Chapter 2

COMMUNICATION PROTOCOLS FOR SENSOR NETWORKS

Weilian Su,[1] Özgür B. Akan,[2] and Erdal Cayirci[3]

[1] *Broadband and Wireless Networking Laboratory*
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332-0250 U.S.A
weilian@ece.gatech.edu

[2] *Broadband and Wireless Networking Laboratory*
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332-0250 U.S.A
akan@ece.gatech.edu

[3] *Istanbul Technical University*
80626 Istanbul Turkey
cayirci@cs.itu.edu.tr

Abstract This chapter describes about the challenges and essence of designing communication protocols for wireless sensor networks. The sensor nodes are densely deployed and collaboratively work together to provide higher quality sensing in time and space as compared to traditional stationary sensors. The applications of these sensor nodes as well as the issues in the transport, network, datalink, and physical layers are discussed. For applications that require precise timing, different types of timing techniques are explored.

Keywords: Wireless Sensor Networks, Sensor Network Applications, Transport Layer, Networking Layer, Data Link Layer, Medium Access Control, Error Control, Physical Layer, and Time Synchronization Schemes.

INTRODUCTION

Recent advances in wireless communications, digital electronics, and analog devices have enabled sensor nodes that are low-cost and low-power to communicate untethered in short distances and collaborate as a group. These sensor nodes leverage the strength of collaborative effort to provide higher quality sensing in time and space as compared to traditional stationary sensors, which are deployed in the following two ways [18]:

- Sensors can be positioned far from the actual *phenomenon*, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.

- Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

The sensor nodes are deployed either inside the phenomenon or very close to it. They may self-organize into clusters or collaborate together to complete a task that is issued by the users. In addition, the positions of these nodes do not need to be predefined. As a result, the sensor nodes are fit for many applications, e.g., location tracking and chemical detection in areas not easily accessible. Since sensing applications generate a large quantity of data, these data may be fused or aggregated together to lower the energy consumption. The sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. In essence, wireless sensor networks with these capabilities may provide the end users with intelligence and a better understanding of the environment. In the future, the wireless sensor networks may be an integral part of our lives, more so than the present-day personal computers.

Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of wireless sensor networks. To illustrate this point, the differences between wireless sensor networks and ad-hoc networks [32] are outlined below:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.

- Sensor nodes are densely deployed.

- Sensor nodes are prone to failures.

- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global *identification* (ID) because of the large amount of overhead and large number of sensors.
- Sensor networks are deployed with a specific sensing application in mind whereas ad-hoc networks are mostly constructed for communication purposes.

Recently, as a result of the above differences and the potential application of wireless sensor networks, the sensor networks have attracted many interest in the research community. In this chapter, the challenges and essence of designing wireless sensor network protocols are described and discussed. We present some potential sensor network applications in Section 2.1. These applications may provide more insight into the usefulness of wireless sensor networks. Also, the challenges and essence of designing transport, network, datalink, and physical layer protocols and algorithms to enable these applications are described. In addition to these guidelines, we explore the different types of timing techniques and the issues that these techniques have to address in Section 2.6. Lastly, we conclude our chapter in Section 2.7.

2.1 APPLICATIONS OF SENSOR NETWORKS

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions that are listed in Table 2.1. An example of some MICA [27] motes is illustrated in Figure 2.1. The size of the MICA motes is small as compared to the size of a dime. These motes may be controlled by a computer through the sink, which is a MICA mote with a computer interface.

Sensor nodes can be used for continuous sensing, event detection, event identification, location sensing, and local control of actuators. The concept of microsensing and wireless connection of these nodes promise many new application areas, e.g., military, environment, health, home, commercial, space exploration, chemical processing and disaster relief, etc. Some of these application areas are described in Section 2.1.1. In addition, some application layer protocols are introduced in Section 2.1.2; they are used to realize these applications.

Table 2.1. Examples of ambient conditions.

Environmental Ambient Conditions
Temperature
Humidity
Vehicular movement
Lightning condition
Pressure
Soil makeup
Noise levels

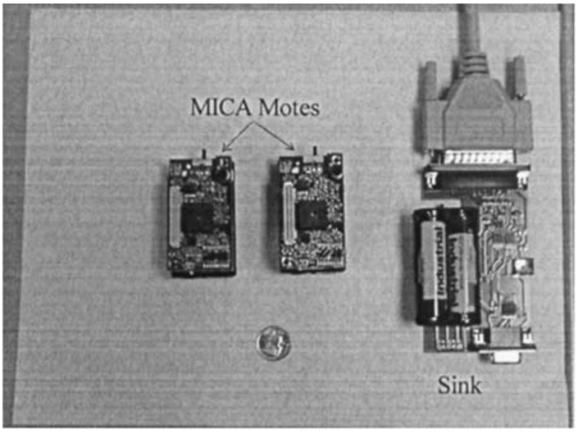

Figure 2.1. Example of MICA motes.

2.1.1 WIRELESS SENSOR NETWORK APPLICATIONS

The number of potential applications for wireless sensor networks is huge. Actuators may also be included in the sensor networks, which makes the number of applications that can be developed much higher. In this section, some example applications are given to provide the reader with a better insight about the potentials of wireless sensor networks.

Military Applications: Wireless sensor networks can be an integral part of military *command, control, communications, computers, intelligence, surveillance, reconnaissance and tracking* (C4ISRT) systems. The rapid deployment, self organization and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military C4ISRT. Since sensor networks are based on the dense deployment of disposable and low cost sensor nodes, destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of a traditional sensor. Some of the military applications are monitoring friendly forces, equipment and ammunition; battlefield surveillance; reconnaissance of opposing forces and terrain; targeting; battle damage assessment; and nuclear, biological and chemical attack detection and reconnaissance.

Environmental Applications: Some environmental applications of sensor networks include tracking the movements of species, i.e., habitat monitoring; monitoring environmental conditions that affect crops and livestock; irrigation; macroinstruments for large-scale Earth monitoring and planetary exploration; and chemical/biological detection [1, 3–5, 16, 18, 20, 21, 43, 47].

Commercial Applications: The sensor networks are also applied in many commercial applications. Some of them are building virtual keyboards; managing inventory control; monitoring product quality; constructing smart office spaces; and environmental control in office buildings [1, 5, 11, 12, 21, 37, 38, 42, 47, 35].

2.1.2 APPLICATION LAYER PROTOCOLS FOR WIRELESS SENSOR NETWORKS

Although many application areas for wireless sensor networks are defined and proposed, potential application layer protocols for sensor networks remain largely unexplored. Three possible application layer protocols are introduced in this section; they are *Sensor Management Protocol*, *Task Assignment and Data Advertisement Protocol*, and *Sensor Query and Data Dissemination Protocol*. These protocols may require protocols at other stack layers that are explained in Sections 2.2, 2.3, 2.4, 2.5, and 2.6.

Sensor Management Protocol (SMP). Designing an application layer management protocol has several advantages. Sensor networks have many different application areas, and accessing them through networks such as Internet is aimed in some current projects [35]. An application layer management protocol makes the hardware and softwares of the lower layers transparent to the sensor network management applications.

System administrators interact with sensor networks by using *sensor management protocol* (SMP). Unlike many other networks, sensor networks consist of nodes that do not have global identification, and they are usually infrastructureless. Therefore, SMP needs to access the nodes by using attribute-based naming and location-based addressing, which are explained in detail in Section 2.3.

SMP is a management protocol that provides the software operations needed to perform the following administrative tasks:

- Introducing the rules related to data aggregation, attribute-based naming and clustering to the sensor nodes,
- Exchanging data related to the location finding algorithms,
- Time synchronization of the sensor nodes,
- Moving sensor nodes,
- Turning sensor nodes on and off,
- Querying the sensor network configuration and the status of nodes, and re-configuring the sensor network, and
- Authentication, key distribution and security in data communications.

The descriptions of some of these tasks are given in [8, 11, 33, 40, 41].

Task Assignment and Data Advertisement Protocol (TADAP). Another important operation in the sensor networks is interest dissemination. Users send their interest to a sensor node, a subset of the nodes or whole network. This interest may be about a certain attribute of the phenomenon or a triggering event. Another approach is the advertisement of available data in which the sensor nodes advertise the available data to the users, and the users query the data which they are interested in. An application layer protocol that provides the user software with efficient interfaces for interest dissemination is useful for lower layer operations, such as routing.

Sensor Query and Data Dissemination Protocol (SQDDP). The *Sensor Query and Data Dissemination Protocol* (SQDDP) provides user applications with interfaces to issue queries, respond to queries and collect incoming replies. Note that these queries are generally not issued to particular nodes. Instead, attribute-based or location-based naming is preferred. For instance, "*the locations of the nodes that sense temperature higher than* 70^oF " is an attribute-based query. Similarly, "*temperatures read by the nodes in Region A*" is an example for location based naming.

Likewise, the *sensor query and tasking language* (SQTL) [41] is proposed as an application that provides even a larger set of services. SQTL supports three types of events, which are defined by keywords *receive*, *every*, and *expire*. *Receive* keyword defines events generated by a sensor node when the sensor node receives a message; *every* keyword defines events occurred periodically due to a timer time-out; and *expire* keyword defines the events occurred when a timer is expired. If a sensor node receives a message that is intended for it and contains a script, the sensor node then executes the script. Although SQTL is proposed, different types of SQDDP can be developed for various applications. The use of SQDDPs may be unique to each application.

2.2 TRANSPORT LAYER

The wireless sensor network is an event driven paradigm that relies on the collective effort of numerous sensor nodes. This collaborative nature brings several advantages over traditional sensing including greater accuracy, larger coverage area and extraction of localized features. The realization of these potential gains, however, directly depends on the efficient reliable communication between the wireless sensor network entities, i.e., the sensor nodes and the sink.

To accomplish this, in addition to robust modulation and media access, link error control and fault tolerant routing, a reliable transport mechanism is imperative. The functionalities and design of a suitable transport solution for the wireless sensor networks are the main issues addressed in this section.

The need for transport layer in the wireless sensor networks is pointed out in the literature [35, 38]. In general, the main objectives of the transport layer are (i) to bridge application and network layers by application multiplexing and demultiplexing; (ii) to provide data delivery service between the source and the sink with an error control mechanism tailored according to the specific reliability requirement of the application layer; and (iii) to regulate the amount of traffic injected to the network via flow and congestion control mechanisms. Although these objectives are still valid, the required transport layer functionalities to achieve these objectives in the wireless sensor networks are subject to significant modifications in order to accommodate unique characteristics of the wireless sensor network paradigm. The energy, processing, and hardware limitations of the wireless sensor nodes bring further constraints on the transport layer protocol design. For example, the conventional end-to-end retransmission-based error control and the window-based additive-increase multiplicative-decrease congestion control mechanisms adopted by the vastly used *Transport Control Protocol* (TCP) protocols may not be feasible for the wireless sensor network domain and hence, may lead to waste of scarce resources.

On the other hand, unlike the other conventional networking paradigms, the wireless sensor networks are deployed with a specific sensing application objective. For example, sensor nodes can be used within a certain deployment scenario to perform continuous sensing, event detection, event identification, location sensing, and local control of actuators for a wide range of applications such as military, environment, health, space exploration, and disaster relief.

The specific objective of a sensor network also influences the design requirements of the transport layer protocols. For example, the sensor networks deployed for different applications may require different reliability level as well as different congestion control approaches.

Consequently, the development of transport layer protocols is a challenging effort, because the limitations of the sensor nodes and the specific application requirements primarily determine the design principles of the transport layer protocols. With this respect, the main objectives and the desired features of the transport layer protocols that can address the unique requirements of the wireless sensor networks paradigm can be stated as follows:

- *Reliable Transport:* Based on the application requirements, the extracted event features should be reliably transferred to the sink. Similarly, the programming/retasking data for sensor operation, command and queries should be reliably delivered to the target sensor nodes to assure the proper functioning of the wireless sensor network.

- *Congestion Control:* Packet loss due to congestion can impair event detection at the sink even when enough information is sent out by the sources. Hence, congestion control is an important component of the transport layer to achieve reliable event detection. Furthermore, congestion control not only increases the network efficiency but also helps conserve scarce sensor network resources.

- *Self-configuration:* The transport layer protocols must be adaptive to dynamic topologies caused by node mobility/failure/temporary power-down, spatial variation of events and random node deployment.

- *Energy Awareness:* The transport layer functionalities should be energy-aware, i.e., the error and congestion control objectives must be achieved with minimum possible energy expenditure. For instance, if reliability levels at the sink are found to be in excess of that required for the event detection, the source nodes can conserve energy by reducing the amount of information sent out or temporarily powering down.

- *Biased Implementation:* The algorithms must be designed such that they mainly run on the sink with minimum functionalities required at sensor nodes. This helps conserve limited sensor resources and shifts the burden to the high-powered sink.

- *Constrained Routing/Addressing:* Unlike protocols such as TCP, the transport layer protocols for wireless sensor networks should not assume the existence of an end-to-end global addressing. It is more likely to have attribute-based naming and data-centric routing, which call for different transport layer approaches.

Due to the application-oriented and collaborative nature of the wireless sensor networks, the main data flow takes place in the *forward path*, where the source nodes transmit their data to the sink. The *reverse path*, on the other hand, carries the data originated from the sink such as programming/retasking binaries, queries and commands to the source nodes. Although the above objectives and the desired features are common for the transport layer protocols, different functionalities are required to handle the transport needs of the forward and reverse paths.

For example, the correlated data flows in the forward path are loss-tolerant to the extent that event features are reliably communicated to the sink. However, data flows in the reverse channel are mainly related to the operational communication such as dissemination of the new operating system binaries, which usually requires 100 % reliable delivery. Therefore, a reliability mechanism would not suffice to address the requirements of both forward and reverse paths. Hence, the transport layer issues pertaining to these distinct cases are studied separately in the following sections.

2.2.1 EVENT-TO-SINK TRANSPORT

In order to realize the potential gains of the collective effort of numerous sensor nodes, it is detrimental that extracted event features at the sensor nodes are reliably communicated to the sink. This necessitates a reliable transport layer mechanism that can assure the *event-to-sink reliability.*

The need for a transport layer for data delivery in the wireless sensor networks was questioned in [36] under the premise that data flows from source to sink are generally loss tolerant. While the need for end-to-end reliability may not exist due to the sheer amount of correlated data flows, an event in the sensor field needs to be tracked with a certain accuracy at the sink. Hence, unlike traditional communication networks, the sensor network paradigm necessitates an event-to-sink reliability notion at the transport layer [39]. This involves a reliable communication of the event features to the sink rather than conventional packet-based reliable delivery of the individual sensing reports/packets generated by each sensor node in the field. Such *event-to-sink reliable transport* notion based on collective identification of data flows from the event to the sink is illustrated in Figure 2.2.

In order to provide reliable event detection at the sink, possible congestion in the forward path should also be addressed by the transport layer. Once the event is sensed by a number of sensor nodes within the coverage of the phenomenon, i.e., event radius, significant amount of traffic is triggered by these sensor nodes, which may easily lead to congestion in the forward path. The need for transport layer congestion control to assure reliable event detection at the sink is revealed by the results in [19]. It has been shown in [19] that

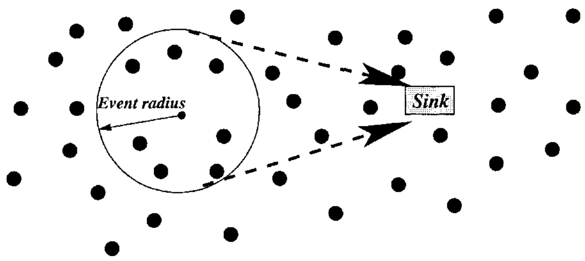

Figure 2.2. Typical sensor network topology with event and sink. The sink is only interested in collective information of sensor nodes within the event radius and not in their individual data.

exceeding network capacity can be detrimental to the observed goodput at the sink. Moreover, although the event-to-sink reliability may be attained even in the presence of packet loss due to network congestion thanks to the correlated data flows, a suitable congestion control mechanism can also help conserve energy while maintaining desired accuracy levels at the sink.

On the other hand, although the transport layer solutions in conventional wireless networks are relevant, they are simply inapplicable for the event-to-sink reliable transport in the wireless sensor networks. These solutions mainly focus on reliable data transport following end-to-end TCP semantics and are proposed to address the challenges posed by wireless link errors and mobility [2]. The primary reason for their inapplicability is their notion of end-to-end reliability which is based on acknowledgments and end-to-end retransmissions. Due to inherent correlation in the data flows generated by the sensor nodes, however, these mechanisms for strict end-to-end reliability are significantly energy-draining and superfluous. Furthermore, all these protocols bring considerable memory requirements to buffer transmitted packets until they are ACKed by the receiver. In contrast, sensor nodes have limited buffering space (<4KB in MICA motes [27]) and processing capabilities.

In contrast to the transport layer protocols for conventional end-to-end reliability, *Event-to-Sink Reliable Transport* (ESRT) protocol [39] is based on the event-to-sink reliability notion and provides reliable event detection without any intermediate caching requirements. ESRT is a novel transport solution developed to achieve reliable event detection in the wireless sensor networks with minimum energy expenditure. It includes a congestion control component that serves the dual purpose of achieving reliability and conserving energy. ESRT also does not require individual sensor identification, i.e., an event ID suffices. Importantly, the algorithms of ESRT mainly run on the sink, with minimal functionality required at resource constrained sensor nodes.

2.2.2 SINK-TO-SENSORS TRANSPORT

While the data flows in the forward path carry correlated sensed/detected event features, the flows in the reverse path mainly contain data transmitted by the sink for an operational or application-specific purposes. This may include the operating system binaries, programming/retasking configuration files, application-specific queries and commands. Dissemination of this type of data mostly requires 100 % reliable delivery. Therefore, the event-to-sink reliability approach introduced before would not suffice to address such tighter reliability requirement of the flows in the reverse paths.

Such strict reliability requirement for the sink-to-sensors transport of operational binaries and application-specific query and commands involves in certain level of retransmission as well as acknowledgment mechanisms. However, these mechanisms should be incorporated into the transport layer protocols cautiously in order not to totally compromise scarce sensor network resources. With this respect, local retransmissions and negative acknowledgment approaches would be preferable over the end-to-end retransmissions and acknowledgments to maintain minimum energy expenditure.

On the other hand, sink is involved more in the sink-to-sensor data transport on the reverse path. Hence, the sink with plentiful energy and communication resources can broadcast the data with its powerful antenna. This helps to reduce the amount of traffic forwarded in the multi-hop wireless sensor network infrastructure and hence, helps sensor nodes conserve energy. Therefore, data flows in the reverse path may experience less congestion in contrast to the forward path, which is totally based on multi-hop communication. This calls for less aggressive congestion control mechanisms for the reverse path as compared to the forward path in the wireless sensor networks.

The multi-hop and one-to-many nature of data flows in the reverse path of the wireless sensor networks prompt a review of reliable multicast solutions proposed in other wired/wireless networks. There exist many such schemes that address the reliable transport and congestion control for the case of single sender and multiple receivers [14]. Although the communication structure of the reverse path, i.e., from sink to sources, is an example of multicast, these schemes do not stand as directly applicable solutions; rather, they need significant modifications/improvements to address the unique requirements of the wireless sensor network paradigm.

In [36], the *Pump Slowly, Fetch Quickly* (PSFQ) mechanism is proposed for reliable retasking/reprogramming in the wireless sensor networks. PSFQ is based on slowly injecting packets into the network but performing aggressive hop-by-hop recovery in case of packet loss. The pump operation in PSFQ simply performs controlled flooding and requires each intermediate node to create and maintain a data cache to be used for local loss recovery and insequence data delivery. Although this is an important transport layer solution for the wireless sensor networks, PSFQ does not address packet loss due to congestion.

In summary, the transport layer mechanisms that can address the unique challenges posed by the wireless sensor network paradigm are essential to realize the potential gains of the collective effort of wireless sensor nodes. As discussed in Sections 2.2.1 and 2.2.2, there exist promising solutions for both event-to-sink and sink-to-sensors reliable transports. These solutions and the ones that are currently under development, however, need to be exhaustively evaluated under the real wireless sensor network deployment scenarios to reveal their shortcomings; hence, necessary modifications/improvements may be required to provide a complete transport layer solution for the wireless sensor networks.

2.3 NETWORK LAYER

Sensor nodes are scattered densely in a field either close to or inside the phenomenon. Since they are densely deployed, neighbor nodes may be very close to each other. As a result, multihop communication in the wireless sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels may be kept low, which is highly desired for covert operations. In addition, multihop communication may effectively overcome some of the signal propagation effects experienced in long distance wireless communication. As discussed in Section 2, the ad hoc routing techniques already proposed in the literature [32] do not usually fit the requirements of the wireless sensor networks. As a result, the networking layer of the sensor networks is usually designed according to the following principles:

- Power efficiency is always an important consideration.
- Sensor networks are mostly data-centric.
- An ideal sensor network has attribute-based addressing and location awareness.
- Data aggregation is useful only when it does not hinder the collaborative effort of the sensor nodes.
- The routing protocol is easily integrated with other networks, e.g., Internet.

The above principles serve as a guideline in designing a routing protocol for the wireless sensor networks. As discussed in Section 2.2, a transport protocol has to be energy aware. This criteria also applies to a routing protocol designed for the wireless sensor networks since the life-time of the networks depends on the longevity of each sensor node. In addition, a routing protocol may be data-centric. A data-centric routing protocol requires attribute-based naming [31, 41, 10, 8]. For attribute-based naming, the users are more interested in querying an attribute of the phenomenon, rather than querying an individual node. For instance, "*the areas where the temperature is over* 70^oF" is a more common query than "*the temperature read by a certain node*". The attribute-based naming is used to carry out queries by using the attributes of the phenomenon. It also makes broadcasting, attribute-based multi-casting, geo-casting and any-casting important for sensor networks.

For example, if interest dissemination is based on data-centric, it is performed by assigning the sensing tasks to the sensor nodes. There are two approaches used for interest dissemination: (i) sinks broadcast the interest [18] and (ii) sensor nodes broadcast an advertisement for the available data [16] and wait for a request from the interested sinks.

As data-centric routing is important, it should also leverage the usefulness of data aggregation. Data-aggregation is a technique used to solve the implosion and overlap problems in data-centric routing [16]. In this technique, a sensor network is usually perceived as a reverse multicast tree as shown in Figure 2.3, where the sink asks the sensor nodes to report the ambient condition of the phenomena. Data coming from multiple sensor nodes are aggregated as if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink. For example, sensor node E aggregates the data from sensor nodes A and B while sensor node F aggregates the data from sensor nodes C and D as shown in Figure 2.3. Data aggregation can be perceived as a set of automated methods of combining the data that comes from many sensor nodes into a set of meaningful information [17]. With this respect, data aggregation is known as data fusion [16]. Also, care must be taken when aggregating data, because the specifics of the data, e.g., the locations of reporting sensor nodes, should not be left out. Such specifics may be needed by certain applications.

One other important function of the network layer is to provide internetworking with other networks such as other sensor networks, command and control systems and the Internet. In one scenario, the sink nodes can be used as a gateway to other networks while in another scenario they serve as a backbone to other networks. As shown in Figure 2.4, the sinks are the gateways to the sensor networks as well as the bases for the communication backbone between the user and the sensor nodes.

When developing a routing protocol with the design-principles in mind, one of the following approaches can be used to select an energy efficient route. Figure 2.5 is used to describe each of these approaches, and node T is the source node that senses the phenomena. The possible routes used to communicate with the sink in these approaches are given in Table 2.2.

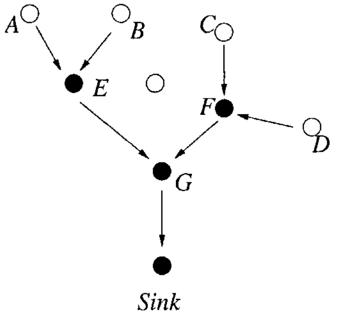

Figure 2.3. Example of data aggregation.

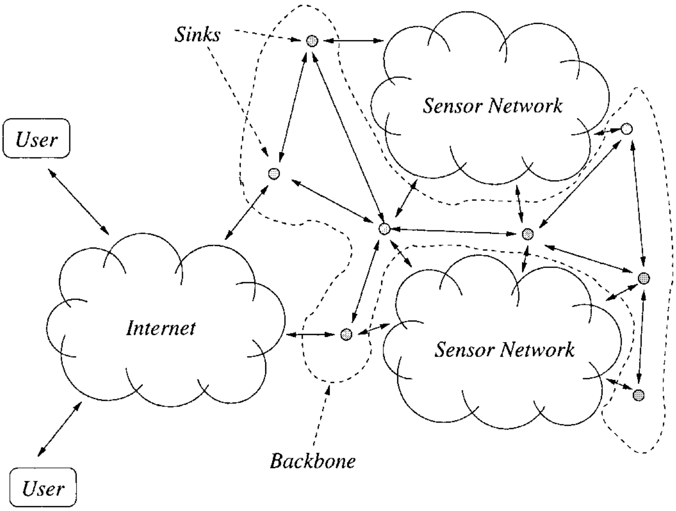

Figure 2.4. Internetworking between sensor nodes and user.

Table 2.2. Possible routes between the source and sink.[a]

Possible Routes	*Description*
Route 1	Sink-A-B-T, total PA=4, total α = 3
Route 2	Sink-A-B-C-T, total PA=6, total α = 6
Route 3	Sink-D-T, total PA=3, total α = 4
Route 4	Sink-E-F-T, total PA=5, total α = 6

[a] PA is the available power, and α_i is the energy required to transmit a data packet through the related link.

- *Maximum Available Power (PA) Route:* The route that has maximum total available power is preferred. The total PA is calculated by summing the PAs of each node along the route. Based on this approach, Route 2

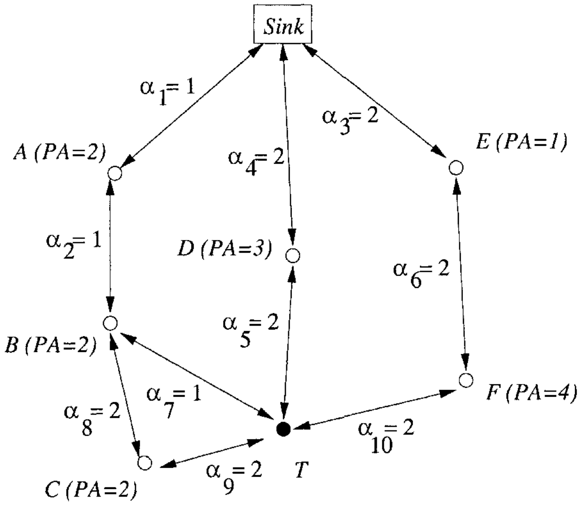

Figure 2.5. The power efficiency of the routes.

is selected in Figure 2.5. However, Route 2 includes the nodes in Route 1 and an extra node. Therefore, although it has a higher total PA, it is not a power efficient one. As a result, it is important not to consider the routes derived by extending the routes that can connect the sensor to the sink as an alternative route. Eliminating Route 2, Route 4 is selected as the power efficient route when the maximum PA scheme is used.

- *Minimum Energy (ME) Route:* The route that consumes minimum energy to transmit the data packets between the sink and the sensor node is the ME route. As shown in Figure 2.5, Route 1 is the ME route.

- *Minimum Hop (MH) Route:* The route that makes the minimum hop to reach the sink is preferred. Route 3 in Figure 2.5 is the most efficient route based on this scheme. Note that the ME scheme selects the same route as the MH when the same amount of energy, i.e., all α are the same, is used on every link. Therefore, when nodes broadcast with same power level without any power control, MH is then equivalent to ME.

- *Maximum Minimum PA Node Route:* The route along which the minimum PA is larger than the minimum PAs of the other routes is preferred. In Figure 2.5, Route 3 is the most efficient and Route 1 is the second efficient paths. This scheme precludes the risk of using up a sensor node with low PA much earlier than the others because they are on a route with nodes which has very high PAs.

A brief summary of the state-of-the-arts in the networking area is shown in Table 2.3. The *Small Minimum Energy Communication Network* (SMECN) [24] creates an energy efficient subgraph of the sensor networks. It tries to minimize the energy consumption while maintaining connectivity of the nodes in the network. Besides subgraph creation, the sensor nodes may form energy efficient clusters using the *Low Energy Adaptive Clustering Hierarchy* (LEACH) scheme [17]. In addition, QoS routing trees may be created with the *Sequential Assignment Routing* (SAR) protocol [45]; the sources send the collected data back to the sink through one of these routing trees. The collected data or queries may also be disseminated by flooding, gossiping [15], *Sensor Protocols for Information via Negotiation* (SPIN) [16], or directed diffusion protocol [18]. The directed diffusion protocol is a data-centric dissemination protocol, and the queries and collected data use the attribute-based naming schemes.

Although the protocols listed in Table 2.3 resolve some of the network layer issues, there are still room for more advanced data-centric routing protocols. In addition, different applications of the sensor networks may require different types of routing protocols. This is also a driving force for developing new transport protocols as described in Section 2.2 as well as data link schemes, which is discussed in the following section.

Table 2.3. An overview of network layer schemes.

Network Layer Scheme	*Description*
SMECN [24]	-Creates a sub graph of the sensor network that contains the minimum-energy path.
LEACH [17]	-Forms clusters to minimize energy dissipation.
SAR [45]	-Creates multiple trees where the root of each tree is one hop neighbor from the sink; select a tree for data to be routed back to the sink according to the energy resources and additive QoS Metric.
Flooding	-Broadcasts data to all neighbor nodes regardless if they receive it before or not.
Gossiping [15]	-Sends data to one randomly selected neighbor.
SPIN [16]	-Sends data to sensor nodes only if they are interested; has three types of messages, i.e., ADV, REQ, and DATA.
Directed Diffusion [18]	-Sets up gradients for data to flow from source to sink during interest dissemination.

2.4 DATA LINK LAYER

As discussed in Section 2.2, the wireless sensor networks are deployed with an objective of reliable event detection at the sink based on the collective effort of numerous sensor nodes spread in the sensor field. Although the transport layer is essential to achieve higher level error and congestion control, it is still imperative to have the data link layer functionalities in the wireless sensor networks.

In general, the data link layer is primarily responsible for the multiplexing of data streams, data frame detection, medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network. Nevertheless, the collaborative and application-oriented nature of the wireless sensor networks and the physical constraints of the sensor nodes such as energy and processing limitations determine the way these responsibilities are fulfilled. In the following two subsections, the data link layer issues are explored within the discussion of the medium access and error control strategies in the wireless sensor networks.

2.4.1 MEDIUM ACCESS CONTROL

The *Medium Access Control* (MAC) layer protocols in a wireless multi-hop self-organizing sensor network must achieve two objectives. The first one is to establish communication links for data transfer; this is necessary for creating a basic network infrastructure that is needed for multi-hop wireless communication in a densely scattered sensor field. This also provides the sensor network with self-organizing ability. The second objective is to regulate the access to the shared media such that communication resources are fairly and efficiently shared between the wireless sensor nodes.

The unique resource constraints and application requirements of sensor networks, however, denounce the MAC protocols for the conventional wireless networks inapplicable to the wireless sensor network paradigm. For example, the primary goal of a MAC protocol in an infrastructure-based cellular system is the provision of high QoS and bandwidth efficiency mainly with dedicated resource assignment strategy. Power conservation assumes only secondary importance as base stations have unlimited power supply and the mobile user can replenish exhausted batteries in the handset. Such an access scheme is impractical for sensor networks as there is no central controlling agent like the base station. Moreover, power efficiency directly influences network lifetime in a sensor network and hence, is of prime importance.

While Bluetooth and the *Mobile Ad-Hoc Network* (MANET) show similarities to the wireless sensor networks in terms of communication infrastructure, both of them consist of the nodes that have portable battery-powered devices, which can be replaced by the user. Hence, unlike the wireless sensor networks, power consumption is only of secondary importance in both of these systems. For example, the transmission power of a Bluetooth device is typically around 20 dBm, and the transmission range is of the order of 10s of meters. However, the transmission power of a sensor node is around 0 dBm, and hence, the radio range is much less than the one of a Bluetooth or MANET device. Therefore, none of the existing Bluetooth or MANET MAC protocols can be directly used in the wireless sensor networks due to the network lifetime concerns in a sensor network.

It is evident that the MAC protocol for sensor networks must have built-in power conservation, mobility management, and failure recovery strategies. Thus far, both *fixed allocation* and *random access* versions of medium access have been proposed [45, 49]. *Demand-based* MAC schemes may be unsuitable for sensor networks due to their large messaging overhead and link setup delay. Furthermore, contention-based channel access is deemed unsuitable due to their requirement to monitor the channel at all times, which is an energy-draining task. A qualitative overview of some MAC protocols proposed for wireless sensor networks are summarized in Table 2.4. The applicability of the fundamental MAC schemes in the wireless sensor networks is discussed along with some proposed MAC solutions using that access method as follows:

Table 2.4. Qualitative overview of MAC protocols for sensor networks.

MAC Protocol	*Channel Access*	*Features and Advantages*
SMACS [45]	Fixed allocation of duplex time slots at fixed frequency	- Exploits large available bandwidth compared to sensor data rate - Random wake up during setup and turning radio off while idle
Hybrid TDMA/FDMA [42]	Centralized frequency and time division	- Optimum number of channels for minimum system energy - Hardware based approach for system energy minimization
CSMA based [49]	Contention based random access	- Application phase shift and pre-transmit delay - Constant listening time for energy efficiency

- *TDMA-Based Medium Access:* In a *time-division multiple-access* (TDMA) scheme, a channel is granted to a source for a certain time duration. TDMA-based access schemes are inherently more energy-conserving compared to contention-based schemes since the duty cycle of the radio is reduced, and there is no contention-introduced overhead and collisions. It has been reasoned in [35] that MAC scheme for energy-constrained sensor networks should include a variant of TDMA since radios must be turned off during idling for precious power savings. The *Self-organizing Medium Access Control for Sensor networks* (SMACS)

[45] is such a time-slot based access protocol where each sensor node maintains a TDMA-like frame, called super frame, in which the node schedules different time slots to communicate with its known neighbors. SMACS achieves power conservation by using a random wake-up schedule during the connection phase and by turning the radio off during idle time slots. However, while TDMA-based access scheme minimizes the transmit-on time, it is not always preferred due to the associated time synchronization costs.

- *Hybrid TDMA/FDMA Based Medium Access:* While a pure TDMA-based access scheme dedicates the entire channel to a single sensor node, a pure *Frequency-Division Multiple Access* (FDMA) scheme allocates minimum signal bandwidth per node. Such contrast brings the tradeoff between the access capacity and the energy consumption. An analytical formula is derived in [42] to find the optimum number of channels, which gives the minimum system *power consumption.* This determines the hybrid TDMA-FDMA scheme to be used. The optimum number of channels is found to depend on the ratio of the power consumption of the transmitter to that of the receiver. If the transmitter consumes more power, a TDMA scheme is favored, while the scheme leans toward FDMA when the receiver consumes greater power. Such centrally controlled hybrid TDMA/FDMA based MAC scheme is already developed [42] for a time-sensitive machine monitoring application of the energy-constrained sensor network.

- *CSMA-Based Medium Access:* The traditional *Carrier-Sense Multiple Access* (CSMA) based schemes, which are based on carrier sensing and backoff mechanism, are deemed inappropriate since they all make the fundamental assumption of stochastically distributed traffic and tend to support independent point-to-point flows. On the contrary, the MAC protocol for sensor networks must be able to support variable, but highly correlated and dominantly periodic traffic. Any CSMA-based medium access scheme has two important components, the *listening mechanism* and the *backoff scheme.* A CSMA-based MAC scheme for sensor networks is presented in [49]. As reported and based on simulations in [49], the constant listen periods are energy efficient and the introduction of random delay provides robustness against repeated collisions.

2.4.2 ERROR CONTROL

In addition to the medium access control, error control of the transmitted data in the wireless sensor networks is another extremely important function of the data link layer. Error control is critical especially in some sensor network applications such as mobile tracking and machine monitoring. In general, the error control mechanisms in communication networks can be categorized into two main approaches, i.e., *Forward Error Correction* (FEC) and *Automatic Repeat reQuest* (ARQ).

ARQ-based error control mainly depends on the retransmission for the recovery of the lost data packets/frames. It is clear that such ARQ-based error control mechanism incurs significant additional retransmission cost and overhead. Although ARQ-based error control schemes are utilized at the data link layer for the other wireless networks, the usefulness of ARQ in sensor network applications is limited due to the scarcity of the energy and processing resources of the wireless sensor nodes. On the other hand, FEC schemes have inherent decoding complexity which require relatively considerable processing resources in the wireless sensor nodes. In this respect, simple error control codes with low-complexity encoding and decoding might present the best solutions for error control in the wireless sensor networks. In the following sections, the motivation and basic design requirements for FEC in the wireless sensor networks are explored.

Forward Error Correction. Due to the unpredictable and harsh nature of channels encountered in various wireless sensor network application scenarios, link reliability is detrimental to the performance of the entire sensor network. Some of the applications like mobile tracking and machine monitoring require high data precision. It is important to have good knowledge of the channel characteristics and implementation techniques for the design of efficient FEC schemes.

Channel *bit error rate* (BER) is a good indicator of link reliability. The BER is directly proportional to the symbol rate and inversely proportional to both the received signal-to-noise ratio and the transmitter power level. For a given error coding scheme, the received energy per symbol decreases if the data symbol rate and the transmission power remain unchanged. This corresponds to a higher BER at the decoder input than the one without coding. The decoder equipped with the coding scheme can then utilize the received redundant bits to correct the transmission errors to a certain degree. In fact, a good choice of the error correcting code can result in several orders of magnitude reduction in BER and an overall gain. The coding gain is generally expressed in terms of the additional transmit power needed to obtain the same BER without coding. For instance, a simple (15,11) Hamming code reduces BER by almost 10^3 and achieves a coding gain of 1.5 dB for binary phase shift keying modulated data and additive white gaussian noise model [48].

Therefore, the link reliability can be achieved either by increasing the output transmit power or the use of suitable FEC scheme. Due to the energy constraints of the wireless sensor nodes, increasing the transmit power is not a feasible option. Therefore, use of FEC is still the most efficient solution given the constraints of the sensor nodes. Although the FEC can achieve significant reduction in the BER for any given value of the transmit power, the additional processing power that is consumed during encoding and decoding must be considered when designing an FEC scheme. If the additional processing power is greater than the coding gain, then the whole process is not energy efficient and hence, the system is better off without coding. On the other hand, the FEC is a valuable asset to the sensor networks if the additional processing power is less than the transmission power savings. Thus, the tradeoff between this additional processing power and the associated coding gain need to be optimized in order to have powerful, energy-efficient and low-complexity FEC schemes for the error control in the wireless sensor networks.

In summary, it is evident that the performance of the entire wireless sensor network directly depends on the performance of the medium access and error control protocols used for the data link layer. Much additional research effort will be required to ultimately obtain the complete data link layer solutions that can efficiently address the unique challenges posed by the wireless sensor network paradigm.

2.5 PHYSICAL LAYER

The data link layer discussed in Section 2.4 multiplex the data streams and pass them to the the lowest layer in the communication architecture, i.e., the physical layer, for transmission. The physical layer is responsible for the conversion of bit streams into signals that are best suited for communication across the channel. More specifically, the physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption.

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. These links can be formed by radio, infrared or optical media. To enable global operation of these networks, the chosen transmission medium must be available worldwide. One option for radio links is the use of *Industrial, Scientific and Medical* (ISM) bands, which offer license-free communication in most countries. The *International Table of Frequency Allocations*, contained in Article S5 of the Radio Regulations (volume 1), specifies some frequency bands that may be made available for ISM applications. These frequency bands and the corresponding center frequencies are shown in Table 2.5.
Some of these frequency bands are already being used for communication in cordless phone systems and wireless local area networks. For sensor networks, a small sized, low cost, ultralow power transceiver is required. According to the authors of [34], certain hardware constraints and the tradeoff between antenna efficiency and power consumption limit the choice of a carrier frequency for such transceivers to the ultra high frequency range. They also propose

Table 2.5. Frequency bands available for ISM applications.

Frequency Band	*Center Frequency*
6765-6795 kHz	6780 kHz
13553-13567 kHz	13560 kHz
26957-27283 kHz	27120 kHz
40.66-40.70 MHz	40.68 MHz
433.05-434.79 MHz	433.92 MHz
902-928 MHz	915 MHz
2400-2500 MHz	2450 MHz
5725-5875 MHz	5800 MHz
24-24.25 GHz	24.125 GHz
61-61.5 GHz	61.25 GHz
122-123 GHz	122.5 GHz
244-246 GHz	245 GHz

the use of the 433 MHz ISM band in Europe and the 917 MHz ISM band in North America. Transceiver design issues in these two bands are addressed in [13, 26]. The main advantages of using the ISM bands are the free radio, huge spectrum allocation and global availability. They are not bound to a particular standard, thereby giving more freedom for the implementation of power saving strategies in sensor networks. On the other hand, there are various rules and constraints, like power limitations and harmful interference from existing applications. These frequency bands are also referred to as unregulated frequencies in literature.

Much of the current hardware for sensor nodes is based upon *radio frequency* (RF) circuit design. The μAMPS wireless sensor node [42] uses a Bluetooth-compatible 2.4 GHz transceiver with an integrated frequency synthesizer. In addition, the low-power sensor device [49] uses a single channel RF transceiver operating at 916 MHz. The *Wireless Integrated Network Sensors* architecture [35] also uses radio links for communication.

Another possible mode of inter-node communication in sensor networks is by infrared. Infrared communication is license-free and robust to interference from electrical devices. Infrared based transceivers are cheaper and easier to build. Many of today's laptop's, PDAs, and mobile phones offer an *Infrared Data Association* interface. The main drawback is the requirement of a line-of-sight between the sender and receiver. This makes infrared a reluctant choice for transmission medium in the sensor network scenario.

An interesting development is the *Smart Dust* mote [21], which is an autonomous sensing, computing, and communication system that uses optical medium for transmission. Two transmission schemes, passive transmission using a *corner-cube retroreflector* and active communication using a laser diode and steerable mirrors, are examined in [47]. In the former, the mote does not require an on-board light source. A configuration of three mirrors is used to communicate a digital high or low. The latter uses an on-board laser diode and an active-steered laser communication system to send a tightly collimated light beam toward the intended receiver.

The unusual application requirements of the wireless sensor networks make the choice of transmission media more challenging. For instance, marine applications may require the use of the aqueous transmission medium. Here, one would like to use long-wavelength radiation that can penetrate the water surface. Inhospitable terrain or battlefield applications might encounter error prone channels and greater interference. Moreover, the antenna of the sensor nodes might not have the height and radiation power of those in traditional wireless devices. Hence, the choice of transmission medium must be supported by robust coding and modulation schemes that efficiently model these vastly different channel characteristics.

The choice of a good modulation scheme is critical for reliable communication in a sensor network. Binary and M-ary modulation schemes are compared in [42]. While an M-ary scheme can reduce the transmit on-time by sending multiple bits per symbol, it results in complex circuitry and increased radio power consumption. The authors formulate these trade-off parameters and conclude that under startup power dominant conditions, the binary modulation scheme is more energy efficient. Hence, M-ary modulation gains are significant only for low startup power systems. A low-power direct-sequence spread-spectrum modem architecture for sensor networks is presented in [6]. This low power architecture can be mapped to an application-specific integrated circuit technology to further improve efficiency.

The *Ultra Wideband* (UWB) or impulse radio has been used for baseband pulse radar and ranging systems and has recently drawn considerable interest for communication applications, especially in indoor wireless networks [30]. The UWB employs baseband transmission and thus, requires no intermediate or radio carrier frequencies. Generally, pulse position modulation is used. The main advantage of UWB is its resilience to multipath [7, 22, 25]. Low transmission power and simple transceiver circuitry make UWB an attractive candidate for the wireless sensor networks.

It is well known that long distance wireless communication can be expensive, both in terms of energy and cost. While designing the physical layer for sensor networks, energy minimization assumes significant importance, over and above the decay, scattering, shadowing, reflection, diffraction, multipath and fading effects. In general, the minimum output power required to transmit a signal over a distance d is proportional to d^n, where $2 <= n < 4$. The exponent n is closer to four for low-lying antennae and near-ground channels [44], as is typical in sensor network communication. This can be attributed to the partial signal cancellation by a ground-reflected ray. While trying to resolve these problems, it is important that the designer is aware of inbuilt diversities and exploits this to the fullest. For instance, multihop communication in a sensor network can effectively overcome shadowing and path loss effects, if the node density is high enough. Similarly, while propagation losses and channel capacity limit data reliability, this very fact can be used for spatial frequency re-use. Energy efficient physical layer solutions are currently being pursued by researchers. Although some of these topics have been addressed in literature, it still remains a vastly unexplored domain of the wireless sensor network.

2.6 TIME SYNCHRONIZATION

Instead of time synchronization between just the sender and receiver during an application like in the Internet, the sensor nodes in the sensor field have to maintain a similar time within a certain tolerance throughout the lifetime of the network. Combining with the criteria that sensor nodes have to be energy efficient, low-cost, and small in a multi-hop environment as described in Section 2, this requirement makes a challenging problem to solve. In addition, the sensor nodes may be left unattended for a long period of time, e.g. in deep space or on an ocean floor. For short distance multi-hop broadcast, the data processing time and the variation of the data processing time may contribute the most in time fluctuations and differences in the path delays. Also, the time difference between two sensor nodes is significant over time due to the wandering effect of the local clocks.

Small and low-end sensor nodes may exhibit device behaviors that may be much worst than large systems such as *personal computers* (*PCs*). Some of the factors influencing time synchronization in large systems also apply to sensor networks [23]; they are *temperature*, *phase noise*, *frequency noise*, *asymmetric delays*, and *clock glitches*.

- *Temperature:* Since sensor nodes are deployed in various places, the temperature variation throughout the day may cause the clock to speed up or slow down. For a typical PC, the clock drifts few parts per million during the day [29]. For low end sensor nodes, the drifting may be even worst.

- *Phase Noise:* Some of the causes of phase noise are due to access fluctuation at the hardware interface, response variation of the operating system to interrupts, and jitter in the network delay. The jitter in the network delay may be due to medium access and queueing delays.

- *Frequency Noise:* The frequency noise is due to the unstability of the clock crystal. A low-end crystal may experience large frequency fluctuation, because the frequency spectrum of the crystal has large sidebands on adjacent frequencies.
- *Asymmetric Delay:* Since sensor nodes communicate with each other through the wireless medium, the delay of the path from one node to another may be different than the return path. As a result, an asymmetric delay may cause an offset to the clock that can not be detected by a variance type method [23]. If the asymmetric delay is static, the time offset between any two nodes is also static. The asymmetric delay is bounded by one-half the round trip time between the two nodes [23].
- *Clock Glitches:* Clock glitches are sudden jumps in time. This may be caused by hardware or software anomalies such as frequency and time steps.

Table 2.6. Three types of timing techniques.

Type	*Description*
(1) Relies on fixed time servers to synchronize the network	-The nodes are synchronized to time servers that are readily available. These time servers are expected to be robust and highly precise.
(2) Translates time throughout the network	-The time is translated hop-by-hop from the source to the sink. In essence, it is a time translation service.
(3) Self-organizes to synchronize the network	-The protocol does not depend on specialized time servers. It automatically organizes and determines the master nodes as the temporary time-servers.

There are three types of timing techniques as shown in Table 2.6, and each of these types has to address the challenges mentioned above. In addition, the timing techniques have to be energy aware since the batteries of the sensor nodes are limited. Also, they have to address the mapping between the sensor network time and the Internet time, e.g., universal coordinated time. In the following, examples of these types of timing techniques are described, namely the *Network Time Protocol* (NTP) [28], the *Reference-Broadcast Synchronization* (RBS) [9], and the *Time-Diffusion Synchronization Protocol* (TDP) [46].

In Internet, the NTP is used to discipline the frequency of each node's oscillator. It may be useful to use NTP to disciple the oscillators of the sensor nodes, but the connection to the time servers may not be possible because of frequent sensor node failures. In addition, disciplining all the sensor nodes in

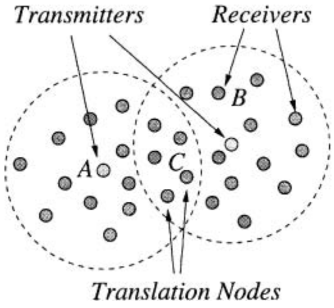

Figure 2.6. Illustration of the RBS.

the sensor field may be a problem due to interference from the environment and large variation of delay between different parts of the sensor field. The interference can temporarily disjoint the sensor field into multiple smaller fields causing undisciplined clocks among these smaller fields. The NTP protocol may be considered as type (1) of the timing techniques. In addition, it has to be refined to address the timing challenges in the wireless sensor networks.

As for type (2) of the timing techniques, the RBS provides an instantaneous time synchronization among a set of receivers that are within the reference broadcast of the transmitter. The transmitter broadcasts m reference packets. Each of the receivers that are within the broadcast range records the time-of-arrival of the reference packets. Afterwards, the receivers communicate with each other to determine the offsets. To provide multi-hop synchronization, it is proposed to use nodes that are receiving two or more reference broadcasts from different transmitters as translation nodes. These translation nodes are used to translate the time between different broadcast domains. As shown in Figure 2.6, nodes A, B, and C are the transmitter, receiver, and translation nodes, respectively.

Another emerging timing technique is the TDP. The TDP is used to maintain the time throughout the network within a certain tolerance. The tolerance level can be adjusted based on the purpose of the sensor networks. The TDP automatically self-configures by electing master nodes to synchronize the sensor network. In addition, the election process is sensitive to energy requirement as well as the quality of the clocks. The sensor network may be deployed in unattended areas, and the TDP still synchronizes the unattended network to a common time. It is considered as a type (3) of the timing techniques.

In summary, these timing techniques may be used for different types of applications as discussed in Section 2.1; each of these types has its benefits. A time-sensitive application has to choose not only the type of timing techniques but also the type of transport, network, datalink, and physical schemes as described in Sections 2.2, 2.3, 2.4, and 2.5, respectively. This is because different protocols provide different features and services to the time-sensitive application.

2.7 CONCLUSION

The design-principles of developing application, transport, network, datalink, and physical schemes as well as timing techniques are described. They are to guide and encourage new developments in the wireless sensor network areas. As the technologies for the wireless sensor networks advanced, the pervasive daily usage of the wireless sensor networks is foreseeable in the near future.

ACKNOWLEDGMENTS

The authors wish to thank Dr. Ian F. Akyildiz for his encouragement and support.

REFERENCES

[1] Agre, J., and Clare, L., "An Integrated Architecture for Cooperative Sensing Networks," *IEEE Computer Magazine*, pp.106-108, May 2000.

[2] Balakrishnan, H., Padmanabhan, V. N., Seshan, S., and Katz, R. H., "A Comparison of Mechanisms for Improving TCP Performance over Wireless Links", *IEEE/ACM Trans. Networking*, vol. 5, no. 6, pp. 756-769, December 1997.

[3] Bhardwaj, M., Garnett, T., and Chandrakasan, A. P., "Upper Bounds on the Lifetime of Sensor Networks," *IEEE International Conference on Communications '01*, Helsinki, Finland, June 2001.

[4] Bonnet, P., Gehrke J., and Seshadri, P., "Querying the Physical World," *IEEE Personal Communications*, pp. 10-15, October 2000.

[5] Bulusu, N., Estrin, D., Girod, L., and Heidemann, J., "Scalable Coordination for Wireless Sensor Networks: Self-Configuring Localization Systems," *International Symposium on Communication Theory and Applications (ISCTA 2001)*, Ambleside, UK, July 2001.

[6] Chien, C., Elgorriaga, I., and McConaghy, C., "Low-Power Direct-Sequence Spread-Spectrum Modem Architecture For Distributed Wireless Sensor Networks," *in ISLPED '01*, Huntington Beach, California, USA, August 2001.

[7] Cramer, R.J., Win, M. Z., and Scholtz, R. A., "Impulse radio multipath characteristics and diversity reception," *IEEE International Conference on Communications '98*, vol. 3, pp. 1650-1654, 1998.

[8] Elson, J., and Estrin, D., "Random, Ephemeral Transaction Identifiers in Dynamic Sensor Networks," *Proceedings 21st International Conference on Distributed Computing Systems*, pp. 459-468, Phoenix, Arizona, USA, April 2001.

[9] Elson, J., Girod, L., and Estrin, D., "Fine-Grained Network Time Synchronization using Reference Broadcasts," *in Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002)*, Boston, MA, USA, December 2002.

[10] Estrin, D., Girod, L., Pottie, G., and Srivastava, M., "Instrumenting the World With Wireless Sensor Networks," *International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001)*, Salt Lake City, Utah, USA, May 2001.

[11] Estrin, D., Govindan, R., Heidemann, J., and Kumar, S., "Next Century Challenges: Scalable Coordination in Sensor Networks," *ACM Mobicom'99,* pp.263-270, Seattle, Washingtion, USA, August 1999.

[12] Estrin, D., Govindan R., and Heidemann J., "Embedding the Internet," *Commun. ACM,* vol. 43, pp. 38-41, May 2000.

[13] Favre, P. and et al., "A 2V, 600μA, 1 GHz BiCMOS Super Regenerative Receiver for ISM Applications," *IEEE J. Solid-State Circuits,* vol. 33, pp.2186-2196, December 1998.

[14] Floyd, S., Jacobson, V., Liu, C., Macanne, S., and Zhang, L., "A Reliable Multicast Framework for Lightweight Sessions and Application Level Framing," *IEEE/ACM Trans. Networking,* vol. 5, no. 6, pp.784-803, December 1997.

[15] Hedetniemi, S., Hedetniemi, S., and Liestman, A., "A Survey of Gossiping and Broadcasting in Communication Networks," *Networks*, vol. 18, no. 4, pp. 319-349, 1988.

[16] Heinzelman, W. R., Kulik, J., and Balakrishnan, H., "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," *ACM Mobicom'99,* pp. 174-185, Seattle, Washington, USA, August 1999.

[17] Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *IEEE Proceedings of the Hawaii International Conference on System Sciences,* pp. 1-10, Maui, Hawaii, USA, January 2000.

[18] Intanagonwiwat, C., Govindan, R., and Estrin, D., "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *ACM Mobicom'00,* pp. 56-67, Boston, MA, USA, August 2000.

[19] Tilak, S., Abu-Ghazaleh, N. B., and Heinzelman, W., "Infrastructure Tradeoffs for Sensor Networks," *In Proc. WSNA 2002,* Atlanta, GA, USA, September 2002.

[20] Jaikaeo, C., Srisathapornphat, C., and Shen, C., "Diagnosis of Sensor Networks," *IEEE International Conference on Communications '01,* Helsinki, Finland, June 2001.

[21] Kahn, J. M., Katz, R. H., and Pister, K. S. J., "Next Century Challenges: Mobile Networking for Smart Dust," *ACM Mobicom'99,* pp.271-278, Seattle, Washington, USA, August 1999.

[22] Lee, H., Han, B., Shin, Y., and Im, S., "Multipath characteristics of impulse radio channels," *Vehicular Technology Conference Proceedings 2000,* vol. 3, pp. 2487-2491, Tokyo, Japan, May 2000.

[23] Levine, J., "Time Synchronization Over the Internet Using an Adaptive Frequency-Locked Loop," *IEEE Transaction on Ultrasonics, Ferroelectrics, and Frequency Control,* vol. 46, no. 4, pp. 888-896, July 1999.

[24] Li, L., and Halpern, J. Y., "Minimum-Energy Mobile Wireless Networks Revisited," *IEEE International Conference on Communications ICC'01,* Helsinki, Finland, June 2001.

[25] J. Le Martret, C. and Giannakis, G. B., "All-Digital Impulse radio for MUI/ISI-resilient multiuser communications over frequency-selective multipath channels," *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, vol. 2, pp. 655 -659, Los Angeles, CA, USA, October 2000.

[26] Melly, T., Porret, A., Enz, C. C., and Vittoz, E. A., "A 1.2 V, 430 MHz, 4dBm Power Amplifier and a 250 μW Front-End, using a Standard Digital CMOS Process" *IEEE International Symposium on Low Power Electronics and Design Conf.,* pp.233-237, San Diego, CA, USA, August 1999.

[27] MICA Motes and Sensors, `http://www.xbow.com`.

[28] Mills, D. L. (1994). "Internet Time Synchronization: The Network Time Protocol," *In Z. Yang and T. A. Marsland, editors, Global States and Time in Distributed Systems.* IEEE Computer Society Press.

[29] Mills, D. L., "Adaptive Hybrid Clock Discipline Algorithm for the Network Time Protocol," *IEEE/ACM Trans. on Networking,* vol. 6, no. 5, pp. 505-514, October 1998.

[30} Mireles, F. R. and Scholtz, R. A., "Performance of equicorrelated ultra-wideband pulse-position-modulated signals in the indoor wireless impulse radio channel," *IEEE Conference on Communications, Computers and Signal Processing '97,* vol. 2, pp 640-644, Victoria, BC, Canada, August 1997.

[31] Mirkovic, J., Venkataramani, G. P., Lu, S., and Zhang, L., "A Self-Organizing Approach to Data Forwarding in Large-Scale Sensor Networks," *IEEE International Conference on Communications ICC'01,* Helsinki, Finland, June 2001.

[32] Perkins, C. (2000). *Ad Hoc Networks.* Addison-Wesley.

[33] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks," *Proc. of ACM MobiCom'01,* pp. 189-199, Rome, Italy, July 2001.

[34] Porret, A., Melly, T., Enz, C. C., and Vittoz, E. A., "A Low-Power Low-Voltage Transceiver Architecture Suitable for Wireless Distributed Sensors Network," *IEEE International Symposium on Circuits and Systems '00,* vol. 1, pp.56-59, Geneva, Switzerland, May 2000.

[35] Pottie, G.J. and Kaiser, W.J., "Wireless Integrated Network Sensors," *Communications of the ACM,* vol. 43, no. 5, pp. 551-8, May 2000.

[36] Wan, C. Y., Campbell, A. T., and Krishnamurthy, L., "PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks," *In Proc. WSNA 2002,* Atlanta, GA, USA, September 2002.

[37] Rabaey, J., Ammer, J., L. da Silva Jr., J., and Patel, D., "PicoRadio: Ad-hoc Wireless Networking of Ubiquitous Low-Energy Sensor/Monitor Nodes," *Proceedings of the IEEE Computer Society Annual Workshop on VLSI (WVLSI'00),* pp. 9-12, Orlanda, Florida, USA, April 2000.

[38] Rabaey, J. M., Ammer, M. J., L. da Silva Jr., J., Patel, D., and Roundy, S., "PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking," *IEEE Computer Magazine,* vol. 33, pp. 42-48, July 2000.

[39] Sankarasubramaniam, Y., Akan, O. B., and Akyildiz, I. F., "ESRT: Event-to-Sink Reliable Transport for Wireless Sensor Networks," in *Proc. ACM MOBIHOC 2003,* pp. 177-188, Annapolis, Maryland, USA, June 2003.

[40] Savvides, A., Han, C., and Srivastava, M., "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," *Proc. of ACM MobiCom'01,* pp. 166-179, Rome, Italy, July 2001.

[41] Shen, C., Srisathapornphat, C., and Jaikaeo, C., "Sensor Information Networking Architecture and Applications," *IEEE Personal Communications,* pp. 52-59, August 2001.

[42] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A., and Chandrakasan, A., "Physical layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks," *ACM Mobicom'01,* pp. 272-286, Rome, Italy, July 2001.

[43] Slijepcevic, S. and Potkonjak, M., "Power Efficient Organization of Wireless Sensor Networks," *IEEE International Conference on Communications '01,* Helsinki, Finland, June 2001.

[44] Sohrabi, K., Manriquez, B., and Pottie, G. J., "Near-ground Wideband Channel Measurements in 800-1000 MHz," *IEEE Proc.of 49th Vehicular Technology Conference,* Houston, TX, USA, May 1999.

[45] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., "Protocols for Self-Organization of a Wireless Sensor Network," *IEEE Personal Communications,* pp. 16-27, October 2000.

[46] Su, W. and Akyildiz, I. F., "Time-Diffusion Synchronization Protocol for Sensor Networks," *Georgia Tech Technical Report,* 2003.

[47] Warneke, B., Liebowitz, B., and Pister, K. S. J., "Smart Dust: Communicating with a Cubic-Millimeter Computer," *IEEE Computer Magazine,* pp. 2-9, January 2001.

[48] Wicker, S. (1995). *Error Control Coding for Digital Communication and Storage.* Prentice-Hall.

[49] Woo, A. and Culler, D., "A Transmission Control Scheme for Media Access in Sensor Networks," *ACM Mobicom'01,* pp.221-235, Rome, Italy, July 2001.