CHAPTER-3

WIRELESS SENSOR NETWORKS

The concept of wireless sensor networks is based on a simple equation:

Sensing + CPU + Radio = Thousands of potential applications

As soon as people understand the capabilities of a wireless sensor network, hundreds of applications spring to mind. It seems like a straightforward combination of modern technology.

However, actually combining sensors, radios, and CPU’s into an effective wireless sensor network requires a detailed understanding of the both capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption. A core challenge is to map the overall system requirements down to individual device capabilities, requirements and actions. To make the wireless sensor network vision a reality, architecture must be developed that synthesizes the envisioned applications out of the underlying hardware capabilities.

To develop this system architecture we work from the high level application requirements down through the low-level hardware
requirements. In this process we first attempt to understand the set of target applications. To limit the number of applications that we must consider, we focus on a set of application classes that we believe are representative of a large fraction of the potential usage scenarios. We use this set of application classes to explore the system-level requirements that are placed on the overall architecture. From these system-level requirements we can then drill down into the individual node-level requirements. Additionally, we must provide a detailed background into the capabilities of modern hardware.

After we present the raw hardware capabilities, we present a basic wireless sensor node. The Rene node represents a first cut at system architecture, and is used for comparison against the system architectures presented in later chapters.

3.1. HISTORY OF WIRELESS SENSOR NETWORKS

Wireless Sensor Networks consists of individual nodes that are able to interact with their environment by sensing or controlling physical parameter; these nodes have to collaborate in order to fulfill their tasks as usually, a single node is incapable of doing so; and they use wireless communication to enable this collaboration. The definition of WSN, according to, Smart Dust program of DARPA is: “A sensor network is a deployment of massive numbers of small, inexpensive, self powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local
information to make global decisions about a physical environment” [96].

3.1.1. Evolution of Sensor Network

Sensor network development was initiated by the United States during the Cold War [96]. A network of acoustic sensors was placed at strategic locations on the bottom of the ocean to detect and track Soviet submarines. This system of acoustic sensors was called the Sound Surveillance System (SOSUS). Human operators played an important role in these systems. The sensor network was wired network that did not have the energy bandwidth constraints of wireless system.

Modern research on sensor networks started around 1980 with the Distributed Sensor Networks (DSN) program at the Defense Advanced Research Projects Agency (DARPA). These included acoustic sensors communication (a high-level protocols that link processes working on a common application in a resource-sharing network), processing techniques, algorithms (including self-location algorithms for sensors), and distributed software (dynamically modifiable distributed systems and language design).

Recent advances in computing and communication have caused a significant shift in sensor network research and brought it closer to achieving the original vision. Small and inexpensive sensors based upon micro-electro-mechanical system (MEMS) Routing in Wireless Sensor Networks technology, wireless networking, and inexpensive
low-power processors allow the deployment of wireless ad hoc networks for various applications. Thus, the program developed with new networking techniques is suitable for highly dynamic ad hoc environments.

**Table 3.1: Evaluation of Sensor Node**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manufacturer</strong></td>
<td>Custom contractors</td>
<td>Commercial, Crossbow Technology Inc., Sensoria Corp., Ember Corp.</td>
<td>Dust Inc. and others</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>Large shoe box and up</td>
<td>Pack of cards to small shoe box</td>
<td>Dust particles</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>Kilograms</td>
<td>Grams</td>
<td>Negligible</td>
</tr>
<tr>
<td><strong>Node Architecture</strong></td>
<td>Separate sensing, processing and communication</td>
<td>Integrated sensing, processing and communication</td>
<td>Integrated sensing, processing and communication</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>Point-to-point, star</td>
<td>Client-server, peer-to-peer</td>
<td>Peer-to-peer</td>
</tr>
<tr>
<td><strong>Power Supply Lifetime</strong></td>
<td>Large batteries, hours days and longer</td>
<td>AA batteries, days to weeks weeks</td>
<td>Solar; months to years</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>Vehicle-placed on air-dropped single sensors</td>
<td>Hand-placed</td>
<td>Embedded, sprinkled, left behind</td>
</tr>
</tbody>
</table>

Wireless networks based upon IEEE 802.11 standards [20] can now provide bandwidth approaching those of wired networks. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer. The organization has defined the IEEE 802.15 standard [56] for personal area networks (PANs), with “personal networks” defined to have a radius of 5 to 10 m. Networks of short-range sensors are the ideal technology to be employed in PANs.
Furthermore, increases in chip capacity and processor production capabilities have reduced the energy per bit requirement for both computing and communication. Sensing, computing, and communications can now be performed on a single chip, further reducing the cost and allowing deployment in ever-larger numbers.

3.1.2. Wireless Sensor Network Model

Unlike their ancestor ad-hoc networks, WSNs are resource limited, they are deployed densely, they are prone to failures, the number of nodes in WSNs is several orders higher than that of ad hoc networks, WSN network topology is constantly changing, WSNs use broadcast communication mediums and finally sensor nodes don’t have a global identification tags [58]. The major components of a typical sensor network are:

- **Sensor Field**: A sensor field can be considered as the area in which the nodes are placed.

- **Sensor Nodes**: Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.

- **Sink**: A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. Sinks are also known as data aggregation points.
**Task Manager:** The task manager also known as base station is a centralized point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface. The base station is either a laptop or a workstation.

**Fig. 3.1: Components of Wireless Sensor Networks**

Data is streamed to these workstations either via the internet, wireless channels, satellite etc. So, hundreds to several thousand nodes are deployed throughout a sensor field to create a wireless multi-hop network. Nodes can use wireless communication media such as infrared, radio, optical media or Bluetooth for their communications. The transmission range of the nodes varies according to the communication protocol is used.
3.2. SENSOR NETWORK APPLICATION CLASSES

The three application classes we have selected are: environmental data collection, security monitoring, and sensor node tracking. We believe that the majority of wireless sensor network deployments will fall into one of these class templates.

3.2.1. Environmental Data Collection

A canonical environmental data collection application is one where a research scientist wants to collect several sensor readings from a set of points in an environment over a period of time in order to detect trends and interdependencies. This scientist would want to collect data from hundreds of points spread throughout the area and then analyze the data offline [27, 70]. The scientist would be interested in collecting data over several months or years in order to look for long-term and seasonal trends. For the data to be meaningful it would have to be collected at regular intervals and the nodes would remain at known locations.

At the network level, the environmental data collection application is characterized by having a large number of nodes continually sensing and transmitting data back to a set of base stations that store the data using traditional methods. These networks generally require very low data rates and extremely long lifetimes. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment. This distance between adjacent nodes will be minimal yet the distance across the entire network will be significant.
After deployment, the nodes must first discover the topology of the network and estimate optimal routing strategies [103]. The routing strategy can then be used to route data to a central collection points. In environmental monitoring applications, it is not essential that the nodes develop the optimal routing strategies on their own. Instead, it may be possible to calculate the optimal routing topology outside of the network and then communicate the necessary information to the nodes as required. This is possible because the physical topology of the network is relatively constant. While the time variant nature of RF communication may cause connectivity between two nodes to be intermittent, the overall topology of the network will be relatively stable. Environmental data collection applications typically use tree-based routing topologies where each routing tree is rooted at high-capability nodes that sink data. Data is periodically transmitted from child node to parent node up the tree-structure until it reaches the sink. With tree-based data collection each node is responsible for forwarding the data of all its descendants. Nodes with a large number of descendants transmit significantly more data than leaf nodes. These nodes can quickly become energy bottlenecks [105, 111]. Once the network is configured, each node periodically samples its sensors and transmits its data up the routing tree and back to the base station. For many scenarios, the interval between these transmissions can be on the order of minutes. Typical reporting periods are expected to be between 1 and 15 minutes; while it is possible for networks to have significantly higher reporting rates. The typical environment
parameters being monitored, such as temperature, light intensity, and humidity, does not change quickly enough to require higher reporting rates. In addition to large sample intervals, environmental monitoring applications do not have strict latency requirements. Data samples can be delayed inside the network for moderate periods of time without significantly affecting application performance. In general the data is collected for future analysis, not for real-time operation. In order to meet lifetime requirements, each communication event must be precisely scheduled. The sensor nodes will remain dormant a majority of the time; they will only wake to transmit or receive data. If the precise schedule is not met, the communication events will fail.

As the network ages, it is expected that nodes will fail over time. Periodically the network will have to reconfigure to handle node/link failure or to redistribute network load. Additionally, as the researchers learn more about the environment they study, they may want to go in and insert additional sensing points. In both cases, the reconfigurations are relatively infrequent and will not represent a significant amount of the overall system energy usage.

The most important characteristics of the environmental monitoring requirements are long lifetime, precise synchronization, low data rates and relatively static topologies. Additionally it is not essential that the data be transmitted in real-time back to the central collection point. The data transmissions can be delayed inside the network as necessary in order to improve network efficiency.
3.2.2. Security Monitoring

Our second class of sensor network application is security monitoring. Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement. These are “report by exception” networks.

Additionally, it is essential that it is confirmed that each node is still present and functioning. If a node were to be disabled or fail, it would represent a security violation that should be reported. For security monitoring applications, the network must be configured so that nodes are responsible for confirming the status of each other. One approach is to have each node be assigned to a peer that will report if a node is not functioning. The optimal topology of a security monitoring network will look quite different from that of a data collection network.

In a collection tree, each node must transmit the data of all of its decedents. Because of this, it is optimal to have a short, wide tree.
In contrast, with a security network the optimal configuration would be to have a linear topology that forms a Hamiltonian cycle of the network. The power consumption of each node is only proportional to the number of children it has. In a linear network, each node would have only one child. This would evenly distribute the energy consumption of the network.

The accepted norm for security systems today is that each sensor should be checked approximately once per hour. Combined with the ability to evenly distribute the load of checking nodes, the energy cost of performing this check becomes minimal. A majority of the energy consumption in a security network is spent on meeting the strict latency requirements associated with the signaling the alarm when a security violation occurs. Once detected, a security violation must be communicated to the base station immediately. The latency of the data communication across the network to the base station has a critical impact on application performance. Users demand that alarm situations be reported within seconds of detection. This means that network nodes must be able to respond quickly to requests from their neighbors to forward data. In security networks reducing the latency of an alarm transmission is significantly more important than reducing the energy cost of the transmissions.

This is because alarm events are expected to be rare. In a fire security system alarms would almost never be signaled. In the event that one does occur a significant amount of energy could be dedicated
to the transmission. Reducing the transmission latency leads to higher energy consumption because routing nodes must monitor the radio channel more frequently.

In security networks, a vast majority of the energy will be spent on confirming the functionality of neighboring nodes and in being prepared to instantly forward alarm announcements. Actual data transmission will consume a small fraction of the network energy.

3.2.3. Node Tracking Scenarios

A third usage scenario commonly discussed for sensor networks is the tracking of a tagged object through a region of space monitored by a sensor network. There are many situations where one would like to track the location of valuable assets or personnel. Current inventory control systems attempt to track objects by recording the last checkpoint that an object passed through. However, with these systems it is not possible to determine the current location of an object. For example, UPS tracks every shipment by scanning it with a barcode whenever it passes through a routing center. The system breaks down when objects do not flow from checkpoint to checkpoint. In typical work environments it is impractical to expect objects to be continually passed through checkpoints.

With wireless sensor networks, objects can be tracked by simply tagging them with a small sensor node. The sensor node will be tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. Instead of sensing
environmental data, these nodes will be deployed to sense the RF messages of the nodes attached to various objects. The nodes can be used as active tags that announce the presence of a device. A database can be used to record the location of tracked objects relative to the set of nodes at known locations. With this system, it becomes possible to ask where an object is currently, not simply where it was last scanned [102].

Unlike sensing or security networks, node tracking applications will continually have topology changes as nodes move through the network. While the connectivity between the nodes at fixed locations will remain relatively stable, the connectivity to mobile nodes will be continually changing. Additionally the set of nodes being tracked will continually change as objects enter and leave the system. It is essential that the network be able to efficiently detect the presence of new nodes that enter the network.

### 3.2.4. Hybrid Networks

In general, complete application scenarios contain aspects of all three categories. For example, in a network designed to track vehicles that pass through it, the network may switch between being an alarm monitoring network and a data collection network.

During the long periods of inactivity when no vehicles are present, the network will simply perform an alarm monitoring function. Each node will monitor its sensors waiting to detect a vehicle. Once an alarm event is detected, all or part of the network,
will switch into a data collection network and periodically report sensor readings up to a base station that track the vehicles progress. Because of this multi-modal network behavior, it is important to develop a single architecture that and handle all three of these application scenarios.

### 3.3. SYSTEM EVALUATION METRICS

Now that we have established the set of application scenarios that we are addressing, we explore the evaluation metrics that will be used to evaluate a wireless sensor network. To do this we keep in mind the high-level objectives of the network deployment, the intended usage of the network, and the key advantages of wireless sensor networks over existing technologies. The key evaluation metrics for wireless sensor networks are lifetime, coverage, cost and ease of deployment, response time, temporal accuracy, security, and effective sample rate. Their importance is discussed below.

One result is that many of these evaluation metrics are interrelated. Often it may be necessary to decrease performance in one metric, such as sample rate, in order to increase another, such as lifetime. Taken together, this set of metrics form a multidimensional space that can be used to describe the capabilities of a wireless sensor network. The capabilities of a platform are represented by a volume in this multidimensional space that contains all of the valid operating points. In turn, a specific application deployment is represented by a single point. A system platform can successfully perform the
application if and only if the application requirements point lies inside the capability hyperspace.

3.3.1. Lifetime

Critical to any wireless sensor network deployment is the expected lifetime. The goal of both the environmental monitoring and security application scenarios is to have nodes placed out in the field, unattended, for months or years.

The primary limiting factor for the lifetime of a sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize total network lifetime. In many deployments it is not the average node lifetime that is important, but rather the minimum node lifetime. In the case of wireless security systems, every node must last for multiple years. A single node failure would create vulnerability in the security systems.

In some situations it may be possible to exploit external power, perhaps by tapping into building power with some or all nodes. However, one of the major benefits to wireless systems is the ease of installation. Requiring power to be supplied externally to all nodes largely negates this advantage. A compromise is to have a handful of special nodes that are wired into the building’s power infrastructure.

In most application scenarios, a majority of the nodes will have to be self powered. They will either have to contain enough stored energy to last for years, or they will have to be able to scavenge energy
from the environment through devices, such as solar cells or piezoelectric generators [20, 56]. Both of these options demand that that the average energy consumption of the nodes be as low as possible.

The most significant factor in determining lifetime of a given energy supply is radio power consumption. In a wireless sensor node the radio consumes a vast majority of the system energy. This power consumption can be reduced through decreasing the transmission output power or through decreasing the radio duty cycle. Both of these alternatives involve sacrificing other system metrics.

3.3.2. Coverage

Next to lifetime, coverage is the primary evaluation metric for a wireless network. It is always advantageous to have the ability to deploy a network over a larger physical area. This can significantly increase a system’s value to the end user. It is important to keep in mind that the coverage of the network is not equal to the range of the wireless communication links being used. Multi-hop communication techniques can extend the coverage of the network well beyond the range of the radio technology alone. In theory they have the ability to extend network range indefinitely. However, for a given transmission range, multi-hop networking protocols increase the power consumption of the nodes, which may decrease the network lifetime. Additionally, they require a minimal node density, which may increase the deployment cost.
Tied to range is a network’s ability to scale to a large number of nodes. Scalability is a key component of the wireless sensor network value proposition. A user can deploy a small trial network at first and then can continually add sense points to collect more and different information. A user must be confident that the network technology being used is capable of scaling to meet his eventual need. Increasing the number of nodes in the system will impact either the lifetime or effective sample rate. More sensing points will cause more data to be transmitted which will increase the power consumption of the network. This can be offset by sampling less often.

### 3.3.3. Cost and Ease of Deployment

A key advantage of wireless sensor networks is their ease of deployment. Biologists and construction workers installing networks cannot be expected to understand the underlying networking and communication mechanisms at work inside the wireless network. For system deployments to be successful, the wireless sensor network must configure itself. It must be possible for nodes to be placed throughout the environment by an untrained person and have the system simply work.

Ideally, the system would automatically configure itself for any possible physical node placement. However, real systems must place constraints on actual node placements – it is not possible to have nodes with infinite range. The wireless sensor network must be capable of providing feedback as to when these constraints are
violated. The network should be able to assess quality of the network deployment and indicate any potential problems. This translates to requiring that each device be capable of performing link discovery and determining link quality.

In addition to an initial configuration phase, the system must also adapt to changing environmental conditions. Throughout the lifetime of a deployment, nodes may be relocated or large physical objects may be placed so that they interfere with the communication between two nodes. The network should be able to automatically reconfigure on demand in order to tolerate these occurrences.

The initial deployment and configuration is only the first step in the network lifecycle. In the long term, the total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost. The security application scenario in particular requires that the system be extremely robust. In addition to extensive hardware and software testing prior to deployment, the sensor system must be constructed so that it is capable of performing continual self-maintenance. When necessary, it should also be able to generate requests when external maintenance is required.

In a real deployment, a fraction of the total energy budget must be dedicated to system maintenance and verification. The generation of diagnostic and reconfiguration traffic reduces the network lifetime. It can also decrease the effective sample rate.
3.3.4. Response Time

Particularly in our alarm application scenario, system response time is a critical performance metric. An alarm must be signaled immediately when an intrusion is detected. Despite low power operation, nodes must be capable of having immediate, high-priority messages communicated across the network as quickly as possible. While these events will be infrequent, they may occur at any time without notice. Response time is also critical when environmental monitoring is used to control factory machines and equipment. Many users envision wireless sensor networks as useful tools for industrial process control. These systems would only be practical if response time guarantees could be met.

The ability to have low response time conflicts with many of the techniques used to increase network lifetime. Network lifetime can be increased by having nodes only operate their radios for brief periods of time. If a node only turns on its radio once per minute to transmit and receive data, it would be impossible to meet the application requirements for response time of a security system. Response time can be improved by including nodes that are powered all the time. These nodes can listen for the alarm messages and forward them down a routing backbone when necessary. This, however, reduces the ease of deployment for the system.
3.3.5. Temporal Accuracy

In environmental and tracking applications, samples from multiple nodes must be cross-correlated in time in order to determine the nature of phenomenon being measured.

The necessary accuracy of this correlation mechanism will depend on the rate of propagation of the phenomenon being measured. In the case of determining the average temperature of a building, samples must only be correlated to within seconds. However, to determine how a building reacts to a seismic event, millisecond accuracy is required.

To achieve temporal accuracy, a network must be capable of constructing and maintaining a global time base that can be used to chronologically order samples and events. In a distributed system, energy must be expended to maintain this distributed clock. Time synchronization information must be continually communicated between nodes. The frequency of the synchronization messages is dependent on the desired accuracy of the time clock. The bottom line is maintenance of a distributed time base requires both power and bandwidth.

3.3.6. Security

Despite the seemingly harmless nature of simple temperature and light information from an environmental monitoring application, keeping this information secure can be extremely important.
Significant patterns of building use and activity can be easily extracted from a trace of temperature and light activity in an office building. In the wrong hands, this information can be exploited to plan a strategic or physical attack on a company. Wireless sensor networks must be capable of keeping the information they are collecting private from eavesdropping. As we consider security oriented applications, data security becomes even more significant. Not only must the system maintain privacy, it must also be able to authenticate data communication. It should not be possible to introduce a false alarm message or to replay an old alarm message as a current one. A combination of privacy and authentication is required to address the needs of all three scenarios. Additionally, it should not be possible to prevent proper operation by interfering with transmitted signals.

Use of encryption and cryptographic authentication costs both power and network bandwidth [76, 87]. Extra computation must be performed to encrypt and decrypt data and extra authentication bits must be transmitted with each packet. This impacts application performance by decreasing the number of samples than can be extracted from a given network and the expected network lifetime.

**3.3.7. Effective Sample Rate**

In a data collection network, effective sample rate is a primary application performance metric. We define the effective sample rate as the sample rate that sensor data can be taken at each individual
sensor and communicated to a collection point in a data collection network. Fortunately, environmental data collection applications typically only demand sampling rates of 1-2 samples per minute. However, in addition to the sample rate of a single sensor, we must also consider the impact of the multi-hop networking architectures on a node's ability to effectively relay the data of surrounding nodes.

In a data collection tree, a node must handle the data of all of its descendents. If each child transmits a single sensor reading and a node has a total of 60 descendents, then it will be forced to transmit 60 times as much data. Additionally, it must be capable of receiving those 60 readings in a single sample period. This multiplicative increase in data communication has a significant effect on system requirements. Network bit rates combined with maximum network size end up impacting the effective per-node sample rate of the complete system [35]. One mechanism for increasing the effective sample rate beyond the raw communication capabilities of the network is to exploit in-network processing. Various forms of spatial and temporal compression can be used to reduce the communication bandwidth required while maintaining the same effective sampling rate. Additionally local storage can be used to collect and store data at a high sample rate for short periods of time. In-network data processing can be used to determine when an “interesting” event has occurred and automatically trigger data storage. The data can then be downloaded over the multi-hop network as bandwidth allows.
Triggering is the simplest form of in-network processing. It is commonly used in security systems. Effectively, each individual sensor is sampled continuously, processed, and only when a security breach has occurred is data transmitted to the base station. If there were no local computation, a continuous stream of redundant sensor readings would have to be transmitted. We show how this same process can be extended to complex detection events.

3.4. INDIVIDUAL NODE EVALUATION METRICS

Now that we have established the set of metrics that will be used to evaluate the performance of the sensor network as a whole, we can attempt to link the system performance metrics down to the individual node characteristics that support them. The end goal is to understand how changes to the low-level system architecture impact application performance. Just as application metrics are often interrelated, we will see that an improvement in one node-level evaluation metric (e.g., range) often comes at the expense of another (e.g., power).

3.4.1. Power

To meet the multi-year application requirements individual sensor nodes must be incredibly low-power. Unlike cell phones, with average power consumption measured in hundreds of milliamps and multi-day lifetimes, the average power consumption of wireless sensor network nodes must be measured in micro amps. This ultra-low-
power operation can only be achieved by combining both low-power hardware components and low duty-cycle operation techniques.

During active operation, radio communication will constitute a significant fraction of the node’s total energy budget. Algorithms and protocols must be developed to reduce radio activity whenever possible. This can be achieved by using localized computation to reduce the streams of data being generated by sensors and through application specific protocols. For example, events from multiple sensor nodes can be combined together by a local group of nodes before transmitting a single result across the sensor network.

Our discussion on available energy sources will show that a node must consume less that 200 uA on average to last for one year on a pair of AA batteries. In contrast the average power consumption of a cell phone is typically more than 4000 uA, a 20 fold difference.

3.4.2. Flexibility

The wide range of usage scenarios being considered means that the node architecture must be flexible and adaptive. Each application scenario will demand a slightly different mix of lifetime, sample rate, response time and in-network processing.

Wireless sensor network architecture must be flexible enough to accommodate a wide range of application behaviors. Additionally, for cost reasons each device will have only the hardware and software it actually needs for a given the application. The architecture must make
it easy to assemble just the right set of software and hardware components.

Thus, these devices require an unusual degree of hardware and software modularity while simultaneously maintaining efficiency.

3.4.3. Robustness

In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible. In a typical deployment, hundreds of nodes will have to work in harmony for years. To achieve this, the system must be constructed so that it can tolerate and adapt to individual node failure. Additionally, each node must be designed to be as robust as possible.

System modularity is a powerful tool that can be used to develop a robust system. By dividing system functionality into isolated sub-pieces, each function can be fully tested in isolation prior to combining them into a complete application. To facilitate this, system components should be as independent as possible and have interfaces that are narrow, in order to prevent unexpected interactions.

In addition to increasing the system’s robustness to node failure, a wireless sensor network must also be robust to external interference. As these networks will often coexist with other wireless systems, they need the ability to adapt their behavior accordingly. The robustness of wireless links to external interference can be greatly increased through the use of multi-channel and spread spectrum
radios. It is common for facilities to have existing wireless devices that operate on one or more frequencies. The ability to avoid congested frequencies is essential in order to guarantee a successful deployment.

3.4.4. Security

In order to meet the application level security requirements, the individual nodes must be capable of performing complex encrypting and authentication algorithms.

Wireless data communication is easily susceptible to interception. The only way to keep data carried by these networks private and authentic is to encrypt all data transmissions. The CPU must be capable of performing the required cryptographic operations itself or with the help of included cryptographic accelerators [76].

In addition to securing all data transmission, the nodes themselves must secure the data that they contain. While they will not have large amounts of application data stored internally, they will have to store secret encryption keys used in the network. If these keys are revealed, the security of the network could crumble. To provide true security, it must be difficult to extract the encryption keys of from any node.

3.4.5. Communication

A key evaluation metric for any wireless sensor network is its communication rate, power consumption, and range. While we have made the argument that the coverage of the network is not limited by
the transmission range of the individual nodes, the transmission range does have a significant impact on the minimal acceptable node density. If nodes are placed too far apart it may not be possible to create an interconnected network or one with enough redundancy to maintain a high level of reliability. Most application scenarios have natural node densities that correspond to the granularity of sensing that is desired. If the radio communications range demands a higher node density, additional nodes must be added to the system in to increase node density to a tolerable level.

The communication rate also has a significant impact on node performance. Higher communication rates translate into the ability to achieve higher effective sampling rates and lower network power consumption. As bit rates increase, transmissions take less time and therefore potentially require less energy. However, an increase in radio bit rate is often accompanied by an increase in radio power consumption. All things being equal, a higher transmission bit rate will result in higher system performance. However, we show later that an increase in the communication bit rate has a significant impact on the power consumption and computational requirement of the node. In total, the benefits of an increase in bit rate can be offset by several other factors.
3.4.6. Computation

The two most computationally intensive operations for a wireless sensor node are the in-network data processing and the management of the low-level wireless communication protocols. As we discuss later, there are strict real-time requirements associated with both communication and sensing. As data is arriving over the network, the CPU must simultaneously control the radio and record/decode the incoming data.

Higher communication rates required faster computation. The same is true for processing being performed on sensor data. Analog sensors can generate thousands of samples per second. Common sensor processing operations include digital filtering, averaging, threshold detection, correlation and spectral analysis. It may even be necessary to perform a real-time FFT on incoming data in order to detect a high-level event. In addition to being able to locally process, refine and discard sensor readings, it can be beneficial to combine data with neighboring sensors before transmission across a network. Just as complex sensor waveforms can be reduced to key events, the results from multiple nodes can be synthesized together. This in-network processing requires additional computational resources.

In our experience, 2-4 MIPS of processing are required to implement the radio communication protocols used in wireless sensor networks. Beyond that, the application data processing can consume
an arbitrary amount of computation depending on the calculations being performed.

3.4.7. Time Synchronization

In order to support time correlated sensor readings and low-duty cycle operation of our data collection application scenario, nodes must be able to maintain precise time synchronization with other members of the network. Nodes need to sleep and awake together so that they can periodically communicate. Errors in the timing mechanism will create inefficiencies that result in increased duty cycles. In distributed systems, clocks drift apart over time due to inaccuracies in timekeeping mechanisms. Depending on temperature, voltage, humidity, time keeping oscillators operate at slightly different frequencies. High-precision synchronization mechanisms must be provided to continually compensate for these inaccuracies.

3.4.8. Size & Cost

The physical size and cost of each individual sensor node has a significant and direct impact on the ease and cost of deployment. Total cost of ownership and initial deployment cost are two key factors that will drive the adoption of wireless sensor network technologies. In data collection networks, researchers will often be operating off of a fixed budget. Their primary goal will be to collect data from as many locations as possible without exceeding their fixed budget. A reduction in per-node cost will result in the ability to purchase more nodes, deploy a collection network with higher density, and collect more data.
Physical size also impacts the ease of network deployment. Smaller nodes can be placed in more locations and used in more scenarios. In the node tracking scenario, smaller, lower cost nodes will result in the ability to track more objects.