Research Challenges for Wireless Sensor Networks

John A. Stankovic
Department of Computer Science
University of Virginia

Abstract

Wireless sensor networks (WSN) are currently receiving significant attention due to their unlimited potential. However, it is still very early in the lifetime of such systems and many research challenges exist. In this brief article, I concentrate on six key research challenges for wireless sensor networks. I conclude with a brief mention of a number of other research challenges that must be met before WSN become pervasive.

Real-world Protocols:

Many current WSN solutions are developed with simplifying assumptions about wireless communication and the environment, even though the realities of wireless communication and environmental sensing are well known. Many of these solutions work very well in simulation. It is either unknown how the solutions work in the real world or they can be shown to work poorly in practice. We note that, in general, there is an excellent understanding of both the theoretical and practical issues related to wireless communication. For example, it is well known how the signal strength drops over distance. Effects of signal reflection, scattering and fading are understood. However, when building an actual WSN, many specific system, application, and cost issues also affect the communication properties of the system. Radio communication in the form of AM or FM broadcast from towers performs quite differently than short range, low power wireless found in self-organizing WSNs. Of course, while the same basic principles apply, the system performance characteristics vary considerably. In other words, the size, power, cost constraints and their tradeoffs are fundamental constraints. In the current state of the art, the tradeoff among these constraints has produced a number of devices currently being used in WSNs. For example, one such device is the Mica mote that uses 2 AA batteries, a 7 MHz microcontroller, an RF Chipcon radio, and costs about $100. As better batteries, radios, and microcontrollers become available and as costs reduce, new platforms will be developed. These new platforms will continue to have tradeoffs between these parameters.

Novel network protocols that account for the key realities in wireless communication are required. New research is needed to:

- Measure and assess how the theoretical properties of wireless communication are exhibited in today's and tomorrow's sensing and communication devices,
- Establish better models of communication realities to feed back into improved simulation tools,
- Invent new network protocols that account for the communication realities of real world environments,
- Test the individual solutions on real platforms in real world settings, and
- Synthesize novel solutions into a complete system-wide protocol stack for a real application.

Real-Time:

WSN deal with real world environments. In many cases, sensor data must be delivered within time constraints so that appropriate observations can be made or actions taken. Very few results exist to date regarding meeting real-time requirements in WSN. Most protocols either ignore real-time or simply attempt to process as fast as possible and hope that this speed is sufficient to meet deadlines. Some initial results exist for real-time routing. For example, the RAP protocol [1] proposes a new policy called velocity monotonic scheduling. Here a packet has a deadline and a distance to travel. Using these parameters a packet's average velocity requirement is computed and at each hop packets are scheduled for transmission based on the highest velocity requirement of any packets at this node. While this protocol addresses real-time, no guarantees are given. Another routing protocol that addresses real-time is called SPEED [2]. This protocol uses feedback control to guarantee that each node maintains an average

delay for packets transiting a node. Given this delay and the distance to travel (in hops), it can be determined if a packet meets its deadline (in steady state). However, transient behavior, message losses, congestion, noise and other problems cause these guarantees to be limited. To date, the limited results that have appeared for WSN regarding real-time issues has been in routing. Many other functions must also meet real-time constraints including: data fusion, data transmission, target and event detection and classification, query processing, and security. New results are needed to guarantee soft real-time requirements and that deal with the realities of WSN such as lost messages, noise and congestion. Using feedback control to address both steady state and transient behavior seems to hold promise. Dealing with real-time usually identifies the need for differentiated services, e.g., routing solutions need to support different classes of traffic; guarantees for the important traffic and less support for unimportant traffic. It is important not only to develop real-time protocols for WSN, but associated analysis techniques must also be developed (see the section below on *Analysis*).

Power Management (in the large):

Low-cost deployment is one acclaimed advantage of sensor networks. Limited processor bandwidth and small memory are two arguable constraints in sensor networks, which will disappear with the development of fabrication techniques. However, the energy constraint is unlikely to be solved soon due to slow progress in developing battery capacity. Moreover, the untended nature of sensor nodes and hazardous sensing environments preclude battery replacement as a feasible solution. On the other hand, the surveillance nature of many sensor network applications requires a long lifetime; therefore, it is a very important research issue to provide a form of energy-efficient surveillance service for a geographic area. Much of the current research focuses on how to provide full or partial sensing coverage in the context of energy conservation. In such an approach, nodes are put into a dormant state as long as their neighbors can provide sensing coverage for them. These solutions regard the sensing coverage to a certain geographic area as binary, either it provides coverage or not. However, we argue that, in most scenarios such as battlefields, there are certain geographic sections such as the general command center that are much more security-sensitive than others. Based on the fact that individual sensor nodes are not reliable and subject to failure and single sensing readings can be easily distorted by background noise and cause false alarms, it is simply not sufficient to rely on a single sensor to safeguard a critical area. In this case, it is desired to provide higher degree of coverage in which multiple sensors monitor the same location at the same time in order to obtain high confidence in detection. On the other hand, it is overkill and energy consuming to support the same high degree of coverage for some non-critical area.

Programming Abstractions:

A key to the growth of WSN is raising the level of abstraction for programmers. Currently, programmers deal with too many low levels details regarding sensing and node to node communication. For example, they typically deal with sensing data, fusing data and moving data. They deal with particular node to node communication and details. If we raise the level of abstraction to consider aggregate behavior, application functionality and direct support for scaling issues then productivity increases. Current research in programming abstractions for WSN can be categorized into 7 areas: environmental, middleware APIs, database centric, event based, virtual machines, scripts and component-based. As an example, consider an environmental based abstraction called EnviroTrack [3]. Here the programmer deals with entities found in an application. If the application tracks people and vehicles, then the programmer can define people and vehicle entities and utilize library routines that support low level sensing functions that can detect and classify objects of these types. They can also easily specify the application level processing associated with each type of entity. This allows programmers to deal with application level functionality rather than low level details. Since WSN deal primarily with collecting, analyzing and acting on data, a database view of such systems is popular. In this view, a programmer deals with queries written in an SQL-like format. However, real-world data issues such as probabilistic data, various levels of confidence in data and missing or late data sometimes make the SQL paradigm insufficient. It is likely that no one programming abstraction for WSN will exist. Rather, a number of solutions will emerge, each better for certain domains. Results in this area are critical in order to expand the

development and deployment of WSN by the general programmer as opposed to the WSN specialist.

Security and Privacy:

WSN are limited in their energy, computation, and communication capabilities. In contrast to traditional networks, sensor nodes are often deployed in accessible areas, presenting a risk of physical attacks. Sensor networks interact closely with their physical environment and with people, posing additional security problems. Because of these reasons current security mechanisms are inadequate for WSN. These new constraints pose new research challenges on key establishment, secrecy and authentication, privacy, robustness to denial-of-service attacks, secure routing, and node capture. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security and privacy pervade every aspect of system design. Consider one of the most difficult attacks to defend against. Adversaries can severely limit the value of a wireless sensor network by denial-of-service attacks [4]. In the simplest form of denial-of-service attack, an adversary attempts to disrupt operation by broadcasting a high-energy signal. If the transmission is strong enough, the entire system could be jammed. More sophisticated attacks are also possible: the adversary can inhibit communication by violating the MAC protocol, for instance by transmitting while a neighbor is also transmitting or by continuously requesting channel access with a RTS (request-to-send). New techniques for dealing with this simple yet potentially devastating attack are needed. Many other security related problems need further research [5]. One challenge is how to secure wireless communication links against eavesdropping and tampering. Overall, security is a difficult challenge for any system. The severe constraints and demanding environments of WSN make computer security for these systems even more challenging.

Analysis:

Few analytical results exist for WSN. Since WSN are in the early stage of development it is not surprising that few analytical results exist. Researchers are busy inventing new protocols and new applications for WSN. The solutions are built, tested and evaluated either by simulation or testbeds; sometimes an actual system has been deployed. Empirical evidence is beginning to accumulate. However, a more scientific approach is required where a system can be designed and analyzed before it is deployed. The analysis needs to provide confidence that the system will meet its requirements and to indicate the efficiency and performance of the system. Consider the following interesting analysis questions. What density of nodes is required to meet the lifetime requirements of the system? What sensing and communication ranges are needed to detect, classify and report a target to a base station by a deadline? What sensing range and what nodes need to be awake in order to guarantee a certain degree of sensing coverage for a system? Given n streams of periodic sensing traffic characterized by a start time, period, message size, deadline, source location and destination location for a given WSN will all the traffic meet their deadlines? To answer this last question, the interference patterns of wireless communication must be taken into account. Once analysis techniques and solutions are developed for these types of questions, they must also be validated with real systems.

Summary:

In this brief note six key research areas were highlighted. However, many other research areas are very important including: localization, topology control, dependability, self-calibration, self-healing, data aggregation, group management, clock synchronization, query processing, sensor processing and fusion under limited capacities, and testing and debugging. WSN are a fascinating area with great potential. The impact of this area on the world can rival the impact that the Internet has had. Exciting and difficult research challenges lie ahead before this becomes reality.

References

[1] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, RAP: A Real-Time Communication Architecture for Large-Scale Wireless Sensor Networks, RTAS, June 2002.

[2] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, SPEED: A Stateless Protocol for Real-Time
Communication in Ad Hoc Sensor Networks, IEEE ICDCS, May 2003.

[3] T. Abdelzaher, B. Blum, D. Evans, J. George, S. George, L. Gu, T. He, C. Huang, P. Nagaraddi, S. Son, P. Sorokin, J. Stankovic, and A. Wood, EnviroTrack: Towards an Environmental Computing Paradigm for Distributed Sensor Networks, IEEE ICDCS, April 2004.

[4] A. Wood and J. Stankovic, Denial of Service in Sensor Networks, IEEE Computer, Vol. 35, No. 10, October 2002, pp. 54-62.

[5] A. Perrig, J. Stankovic, and D. Wagner, Security in Wireless Sensor Networks, invited paper, CACM, Vol. 47, No.6, June 2004, pp. 53-57.