it broadcasts a description of the data and sends it only to the sensor nodes that expresses interest.
- SAR: Creates multiple trees where the root of each tree is one hop neighbor from the sink. A sensor node selects a tree for data to be routed back to the sink according to the energy resources and additive QoS metric.
- LEACH: Forms a two level cluster hierarchy, where cluster members send data to the cluster head which in turn sends it to the base station. Energy dissipation is evenly spread by dissolving clusters at regular intervals and randomly choosing the cluster heads.
- Directed Diffusion: A sink sends out an interest which propagates in the network and sets up gradients for data to flow from source to sink.

Current Research Projects:

SensoNet	Transport, network, data link and physical layers	Georgia Tech
WINS	Distributed network access to sensors, controls and processors.	UCLA
SINA	Information networking architecture	Univ Delaware
mAMPS	Framework for adaptive energy-aware distributed microsensors.	MIT
LEACH	Cluster formation protocol.	MIT
SmartDust	Laser communication from a cubic millimeter.	Berkeley
SCADDS	Scalable coordination architectures for deeply distributed and dynamic systems.	ISI
PicoRadio	System-on-chip implementation of a PicoNode.	Berkeley
PACMAN	Mathematical framework that incorporates key features of computing nodes and networking elements.	USC
Dynamic Sensor Networks	Routing and power aware sensor management. Network services API.	ISI east
Aware Home	Create home environment to both perceive and assist its occupants.	Georgia Tech
COUGAR	Distributed query processing	Cornell
DataSpace	Distributed query processing.	Rutgers

A Taxonomy of Wireless Micro-Sensor Network Models [2]

S. Tilak, N.B. Abu-Ghazaleh, W. Heinzelman

ACM SIGMOBILE Mobile Computing and Communications Review

Next century challenges: Scalable Coordination in Sensor Networks [21]

D. Estrin and R. Govindan and J. Heidemann and S. Kumar

MOBICOM 1999

C. Intanagonwiwat and R. Govindan and D. Estrin [29]
Directed Diffusion: A Scalable and Robust Communication
MOBICOM 2000

Problem

Sensor networks have different requirements than other wireless networks. The need for robustness and scalability leads to the design of localized algorithms, where sensors only interact with other sensors in a restricted vicinity and have at best an indirect global view.

Approach

The authors argue in favor of designing localized algorithms and present directed diffusion as a set of abstractions that describe the communication patterns underlying such algorithms. The design features differ from traditional wireless networks and are data-centric and application-specific.

Data-centric refers to the fact that in sensor networks we are mostly interested in retrieving information matching certain attribute values and very rarely we will be interested only in data from a specific node. This approach decouples data from the sensor that produced it and unique identification of nodes is of secondary importance. Application-specific refers to the awareness across all layers of the specific application so that intermediate nodes can perform data aggregation, caching and informed forwarding.

The authors proceed to describe a two-level cluster formation algorithm, where cluster heads are elected based on available energy. They present a localized algorithm for object tracking to demonstrate the difficulties that arise. The design is difficult because localized algorithms need to produce a certain global behavior with at best indirect global knowledge. Furthermore, localized algorithms tend to be sensitive in the choice of parameter values.

In order to overcome these difficulties, they suggest the design and prototyping of adaptive fidelity algorithms, where the fidelity of the retrieved data can be traded against energy efficiency, network lifetime and network bandwidth. Furthermore, by developing techniques for characterizing the performance of localized algorithms it is possible to quantify those tradeoffs and produce the expected behavior.

The authors propose ”directed diffusion” to be used as an abstraction to model the communication patterns of localized algorithms. The data that each sensor generates is characterized by a number of attributes. Other sensors that are interested in a certain type of data, disseminate this interest to the network (in the form of attributes and degree of interest). As the interests disseminate, gradients are established that direct the diffusion of data when it becomes available, i.e., reverse paths are established for data that matches an interest.

1.2 Routing Protocols

Rumor routing algorithm for sensor networks [24]
D. Braginsky, D. Estrin
International Workshop on Wireless Sensor Networks and Applications, WSNA 2002

Problem

There is a need for delivering queries to nodes that have observed particular events in the network and getting the data back to the point where the interest was expressed. One way to achieve this is to establish a global coordinate system and perform geographic routing. Another simpler approach would be to just flood the query or the event. However, the sheer number of sensor nodes, which must operate under stringent power constraints, and the data centric nature of sensor networks make such schemes very inefficient. The authors present a method for routing queries to nodes based on the event observed; not based on a unique id or geographic location of a node. This allows data to be retrieved from the network keyed on the event and not on the underlying network addressing scheme or geography.

Two possible solutions to the problem are query and event flooding. In the case of query flooding, the query is flooded in the network and the number of transmissions (a first naive metric of energy efficiency) is independent of the number of events. This scheme is useful when the number of events is very high compared to the number of queries. In the case of event flooding, whenever a node witnesses an event it floods the network and all the other nodes can setup gradients to it, through which any queries can be routed. The number of transmissions in this case is independent of the number of queries and this scheme can be efficient when the number of events is low compared to the number of queries.

Approach

The authors introduce Rumor Routing as a logical compromise between query and event flooding. With Rumor Routing paths (possibly multiple and non-optimal) are created leading to each event. Whenever a query is generated it is sent on a random walk until it crosses one of the paths leading to the event of interest. It is possible that the query will never cross such a path, in which case query flooding can be used as a last resort. The authors use the heuristic of two lines intersecting in a bounded rectangular region to indicate the plausibility of their solution. The main focus of this paper is the method for setting up paths to an event.

The algorithm uses a set of long-lived agents (packets that move between nodes) that create paths (state in every node) toward the events they encounter. Whenever a node witnesses an event it probabilistically generates an agent which travels the network and is initialized with the node's event forwarding table (distance and next hop for events that the node knows about directly or that it can route queries to). As the agent travels, it synchronizes its event table with each node it visits. As a result, it propagates path information and learns about new events that it can propagate further.

The agent employs a straightening algorithm to determine its next hop and avoid loops. Due the broadcast nature of the medium, the agent leaves a fairly thick path as it travels, since nodes close to the agent's path can update their own event tables as well. Any node can generate an agent, but it makes more sense for nodes which have observed events to do so, so that useful information can be disseminated immediately.

Whenever a query is generated, if the node has an entry for the event in its event table it routes the query to the next hop. Otherwise, it picks randomly a next hop in the hope that it will cross a path to the event. Forwarding queries along a straight path seems to yield better results. It is possible that a query will reach its TTL before crossing a path toward the event, in which case it can perform query flooding. The goal of the algorithm is for the latter case to be rare.

Results

The simulation testbed includes a network of (3000, 4000, 5000) nodes scattered randomly over an area $200x200m^2$. After scattering events over the area and letting the agents setup their paths, 1000 queries were generated and the number of successfully routed queries recorded.

According to the results, for most parameter values Rumor Routing can achieve significant savings over flooding up to a certain event cost threshold without sacrificing delivery rate. It handles node failure gracefully by degrading its delivery rate linearly with number of failed nodes.

Energy-efficient communication protocol for wireless microsensor networks [30]
W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan
IEEE Hawaii International Conference on System Sciences, 2000

The authors present a 2-level hierarchical routing protocol (LEACH) which attempts to minimize global energy dissipation and distribute energy consumption evenly across all nodes. This is achieved by the formation of clusters with localized coordination, by rotating the high-energy cluster heads and by locally compressing data.

The model used in this paper makes the following assumptions:

- There exists one fixed base station with no energy constraints and a large number of sensor nodes that are mostly stationary, homogeneous and energy constrained.

- The base station is located at some distance from the sensor nodes and the communication between a sensor node and the base station is expensive.
- The purpose of the network is to collect data through sensing at a fixed rate (i.e. there is always something to send) and convey it to the base station. The raw data is too much and must be locally aggregated into a small set of meaningful information.

The nodes self-organize into local clusters with one node in each cluster acting as a cluster head. Once a cluster has formed, the cluster members send their data to the cluster head (low energy transmission) which in turn combines the data and sends it to the base station (high energy transmission). This organization of the nodes creates a 2-level hierarchy.

The operation of the protocol is broken up into rounds, during which the clusters are dissolved and recreated. During each round, a node decides probabilistically whether to become a cluster head. This decision is based on the suggested percentage of cluster heads for the network (determined a priori) and the number of times the node has been a cluster head so far. The cluster heads advertise their intention and the rest of the nodes decide which cluster to join, usually based on signal strength. Once the clusters are formed, the cluster head creates a TDMA schedule and sends it to its cluster members. To reduce interference, each cluster communicates using different CDMA codes.

For their analysis, the authors compare their scheme with a direct communication protocol (each sensor sends data directly to the base station) and the minimum-energy routing protocol. In the latter, data destined for the base station is routed through many intermediate nodes that can each be reached with minimum-energy transmission. A static clustering scheme is also used where cluster heads are not rotated. Their results indicate that LEACH reduces communication energy by as much as 8x. Also, the first node death in LEACH occurs over 8 times later and the last node dies over 3 times later.

Some criticisms about LEACH ([4]):

- Not taking into account the possibility of nodes failing due to hostile environment.
- There is no provision for the cluster heads to be uniformly distributed with respect to their geographic location. Since in each round a node becomes a cluster head with a certain probability, it is possible that parts of the network will be left without a cluster head.
- In the analysis only a 100-node network is considered, which is at least one order of magnitude less than the envisioned number of nodes.

The design and implementation of an intentional naming system [31]
W. Adjie-Winoto and E. Schwartz and H. Balakrishnan and J. Lilley
ACM SIGOPS Operating Systems Review, 1999

Problem

In a mobile network, because of node and service mobility, the network address of a service/resource is not fixed. A desired property of such an environment would be the ability to discover resources and locate services dynamically based on an assigned ”name” which describes application-specific attributes of the service. However, to make such a system useful in a higly dynamic environment, it would be desirable to postpone the name resolution as much as possible and integrate it with message routing. By using late binding, a session can continue even when the network address of a service changes.

Approach

The authors propose an ”intentional naming system” to address all these considerations. This system is an application level overlay network which integrates name resolution and message routing. The only assumption about the underlying network layer is that it provides IP unicast.

The overlay network is comprised of *Intentional Name Resolvers (INR's)*. The INRs self-configure into a spanning tree overlay network topology optimizing the average delay between neighboring INRs. This requires the existence of a rendez-vous point which maintains a list of active and candidate INRs.

The purpose of the overlay is to exchange service advertisements and route messages towards these services. Each service/resource attaches to an INR and advertises its service description (”name”). Each client that wishes to use a service, issues a query to an INR. The client has three alternatives for locating the service: (i) early binding, in which case the INR just returns the IP address of the service (ii) intentional anycast, in which case the INR acts as a router and forwards (through the INR overlay) the message towards the service that matches that name and has the smallest metric (application specific) (iii) intentional multicast, in which case the message is forwarded towards all the services that match the name. The latter two alternatives are in essence late binding techniques.

The system uses expressions called name-specifiers to specify the destination service for messages. The name-specifier is an hierarchy of attribute-value pairs such that an av-pair that is dependent on another is a descendant of it. The central activity of an INR is to resolve name-specifiers to their corresponding network locations. This is accomplished by building name trees and performing name lookups. It is quite interesting that both the attribute and its value are used as nodes in the tree, instead of the value alone. This allows, depending on the value, to have a different set of attributes.

Results

This algorithm does not scale well in respect with the number of name updates by services, since all resolvers need to be aware of all the names in the system. As the number of updates increases, the available bandwidth or processing power starts to saturate and the lookup time increases. One solution proposed is to divide the name space into virtual spaces and ensure that each resolver is responsible for only a subset of the virutal spaces.

1.3 MAC Layer

A Transmission Control Scheme for Media Access in Sensor Networks [35]
A. Woo, D. Culler
MOBICOM 2001

Problem

Media access control in sensor networks must be energy efficient and allow fair bandwidth allocation to all the nodes. The authors examine how CSMA based medium access can be adapted for sensor networks.

CSMA strategies include listening to the channel before transmission, using explicit positive or negative acknowledgments to signal collision, relying on time synchronized slotted channels or performing collision detection. However, these approaches are not directly applicable due to the characteristics of sensor networks:

- Network operates as a collective structure. Its primary goal is the sampling of the environment and the propagation of the samples, possibly processed and aggregated, toward one or more gateways.
- Traffic tends to be periodic and highly correlated. Conventional schemes make the assumption of stochastically distributed traffic.
- Every node is both a data source and a router.

- Node capabilities are very restricted.
- Equal cost per unit time for listening, receiving and transmitting.

Approach

The authors outline a CSMA-based MAC and transmission control scheme to achieve fairness while being energy efficient. They categorize media access control mechanisms into listening, backoff, contention control and rate control mechanisms.

Listening combined with backoff mechanism: Neighboring nodes will sense the same event and attempt to transmit at the same time. According to the proposed scheme, whenever nodes need to transmit they introduce random delay followed by a constant listening period. If the channel is free, then they transmit. Otherwise, they enter in a backoff period, during which the radio is turned off. This backoff period is also applied as a phase shift to the periodicity of the application, aiming to desynchronize nodes.

Contention control mechanism: Such a mechanism should use the minimum number of control packets. If the traffic load justifies it, then a combination of request-to-send (RTS) and clear-to-send (CTS) control packets can be used.

Rate control mechanism: MAC should control the rate of the originating data of a node in order to allow route-thru traffic to access the channel and reach the base station. The adaptive rate control proposed, uses loss as collision signal to adjust transmission rate in a manner similar to the congestion control in TCP.

Results

For the first set of results, all the CSMA schemes are evaluated over a single hop scenario consisting of 10 nodes with one base station in the middle. The parameters considered are: delay before listening (random vs none), listening period (random vs constant) and the backoff mechanism used (none, fixed window, exp increase, exp decrease).

- All CSMA schemes achieve good channel utilization and aggregate fairness is almost insensitive to the presence of backoff. However, backoff plays an important role in maintaining proportional fairness when using a fixed window size or binary exponential decrease in window size.
- Randomness in the pre-collision phase provides robustness.
- Schemes with constant listen period achieve best energy efficiency.
- Following a transmission failure with a random shift in the sampling interval, allows the nodes to break away from synchronization which listening and backoff fail to detect.

For the next set of results, a multihop scenario is considered with up to five levels deep. The CSMA scheme is augmented with a transmission control protocol so that nodes adapt their data origination rate to give a fair share to downstream nodes and to match available upstream.

- CSMA schemes with no contention or rate control mechanisms fail to deliver any packets from nodes more than two levels deep. This is mainly due to the hidden node problem and the fact that the collective behavior of the nodes is not taken into account.
- When a RTS/CTS contention scheme is used, nodes deep in the network are able to deliver packets to the base station but the resulting bandwidth allocation is very unfair. Nodes close to the base station use up most of the channel for their own original traffic and allocate a small fraction of the channel to route-thru traffic.
- When a rate control mechanism is used, the bandwidth is allocated fairly among originating and route-thru traffic.

Interesting Points

- The adaptive rate control balances the in-node generated traffic with the route-thru traffic by using packet loss as a signal to decrease traffic.
- Notion of a phase shift at the application level to break the periodicity of the sensor sampling.
- Metrics for multihop fairness and energy efficiency (measuring bandwidth delivery to base station) for evaluating MAC schemes.
- Good overview of the purpose and characteristics of sensor networks in the introduction.
- Evaluation platform consists of only 10 nodes with on base station in both single and multihop scenarios.

1.4 Energy

Energy concerns in wireless networks [36]
A. Ephremides
IEEE Wireless Communications, Aug 2002

Problem

This paper focuses on the major energy efficiency issues in ad-hoc networks (not only sensor networks) which are defined as infrastructureless networks that require multiple hops for connecting all the nodes to each other. Vertical layer integration and criticality of energy consumption are the two main charateristics of ad-hoc networks that drive their design. The separation of network functions into layers is characterized as the ”original sin” in networking.

For any wireless node there are three major modes of operation: transmitting, receiving and listening. When the node is in listening mode the energy expenditure is minimal. However, if the node spends most of the time listening then this mode is responsible for a large portion of the consumed energy (as is the case in sensor networks).

In multihop wireless networks it is energy efficient to choose long paths along a series of short hops rather than short paths along a series of long hops. However, even though energy efficiency is our paramount interest it is not the only one. Communication performance is also very important. By choosing many short hops we may lower the energy expenditure, but only to a certain degree, since delay increases, processing energy increases and control overhead increases. Therefore, the choice of how to incorporate energy is not as clear as it seems.

A useful distinction presented in the paper refers to whether energy is treated as a cost function or as a hard constraint. In the former case, the objective of the designer is to minimize the amount of energy per communication task, treating energy as an expensive but inexhaustible resource. However, when energy is a hard constraint, the designer must keep in mind that it is a limited resource that will be exhausted. In this case, the designer's task is more complicated since he has to satisfy conflicting objectives: maximizing the longevity of the network vs communication performance (throughput, total data delivered, etc)

Another interseting point made is the difficulty in defining when the network ”dies”. Is it when the first one dies? When the last one dies? When a portion of them die?

1.5 Security

The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks wireless networks [44]

F. Stajano and R. Anderson
7th International Workshop on Security Protocols, 1999

The Resurrecting Duckling – What Next? [43]

Frank Stajano
Lecture Notes in Computer Science, vol 2133, 2001

Problem

Provide support for secure transient association between a master and a slave device or between peers in a wireless ad-hoc network. Consider, as an example, a universal remote that controls most appliances in your home which are networked in a wireless ad-hoc fashion. The remote needs to be associated with each of the appliances in a secure way, in the sense that an identical remote purchased by your neighbor will not be able to control these devices.

Approach

The solution proposed is formalised in the Resurrecting Duckling security policy model. The slave device is termed as the duckling and the master controller acts as its mother duck. The name and terminology is inspired by biology and specifically from the fact that a duckling recognizes as its mother the first moving object it sees that makes a sound when it emerges from its egg. This phenomenon is called imprinting. Consequently, a device can be in one of two states: imprintable (waiting for a shared secret that will associate it with another master device) and imprinted (already associated).

The imprinting can take place with physical electrical contact, which transfers a secret key that binds the device to the specified master forever. In the original model, once a device is associated with another master device, it only obeys that device until it is instructed to become imprintable again.

However, this model was too limiting since it did not allow interaction with other entities. It was extended in the second paper to include the specification of policy where for each action the master device specifies what credentials are required to be presented by a another device in order to request that action.

The paper is quite interesting in its approach and terminology. It uses biological terms such as ”soul”, ”death”, ”commit suicide”, ”mother duck”, etc.

Talking to strangers: Authentication in adhoc wireless networks [42]

D. Balfanz and D. Smetters and P. Stewart and H. Wong
Symposium on Network and Distributed Systems Security, 2002

Problem

Provide support for secure communication and authentication in wireless ad-hoc networks without any public key infrastructure. Specifically, when device A chooses to establish connection to a previously unknown device B, device A needs know that it is actually communicating securely and authentically with device B and not with an attacker.

Approach

The approach is an extension and formalization of the ”Resurrecting Duckling policy model” and provides bootstrapping secure wireless communication through pre-authentication over a location limited channel. The location-limited channel is different from the main wireless link and is chosen so that it has two special security properties: (i) demonstrative identification (identification based on physical context) (ii) authenticity, in the sense that is difficult for an attacker to transmit on the channel undetected. As an example, good candidates for a location-limited channel are actual physical contact, sound, infrared, etc, (in general communication technologies with inherent physical limitations).

This approach does not require secrecy, necessary in the ”Resurrecting Duckling”, making it impervious to eavesdropping. This is achieved through public key cryptography. The participants use the location-limited channel to exchange their public keys or the digests of the keys. This concludes the pre-authentication phase and they can proceed to authenticate themselves over the wireless channel and establish a secret key for the session.

2 Open Research Issues

Considerable work and effort has focused on designing communication protocols for sensor networks. However, no single protocol has emerged as a major contender and research on this issue is very much active and ongoing. Possible contributions to the field:

2.1 Models for Sensor Networks

What is a wireless sensor network? Is it necessarily thousands of nodes? What makes it a sensor network? - Number of nodes? - Severe resource contraints of nodes? - Sensing? - Information retrieval? Why cannot we do conventional routing? Once we get the information, how does it go back to the sink? Could the model be more general? What short of application classes are envisioned? Can broad classes be specified? Shouldn't we study a little closer the proposed applications? Since data fusion and aggregation is involved, shouldn't we we study the actual methods for getting information out of the network? For example, estimation and detection techniques.

2.2 Development of an Evaluation Framework for Sensor Networks

Each paper on sensor networks presents its own model and assumptions which usually cover a different subset of the design state space. These assumptions are in regard to:

- number of nodes
- mobility of nodes
- node properties
- probability of unanticipated node failures
- presence of non-homogeneous nodes
- presence of base stations that serve as gateways to other networks
- nature of the sensing application

As noted by [1], none of the studies surveyed has a fully integrated view of the design factors influencing the development of protocols for sensor networks. Although it cannot be expected that a single protocol will outperform all others for all possible models, this arbitrary fragmentation of the design state space makes it difficult to evaluate the protocols and compare them to each other. In most cases, the authors evaluate their protocol with ad hoc metrics which make comparisons even more problematic.

It would be useful to have comprehensive guidelines for evaluating a specific protocol and compare it against others. A primary goal for such a framework would be to provide a handful of models to classify sensor networks so that most of the the anticipated uses of such networks are covered in an organized fashion. Based on the model used, appropriate metrics would then be used to evaluate the strengths and weaknesses of each protocol under consideration.

Baseline protocols could also be provided for each defined model in order to get a feeling of the ”goodness” of the protocol under evaluation. For example, a model could define an idealized protocol (e.g. with universal knowledge) and a trivial one (e.g. blind flooding) and then evaluate the new protocol based on how close it comes to the idealized and how much better it performs compared to the trivial one.

Such an evaluation framework could potentially be very beneficial to the research community by introducing a point of reference for the design and evaluation of communication protocols in wireless sensor networks. Its usefulness could extend beyond comparative analysis and could be used to fine tune parameters of a specific protocol. Its clear definition of models could facilitate the extraction and prioritization of the desired properties of new protocols given an application environment.

Due to the nature of sensor networks, there is an inevitable coupling among the layers. Therefore, an evaluation framework would not be useful if it only concentrated on protocols of a specific layer. The framework should evaluate the goodness of the network as a whole and provide metrics to measure the effects of the design on the operation of the network (by evaluating, for example, energy efficiency, communication performance, etc). Not all measures will be applicable or relevant for every design; the objective is to provide the tools to compare the impact of the new design to other alternatives or against the ideal case.

2.3 Prove or disprove that traditional routing is not feasible

It is always assumed that traditional routing with unique global IDs is infeasible. Even with scaled down routing protocols. Further study is warranted so that it is determined if that claim is always true. Calculate processing, memory and communication requirements for performing traditional routing and provide bounds on required resources.

2.4 Collaborative Information Gathering Networks

The main task of a sensor network is to gather and disseminate information. However, the WSN model makes implicit assumptions about the nature and capabilities of the agents (nodes) which do not relate directly to the problem at hand.

2.5 Survey on Routing Protocols for Sensor Networks

There have been a few surveys on sensor networks in general [1, 2, 3, 4] which cover most aspects of sensor networks, but there is still room for a survey that focuses on routing protocols exclusively. This could be extended to also evaluate the surveyed protocols using the evaluation framework developed above, as a proof of concept on the usefulness of the framework.

2.6 Development of a new Transport protocol

As pointed out in [34], which proposes a reliable transport protocol for wireless sensor network, there has been little work on the design of efficient transport protocols in this setting. New transport schemes need to be introduced which will focus on energy efficiency and take advantage of the collaborating nature of sensor networks.

For example, one strategy would be to design a transport protocol that can receive feedback about a variety of attributes (energy state of the node, quality of wireless link, etc). Furthermore, the transport protocol could be aware of or allow the use of intermediate transport proxies (at the border of networks with different characteristics and feedback), thus enabling the transport of data between heterogeneous networks. The usefulness of such a transport protocol would not be limited to sensor network; most wireless networks that communicate with a fixed network would be benefited.

2.7 Development of a new Routing protocol

Disseminating information in sensor networks with tight energy restraints is still an open problem and there is a need for routing protocols specifically tailored for ultra low energy and asymmetric communication with realistic assumptions about the frequency of topology changes and the number of nodes in the network. Quite a few routing protocols have been proposed [24, 25, 26, 27, 28, 29, 30, 31] but most of them need to be improved because they assume mostly static topologies and smaller than envisioned number of nodes (a couple of hundreds instead of thousands).

2.8 Groups of sensor networks

Most attention has been focused on a variety of designe issues for a single sensor network. The interaction with the outside world is not considered and assumed to be application specific and handled by the base station(s) on the edge of the sensor network. Therefore, interaction with other networks as well as cooperation among sensor networks (creating groups of different sensor networks) could be an area worth looking into.

References

[1] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, Aug. 2002.

[2] S. Tilak, N.B. Abu-Ghazaleh, and W. Heinzelman. A Taxonomy of Wireless Micro-Sensor Network Models. *ACM SIGMOBILE Mobile Computing and Communications Review*, April 2002.

[3] A. Bharathidasan and V. Ponduru. Sensor Networks: An Overview. Technical report, University of California, Davis, ?

[4] P. Rentala, R. Musunnuri, S. Gandham, and U. Saxena. Survey on Sensor Networks. Technical report, University of Texas at Dallas, ?

[5] J. Weatherall and A. Jones. Ubiquitous networks and their applications. *IEEE Wireless Communications*, Feb. 2002.

[6] D. Estrin, D. Culler, K. Pister, and G. Sukhatme. Connecting the physical world with pervasive networks. *IEEE Pervasive Computing*, Jan.-March 2002.

[7] D. Estrin, L. Girod, G. Pottie, and M. Srivastava. Instrumenting the world with wireless sensor networks. In *IEEE Conference on Acoustics, Speech, and Signal Processing*, 2001.

[8] G.J. Pottie and W.J Kaiser. Wireless Integrated Network Sensors. *Communications of the ACM*, May 2000.

[9] D. Saha and A. Mukherjee. Pervasive computing: a paradigm for the 21st century. *IEEE Computer*, March 2003.

[10] D. Estrin, R. Govindan, and J. Heidemann. Embedding the Internet. *Communications of the ACM*, May 2000.

[11] Mark Weiser. The Computer for the 21st Century. *Scientific American*, Sep. 1991.

[12] Alan Mainwaring, Joseph Polastre, Robert Szewczyk, David Culler, and John Anderson. Wireless Sensor Networks for Habitat Monitoring. In *ACM International Workshop on Wireless Sensor Networks and Applications*, 2002.

[13] A.J. Goldsmith and S.B. Wicker. Design challenges for energy-constrained ad hoc wireless networks. *IEEE Wireless Communications*, Aug. 2002.

[14] W. Stark, Hua Wang, A. Worthen, S. Lafortune, and D. Teneketzis. Low-energy wireless communication network design. *IEEE Wireless Communications*, Aug. 2002.

[15] S. Tilak, N.B. Abu-Ghazaleh, and W. Heinzelman. Infrastructure tradeoffs for sensor networks. In *ACM International Workshop on Wireless Sensor Networks and Applications*, 2002.

[16] Chien-Chung Shen, C. Srisathapornphat, and C. Jaikaeo. Sensor information networking architecture and applications. *IEEE Personal Communications*, Aug. 2001.

[17] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for networked sensors. In *ACM ASPLOS*, 2000.

[18] J.L. da Silva Jr, J. Shamberger, M.J. Ammer, C. Guo, S. Li, R. Shah, T. Tuan, M. Sheets, J.M. Rabaey, B. Nikolic, A. Sangiovanni-Vincentelli, and P. Wright. Design methodology for PicoRadio networks. In *Proceedings of Design, Automation and Test in Europe*, 2001.

[19] K. Sohrabi, J. Gao, V. Ailawadhi, and G.J. Pottie. Protocols for self-organization of a wireless sensor network. *IEEE Wireless Communications*, Oct. 2000.

[20] J. Byers and G. Nasser. Utility-Based Decision-Making in Wireless Sensor Networks. Technical Report BUCS-TR-2000-014, Boston University, 2000.

[21] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. Next century challenges: Scalable Coordination in Sensor Networks. In *ACM MobiCom*, 1999.

[22] J.M. Kahn, R.H. Katz, and K.S.J. Pister. Next century challenges: Mobile Networking for ”Smart Dust”. In *ACM MobiCom*, 1999.

[23] Scott Shenker. Fundamental Design Issues for the Future Internet. *IEEE Journal on Selected Areas in Communications*, Sep. 1995.

[24] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In *ACM International Workshop on Wireless Sensor Networks and Applications*, 2002.

[25] J. Kulik, W. Heinzelman, and H. Balakrishnan. Negotiation-based protocols for disseminating information in wireless sensor networks. *Wireless Networks*, March 2002.

[26] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan. Building efficient wireless sensor networks with low-level naming. In *ACM SIGOPS Operating Systems Review*, 2001.

[27] A. Manjeshwar and D.P. Agrawal. TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In *Parallel and Distributed Processing Symposium*, 2001.

[28] Fan Ye, A. Chen, Songwu Lu, and Lixia Zhang. A scalable solution to minimum cost forwarding in large sensor networks. In *International Conference on Computer Communications and Networks*, 2001.

[29] C. Intanagonwiwat, R. Govindan, and D. Estrin. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. In *ACM MobiCom*, 2000.

[30] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *IEEE Hawaii International Conference on System Sciences*, 2000.

[31] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan, and J. Lilley. The design and implementation of an intentional naming system. In *ACM SIGOPS Operating Systems Review*, 1999.

[32] E.M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, April 1999.

[33] Yogesh Sankarasubramaniam, zgr B. Akan, and Ian F. Akyildiz. ESRT: event-to-sink reliable transport in wireless sensor networks. In *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2003.

[34] Chieh-Yih Wan, A.T. Campbell, and L. Krishnamurthy. PSFQ: a reliable transport protocol for wireless sensor networks. In *ACM International Workshop on Wireless Sensor Networks and Applications*, 2002.

[35] A. Woo and D. Culler. A Transmission Control Scheme for Media Access in Sensor Networks. In *ACM MobiCom*, 2001.

[36] A. Ephremides. Energy concerns in wireless networks. *IEEE Wireless Communications*, Aug. 2002.

[37] V. Raghunathan, C. Schurgers, Sung Park, and M.B. Srivastava. Energy-aware wireless microsensor networks. *IEEE Signal Processing Magazine*, March 2002.

[38] Y.J. Zhao, R. Srivastava, and D. Estrin. Residual energy scan for monitoring sensor networks. In *IEEE Wireless Communications and Networking Conference*, 2002.

[39] E. Shih, Seong-Hwan Cho, N. Ickes, Rex Min, A. Sinha, A. Wang, and A. Chandrakasan. Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks. In *ACM MobiCom*, 2001.

[40] D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and S. Wicker. Complex Behavior at Scale: An Experimental Study of Low-Power Wireless Sensor Networks. Technical Report UCLA/CSD-TR 02-0013, UCLA Computer Science Dept., 2002.

[41] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. SPINS: security protocols for sensor networks. *Wireless Networks*, Sep. 2002.

[42] D. Balfanz, D. Smetters, P. Stewart, and H. Wong. Talking to strangers: Authentication in adhoc wireless networks. In *Symposium on Network and Distributed Systems Security*, 2002.

[43] Frank Stajano. The Resurrecting Duckling – What Next? *Lecture Notes in Computer Science*, 2133:204–??, Sep. 2001.

[44] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks wireless networks. In *7th International Workshop on Security Protocols*, 1999.