2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing

Integration of Smart Sensor Networks into Internet of Things: Challenges and Applications

Dan Partynski
Department of Mathematics and Computer Science
University of San Diego
San Diego, CA 92110
Email: dpartynski@sandiego.edu

Simon G. M. Koo
Department of Computer Engineering
Santa Clara University
Santa Clara, CA 95053
Email: simonkoo@ieee.org

***Abstract*—With the advancement of sensing technology and the increasing computational power of processors, there is an increased interest in using large, dynamically distributed wireless sensor networks (WSN) in a variety of areas. In recent years, WSN technology has proven to be beneficial in health and environmental monitoring, military applications, and many other fields. Since WSN can both sense the environment and apply algorithms to process the data, more real-time and useful information can be gathered from the physical world than using traditional sensing systems. These networks can also be integrated into the "Internet of Things" in order to allow collaboration and wider access to sensor data. This paper will explore the challenges faced by WSNs and how they can be addressed, from hardware and software aspects to security, which is especially important in an internet context.**

***Keywords*-Internet of Things; wireless sensor networks; smart sensors;**

I. Introduction

As we move toward the future of technology, computers will become increasingly prevalent in our daily lives. Advances in microprocessors and data processing will allow for the use of small, ubiquitous computing devices that may change the way we work with computers. A network of smart wireless sensors has the potential to be of great benefit across a large number of industries.

According to IEEE [1], a smart sensor node is a sensor "that provides a function beyond those necessary for generating a correct representation of a sensed or controlled quantity. This function typically simplifies the integration of the transducer into applications in a networked environment." A smart wireless sensor network thus consists of a large number of dynamically distributed smart sensor nodes. Due to the appeal of a truly dynamic system, the nodes must form an ad-hoc network robust to node failure and other changes in network topology, adding to the complexity of the underlying collective intelligence algorithms.

WSN can also be connected to the internet in order to support the Internet of Things, which is a "a worldwide network of uniquely addressable interconnected objects." [2] This integration will allow for networks to utilize existing data and will allow for data produced by the network to be available to other objects that have been integrated. This will allow for colloboration across many different services.

The main appeal of these networks, their ability to be cast into a dynamic environment for sensing purposes and require little to no human involvement, is the underlying cause of many significant research challenges. Hardware issues are especially challenging, as each sensor node needs sufficient energy and durability to perform its tasks. The underlying software and algorithms must be designed in such a way as to use the hardware to its full potential. Because these networks may be connected to the Internet, security issues become especially important. While there are many challenges to achieving this technology, the progression of sensor networks is an important goal. There are many potential uses of smart sensor networks, and there are likely many applications not yet imagined.

This paper will explore various aspects of Smart Wireless Sensor Networks. The standard architecture of a typical sensor network will be presented in Section II. Section III will explore various research challenges of these networks. Section IV will discuss various applications of sensor networks, and Section V concludes this paper.

II. System Architecture

Before going over research challenges and applications of smart sensor networks, we first give an overview of the architecture of both the individual sensing nodes and then the network as a whole.

A. Sensor Node Architecture

A typical node in a smart sensor network will consist of a few basic modules. These are the sensor module, the computation and communication module, and the power module [3]. The role of the sensor module is to gather different kinds of environmental data. Depending on the application, the nodes can be built with a variety of different sensors including temperature, acoustic, motion, moisture, magnetic, and humidity. Though it is possible that each individual node can include many of these different sensors on its own, it is likely more cost effective to limit a node

978-0-7695-5046-6/13 $26.00 © 2013 IEEE
DOI 10.1109/GreenCom-iThings-CPSCom.2013.202

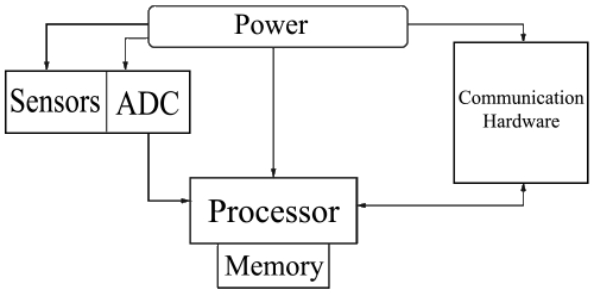

Figure 1. Basic components of a sensor node

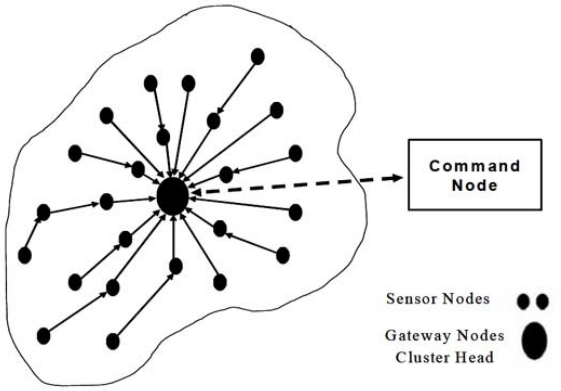

Figure 2. A typical node cluster

to perhaps one or two of these sensors. If an application calls for a large variety of sensors, then certain subsets of sensor nodes can be equipped with different sensor types, and a central intelligence will pool the disparate sensor data for processing. The computation and communication module will analyze sensed data and transmit information where needed. Each node should contain a sufficiently powerful microprocessor to permit the data and signal processing required for many applications. Perhaps the most crucial aspect of the architecture is the node's power module. Typically, the power source will consist of an alkaline battery, though this is not the most energy efficient solution and may lead to a large increase in node size. An overview of the challenges related to power sources for sensor nodes is presented in Section III.

B. Network Architecture

A smart wireless sensor network will consist of hundreds or thousands of these sensor nodes, dynamically distributed into an environment. It is unlikely that the network's topology can be predetermined, so the nodes will have to form an ad hoc network. It is ideal that the network be completely autonomous as to avoid any overhead and cost associated with direct human interaction. The crucial part of the network is the relaying of information to a central base station. This base station may log the data produced by the network and may perform any final analysis needed that may have been too impractical in the nodes themselves. It can also act as a bridge between the sensor nodes and the larger Internet of things. This base station will receive the data streams of the sensor network and process queries, then relay any requested information to an appropraite external entity. Having every node of the network transmit its sensed data directly to the base station works in theory, but due to the energy constraints of a single node, the combination of sensing data, processing it, and transmitting it to a base station may prove to be impractical. One possible solution is to have a central node distributed with the network, which would receive data from other nodes and relay the data to the base station. While this does solve a few energy related problems, having one central node to perform such an important task is undesirable as it leads to a single point of failure for the network. Thus networks will likely form node clusters, where a cluster is "a set of sensor nodes that surround the target phenomena and are capable of detecting and processing the data required by the users." [4] Each cluster selects a node to be the cluster head, which will coordinate the actions of all the nodes within the cluster. Each cluster head will relay information to a central node, or directly to the base station if the central node has failed. The concept of node clustering leads to many benefits in the network architecture. They provide many points of failure rather than just one, and by coordinating behavior, they prevent redundancies among the sensor nodes within the cluster, thus preserving energy [5]. Clearly, network architecture is of critical importance to the success of a smart wireless sensor network, as a poor network design will lead to wasted energy and a short network lifetime.

III. Challenges in Smart Wireless Sensor Networks

There are many interesting researches aimed at addressing challenges related to sensor networks. In this section, we will categorize such challenges into three different areas: security, hardware, and software, and discuss the challenges associated with each aspect.

A. Security

The nature of smart wireless sensor networks leads to several critical security issues that need to be addressed. Such issues include, but are not limited to, node compromise, unauthorized data access, and denial of service attacks. If a network is integrated into the Internet of Things, the severity of many of these issues is increased.

1) Node Compromise: Since wireless sensor networks may consist of hundreds or thousands of smart nodes working together, each node is a potential point of attack. However, due to the dynamic dispersion of these nodes, it

is impractical if not impossible to monitor each one of these nodes to protect them from an attacker [6].

A potential issue is the addition of a false node in the network, which would transmit corrupt information and attempt to falsify sensor data. This type of attack has been studied in other types of ad-hoc networking systems, but the countermeasures tend to be computationally expensive and too impractical for sensor networks given their energy constraints [7].

Other issues arise when the sensor network is connected to the internet. Proximity to the network becomes unimportant for attackers, and nodes can be compromised remotely. This leads to new threats like malware introduced through an internet connection, which could corrupt many of the network nodes [8].

However, if an attacker is close to the network, physical attacks on the individual sensor nodes become an issue. It is possible to make the individual sensing nodes resistant to physical tampering, so that it would be difficult for an attacker to alter a nodes behavior if captured. However, this would likely be a cost ineffective solution for large networks, and does not alleviate all of the issues of node compromise. The end goal is a network that can both detect anomalies and function in the presence of a subset of corrupt or malicious nodes.

2) Unauthorized Data Access: Perhaps the most obvious security hurdle for a smart wireless sensor network is the prevention of access to network‘s transmitted information. There is a large amount of data generated by these networks, which can be easily viewed remotely by an attacker if no security measures are taken.

A standard way to combat this is to encrypt the information, but encryption algorithms may be expensive in a low energy environment. It is also worth noting that if a network wide encryption key was used for security purposes, it is possible that the compromise of a single node could allow for decryption of the entire network. Some potential encryption schemes are described in [9], though due to the complexity of data encryption and the limited availability of power, new schemes may need to be developed.

In an internet context, this issue becomes especially difficult to combat. Where as in a standard sensor network there is mostly concern with attackers in close proximity to the network, a sensor network integrated into the Internet of Things can be accessed by users from around the world. Thus any network can face several unauthorized data requests, and the network must be able to safely check if a user is able to access the data of a sensor node [10].

3) Denial of Service: Rather than compromise individual nodes, a malicious outsider could launch an attack on the entire network, thus rendering the network incapable of performing its task. These attacks may come in many forms, such as transmitting malicious signals into the network in order to interfere with routing protocols, or sending large amounts of useless information to sensors in order to waste their battery life. Some countermeasures to denial of service attacks are presented in [6] such as authentication to prevent unwanted signals from being processed by the network. Yet each countermeasure may in fact open up a number of other vulnerabilities, so much research needs to be done in order to construct a truly secure smart wireless sensor network.

B. Hardware

Wireless sensor networks are an ambitious concept, and there are many software issues that need to be taken care of before these networks can be widely used. However, there are just as many hardware challenges that will arise. These issues center around the difficulty of taking a sensing unit, a transceiver unit, a processing unit, and a power unit, condensing the entire system to the size of a cubic centimeter [11], and have the device be as energy efficient and cost effective as possible. Here we examine two major research challenges, preserving as much energy as possible and maximizing the node‘s processing ability.

1) Energy: Ideally, the nodes that make up a smart wireless sensor network would remain in a dynamic environment for long periods of time until the sensing job is done and all the required data has been collected and analyzed. However, it is inevitable that in the duration of the networks lifetime there will be small subset of the nodes that deplete their source of available energy. The underlying software of the network should be robust enough to handle these small changes in the network‘s topology, but the longer individual nodes can survive the better the collective data will be overall.

The question is what should be the energy source for each of the individual nodes of the network? Battery power is certainly an option, but the end goal is to have each node be as small as possible, and batteries would dominate the size of the structure. A better option is to use fuel cells, which are “rechargeable electrochemical energy-conversion devices where electricity and heat are produced as long as hydrogen is supplied to react with oxygen.” [12] Fuel cells would allow for good energy storage and power delivery, with the downside of a more complicated architecture. Perhaps the most interesting solution is to create energy scavenging devices, which gather acoustic, thermal, or solar energy for storage inside built-in capacitors. This design would allow for the initial goal of tiny sensing nodes that can survive on their own in a dynamic environment for extended periods of time with a minimized risk of node failure. Whether future networks will use these energy saving techniques or others, the task of powering sensing devices for long periods of time while keeping the size of the devices as small as possible remains a significant research challenge.

2) Processing: Due to the complexity of the sensed data across the network, each sensor node would ideally perform a certain amount of data processing before transmitting the

information to another node or to the base station. Thus it is desirable that each node have a modestly fast processor. Due to the previously stated constraints of a sensing node, this may not be very easy to include in a cost effective manner, since each node should only cost around $1 in order for the entire network to be cost effective [11]. It is possible to rely on CMOS technology for each node‘s processor, but it may prove difficult to simultaneously achieve energy efficiency. Designing a processor that can work quickly inside of a tiny sensing node while simultaneously minimizing total energy usage remains an interesting and important research challenge.

C. Software

Coordinating thousands of sensor nodes in a dynamic environment with limited energy will prove to be a difficult challenge, so a robust software system and a new class of algorithms will be needed for the future of smart wireless sensor networks.

One energy related issue that can potentially be alleviated by software is the energy required for the transmission of data. Transmitting data to a base station and even to neighboring nodes can drain large amounts of a sensor node‘s energy supply, thus hindering its lifetime and the lifetime of the network as a whole. A possible solution is to take advantage of a node‘s processing ability and compress the sensed data before transmitting it to the other parts of the network. The idea is that the amount of energy needed to compress the data before sending it is far less expensive than the energy needed to transmit the full uncompressed data. While this idea has potential, existing data compression algorithms may still be too expensive to run in a single energy-constrained sensor node. Thus wireless sensor networks would benefit from a new, efficient data compression algorithm. Some sample algorithms for this task are presented in [13].

To reduce human interaction and to support the concept of an autonomous network, wireless sensor networks must be self-organizing. That is, when cast into an environment, the nodes must attempt to form clusters, assign heads to each of the clusters, and distribute tasks among the individual nodes so as to limit the amount of redundant behavior. For many applications, it may be beneficial for all or some of the nodes to know their location, but location identification techniques (such as GPS) tend to be computationally expensive. It may be possible to have only a small subset of node calculate their position, and design location algorithms to deduce the positions of the rest of the network nodes, thus limiting the energy used across the network.

A difficulty that can arise due to various instances of node failure is a coverage hole. A coverage hole is any region that is not sufficiently covered by a small number of sensors. The environment that the nodes have been deployed in ideally would be fully covered, but this clearly will not happen in the majority of cases. Closely related to a coverage hole is a routing hole, a region where either no nodes exist or are unable to transmit information across the network for various reasons. These challenges are inevitable in any network, and robust software solutions are required. A broader overview of the coverage problem and some potential solutions are presented in [14].

Perhaps the most difficult software challenges associated with these networks is software engineering, efficiently programming the nodes for a desired application. It is perhaps beneficial to break up the software development into different components in order to simplify the process. Three such components could be the sensor applications, the node applications, and the network applications [15]. The sensor application would have complete access to the operating system of each of the individual node and would be most closely linked to the hardware. The node application would be concerned with all high-level node tasks, such as data processing, data transmission, and location algorithms. The highest layer would be the network applications, which would interface with the administrator of the network.

IV. Applications

This section will present a few of the potential applications of wireless sensor networks. There are many applications that these networks could be used for, and perhaps many that are not yet imagined, so here we examine a small application subset.

Because the sensors are equipped with various environmental sensing capabilities, wireless sensor networks are well-suited to environmental monitoring. For example, sensor nodes can be scattered across an environment and constantly collect information relating to temperature and humidity. In the future, the individual nodes may be small enough to literally loft about an environment by the wind, leading to even greater weather sensing opportunities. Various environmental events can also be detected with this kind of widespread continuous data gathering. The data acquired by these networks could help predict oncoming storms and earthquakes, and alert a base station of environmental fires by carefully analyzing sensed temperature data. If the network is integrated into the Internet of things, then anyone with access to the internet would be able to request this environmental data from anywhere in the world. This kind of remote access to global data may lead to larger, widespread, real-time weather monitoring applications.

Wireless sensor networks have many military related applications. One possible application is to use sensor nodes as a replacement to mine fields. Sensor nodes scattered across a battlefield could detect acoustic and seismic activity to detect the presence of a hostile unit [16]. If the nodes determine that there is a threat, then they could relay information to a nearby actuator to handle the situation. Determining that a present unit is indeed an enemy personnel can be quite

complex, and may rely on complex classification algorithms, which can of course be performed by the network. While this has been described as a wartime application, these concepts can be applied in peacetime for surveillance purposes.

If large cities utilize the Internet of things, then sensor networks can enhance the efficiency of the transportation domain. For example, vehicles and roads can be equipped with sensors which communicate with each other and central stations in order to help better route traffic [17]. Such networks could also function in the public transportation domain by equipping buses and taxis with locational sensors and having nearby hubs for information about the routes of these vehicles. In a more futuristic scenario, streets and vehicles may be equipped with various kinds of sensors in order to enable vehicles to safely and autonomously traverse the various streets of a city.

The small size and processing capabilities of sensor nodes make these networks ideal for health related applications. Patients in hospitals can wear a large number of sensor nodes, which will be unobtrusive and carefully monitor and analyze the patients‘ physiological signs. The work can also be split up across many sensor nodes. For example, one subset of the nodes may be responsible for detecting heart rate, and another may only detect blood pressure. This will allow for detailed monitoring of a patient, and because the sensors can collectively analyze the data, they may be able to deduce context information (e.g. they can determine if an increase in heart rate is caused by exercise or a more serious health problem).

The use of sensor networks can also lead to the creation of smart environments, where sensors control the various aspects of a home such as lighting, temperature, and security. For example, external sensor networks can analyze the outside temperature and use this to control the heating system inside of the home. External weather sensors can also send alerts to the smart environment to close windows if a high probability of rain has been calculated. This kind of management makes the lives of the human users easier while at the same time allows for efficient management of the energy used by a home.

V. Conclusion

In the future, Smart Wireless Sensor Networks will become a standard informational tool throughout various industries due to their ability to gather and process data in new ways. As the technology advances, these networks will reduce in cost, and their use will be widespread across various applications. Their integration into the internet will allow for wide access to sensor data and collboration between geographically disparate networks. This paper has presented many of the challenges that must be addressed before the true potential of Wireless Sensor Networks can be fully realized. While issues in security, hardware, and software pose a great barrier to this technology, various research projects hope to address these issues in order to make wireless sensor networks a reality.

It is not entirely clear when these networks will become a fully functional, ubiquitous technology, but the progress in the direction of these networks is greatly important. The complex collective intelligence of smart wireless sensor networks combined with their integration into Internet of Things will enable us to learn more about our world than ever before. It will take ingenuity and a large amount of dedicated research to achieve this futuristic technology, but due to the data acquisition potential of smart wireless sensor networks, it is well worth the effort.

References

[1] Institute of Electrical and Electronics Engineers (IEEE), *1451.2-1997 IEEE Standard for a Smart Transducer Interface for Sensors and Actuators – Transducer to Microprocessor Communication Protocols and TEDS Formats*, Piscataway, NJ 08855, Sep 1997.

[2] L. Mainetti, L. Patrono, and A. Vilei, “Evolution of wireless sensor networks towards the internet of things: a survey,” in *Int. Conf. on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2011, pp. 1–6.

[3] G. Song, Y. Zhou, Z. Wei, and A. Song, “A smart node architecture for adding mobility to wireless sensor networks,” *Sensors and Actuators A: Physical*, vol. 147, no. 1, pp. 216–221, 2008.

[4] A. Al-Ali, Y. Aji, H. Othman, and F. Fakhreddin, “Wireless smart sensors networks overview,” in *Second IFIP International Conference on Wireless and Optical Communications Networks (WOCN) 2005*. IEEE, 2005, pp. 536–540.

[5] I. F. Akyildiz and I. H. Kasimoglu, “Wireless sensor and actor networks: Research challenges,” *Ad hoc networks*, vol. 2, no. 4, pp. 351–367, 2004.

[6] H. Chan and A. Perrig, “Security and privacy in sensor networks,” *Computer*, vol. 36, no. 10, pp. 103–105, 2003.

[7] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, “Security for sensor networks,” in *CADIP Research Symposium*, 2002, pp. 1–11.

[8] D. Christin, A. Reinhardt, P. Mogre, and R. Steinmetz, “Wireless sensor networks and the internet of things: Selected challenges,” in *Proceedings of the 8th Fachgesprach Drahtlose Sensornetze*. IEEE, 2009, pp. 54–57.

[9] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[10] R. Roman and J. Lopez, “Integrating wireless sensor networks and the internet: a security analysis,” *Internet Research*, vol. 19, no. 2, pp. 246–259, 2009.

[11] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[12] D. Puccinelli and M. Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing," *Circuits and Systems Magazine, IEEE*, vol. 5, no. 3, pp. 19–31, 2005.

[13] N. Kimura and S. Latifi, "A survey on data compression in wireless sensor networks," in *International Conference on Information Technology: Coding and Computing (ITCC) 2005*, vol. 2. IEEE, 2005, pp. 8–13.

[14] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: A survey," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 2, pp. 4–18, 2005.

[15] J. Blumenthal, M. Handy, F. Golatowski, M. Haase, and D. Timmermann, "Wireless sensor networks-new challenges in software engineering," in *Proceedings of IEEE Conference on Emerging Technologies and Factory Automation (ETFA) 2003.*, vol. 1. IEEE, 2003, pp. 551–556.

[16] T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*. IEEE, 2005, pp. 719–724.

[17] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Wireless Communications*, vol. 17, no. 6, pp. 44–51, 2010.

[18] M. Gigli and S. G. M. Koo, "Internet of things: Service and applications categorization," *Advances in Internet of Things*, vol. 1, no. 2, pp. 27–31, Jul. 2011.