International Journal of Computer Science and Software Engineering (IJCSSE), Volume 4, Issue 11, November 2015
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 303-307

Standard Issues and Challenges in Wireless Sensor Networks

Jazeb Sayyed

ME Computer Engineering, Dr.D.Y.Patil College of Engineering, Ambi,Talegaon-Dabhade, India

jazebsayyed@gmail.com

ABSTRACT

Advances in the electrical and electronics communication technologies led to large scale development and research in area of Wireless Sensor Network. Wireless Sensor network have numerous applications in recent scenarios. WSN have a large number of constrained attached to them such as less processing capability, low memory, limited energy resources and security issues. WSN generally deployed in natural environment hence a large number of security issues are there. Here we look at the basic Sensor network application classes and hybrid network of wireless sensor network.

Keywords: *WSN, Electronics Communication, Hybrid Network, Issues and Challenges.*

1. INTRODUCTION

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path by hopping data from node to node in search of its destination. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities. The power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real-time tracking, to monitoring of environmental conditions, to ubiquitous computing environments, to in situ monitoring of the health of structures or equipment. While often referred to as wireless sensor networks, they can also control actuators that extend control from cyberspace into the physical world. The most straightforward application of wireless sensor network technology is to monitor remote environments for low frequency data trends. For example, a chemical plant could be easily monitored for leaks by hundreds of sensors that automatically form a wireless interconnection network and immediately report the detection of any chemical leaks. Unlike traditional wired systems, deployment costs would be minimal. Instead of having to deploy thousands of feet of wire routed through protective conduit, installers simply have to place quarter-sized device, such as the one pictured in Figure 1-1, at eachsensing point.

Current wireless systems only scratch the surface of possibilities emerging from the integration of low-power communication, sensing, energy storage, and computation.

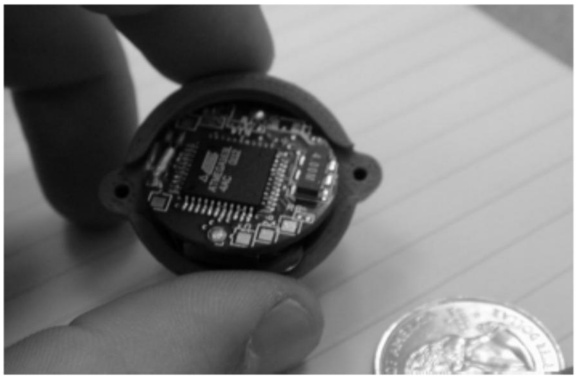

Fig. 1.1. DOT – Wireless sensor network device designed to be the approximate size of a quarter.

Future devices will continue to be smaller, cheaper and longer lasting.

Generally, when people consider wireless devices they think of items such as cell phones, personal digital assistants, or laptops with 802.11. These items costs hundreds of dollars, target specialized applications, and rely on the pre-deployment of extensive infrastructure support. In contrast, wireless sensor networks use small, low-cost embedded devices for a wide range of applications and do not rely on any pre-existing infrastructure. The vision is that these devise will cost less that $1 by 2005. Unlike traditional wireless devices, wireless sensor nodes do not need to communicate directly with the nearest high-power control tower or base station, but only with their local peers. Instead, of relying on a pre-deployed infrastructure, each individual sensor or actuator becomes part of the overall infrastructure. Peer-to-peer networking protocols provide a mesh-like interconnect to shuttle data between the thousands of tiny embedded devices in a multi-hop fashion.

An example network is shown in Figure 1-2. It depicts a precision agriculture deployment—an active area of application research. Hundreds of nodes scattered throughout a field assemble together, establish a routing topology, and transmit data back to a collection point. The application demands for robust, scalable, low-cost and easy to deploy networks are perfectly met by a wireless sensor network. If one of the nodes should fail, a new topology would be selected and the overall network would continue to deliver data. If more nodes are placed in the field, they only create more potential routing opportunities. There is extensive research in the development of new algorithms for data aggregation [1], ad hoc routing [2-4], and distributed signal processing in the context of wireless sensor networks [5, 6]. As the algorithms and protocols for wireless sensor network are developed, they must be supported by a low-power, efficient and flexible hardware platform. This thesis focuses on developing the system architecture required to meet the needs of wireless sensor networks. A core design challenge in wireless sensor networks is coping with the harsh resource constraints placed on the individual devices.

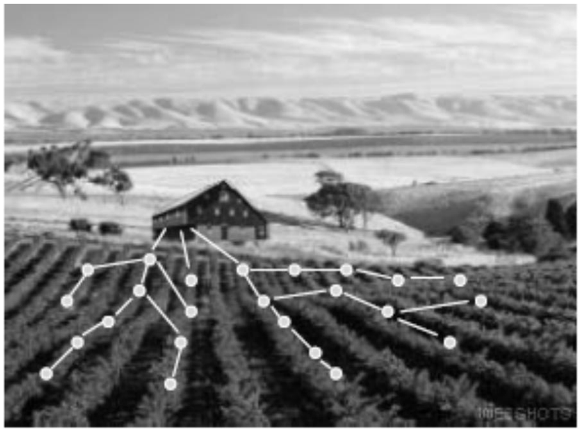

Fig. 1.2. Possible deployment of ad-hoc wireless embedded network for precision agriculture.

Sensors detect temperature, light levels and soil moisture at hundreds of points across a field and communicate their data over a multi-hop network for analysis.

Embedded processors with kilobytes of memory must implement complex, distributed, ad-hoc networking protocols. Many constraints derive from the vision that these devices will be produced in vast quantities and must be small and inexpensive. As Moore's law marches on, each device will get smaller, not just grow more powerful at a given size. Size reduction is essential in order to allow devices to be produced as inexpensively as possible, as well as to be able to allow devices to be used in a wide range of application scenarios. The most difficult resource constraint to meet is power consumption. As physical size decreases, so does energy capacity. Underlying energy constraints end up creating computational and storage limitations that lead to a new set of architectural issues. Many devices, such as cell phones and pagers, reduce their power consumption through the use specialized communication hardware in ASICs that provide low-power implementations of the necessary communication protocols and by relying on highpower infrastructure. However, the strength of wireless sensor networks is their flexibility and universality. The wide range of applications being targeted makes it difficult to develop a single protocol, and in turn, an ASIC, that is efficient for all applications. A wireless sensor network platform must provide support for a suite of application-specific protocols that drastically reduce node size, cost, and power consumption for their target application.

2. 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.

A. 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.

B. 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. 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 . 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.

C. 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 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.

D. 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.

E. 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.

F. 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.

G. 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 a vulnerability in the security systems.

H. 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.

I. 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[2].

J. 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.

4. CONCLUSION

Wireless sensor network have a large number of constrained attached to them such as less processing capability, low memory, limited energy resources and security issues. WSN generally deployed in natural environment hence a large number of security issues are there. Here we studied the concept of wireless sensor network and its Sensor network application classes which includes Environmental Data collection , Security Monitoring ,Node tracking scenarios, Hybrid networks, System Evaluation Metrics.

REFERENCES

[1] Madden, S., et al., TAG: A Tiny AGgregation Service for Ad-Hoc Sensor

[2] Networks. 2002: OSDI.

[3] 2. Culler, D.E and Hong, W., “Wireless Sensor Network”, Communication of the ACM, Vol.47, No. 6, June 2004, pp.30-33.

[4] Akyildiz, I. F., Su , W., Sankarasubramaniam, Y, and Cayirci, E., “Wireless Sensor Networks: A Survey”, Computer Networks, 38, 2002, pp. 393-422.