Approach to the Design of The Intelligent Wireless Sensors

Mare Srbinovska[1] and Vladimir Dimcev[2]

Abstract –**The availability of low cost, low power and miniature embedded processors, radios and sensors, integrated on a single chip, is leading to the use of wireless communications and computing for interacting with the physical world in many civilian and military applications. The resulting systems are called Wireless Sensor Networks (WSN). The advances in the integration of complex wireless integrated products and the increase in performance and functionality of the design tools, the requirements and properties of a single device (sensor node) are elaborated.**

Keywords – **Wireless sensor networks, sensor nodes, embedded processors, radios**

I. INTRODUCTION

A wireless sensor networks (WSNs) consist of an array of sensors, of diverse types, interconnected by a wireless communication network. Sensor data is shared between these sensor nodes and used as input to a distributed estimation system whose function is to extract the relevant information from the available data. Fundamental design objectives of sensor networks include reliability, accuracy, flexibility, cost effectiveness and easiness of deployment. Each node has one or more sensing unit, an embedded processor and low-power radios. The nodes act as information sources, sensing and collecting data samples from their environment. They perform routing functions, creating multi-hop wireless networking fabric that conveys data samples to other sensor nodes. Nodes can also act as information sinks, receiving dynamic configuration information from other nodes or external entities. The rapid deployment, self-organization and fault tolerance characteristics for WSNs make them promising for a number of military and civilian applications [2]. Wide varieties of these applications have been enabled by the promise of inexpensive networks of wireless sensors. Dramatic advances in communication systems and micro-electro-mechanical systems (MEMS) design reduce the cost of the sensor nodes, which in turn enable the use of large scale WSNs for a variety of new monitoring and control applications. For these applications to be viable, the sensed/monitored data must be located. Traditional physical localization techniques are not well suited for these requirements.

Including GPS on every device is cost and energy prohibitive for many applications. The solution is cooperative localization such that sensors work together in a peer-to-peer manner to make measurements and then form a map of the network forming local coordinate systems. Based on the local coordinates formed inside the WSNs, they can be transformed to global coordinates if at least two reference nodes in the WSNs have known coordinates or are equipped with GPS receivers.

The basic functionality of a wireless node generally depends on the application, but the following requirements are typical:

- Determine the value of a parameter at a given location. In, an environment-oriented WSN, one might need to know the temperature, atmospheric pressure and the relative humidity at a number of locations. This example shows that a given wireless nodes may be connected to different types of sensors, each with a different sampling rate and range of allowed values.
- Detect the occurrence of events of interest and estimate the parameters of the events. In traffic – oriented WSN, one would like to detect a vehicle moving through an intersection and estimate the speed and direction of the vehicle.
- Classify an object that has been detected. In a traffic sensor network for example a car, a minivan, a light truck or a bus?
- Track an object. In a military WSN, track an enemy tank as it moves through the geographic area covered by the network.

For WSNs to become truly ubiquitous, a number of challenges must be overcome. Challenges and limitations of wireless sensor networks include, but are not limited to, the following:

- limited functional capabilities, including problems of size,
- power factors,
- node costs,
- environmental factors,
- transmission channel factors,
- topology management complexity and node distribution.

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. However, one of the major benefits to wireless systems is the easiness of installation. Requiring power to be supplied externally to all nodes negates this advantage.

[1] Mare Srbinovska is with the Faculty of Electrical Engineering and Information Technologies, Karpos 2 bb, 1000 Skopje, R. Macedonia E-mail:mares@feit.ukim.edu.mk

[2] Vladimir Dimcev is with the Faculty of Electrical Engineering and Information Technologies, Karpos 2 bb, 1000 Skopje, R. Macedonia E-mail:vladim@feit.ukim.edu.mk

In most application scenarios, a majority of the nodes will have to be self-powered. They will 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.

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. 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.

A key advantage of wireless sensor networks is their easiness of deployment. 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.

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.

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 data is arriving over the network, the Central Processing Unit (CPU) must simultaneously control the radio and record/decode the incoming data. Higher communication rates required faster computation.

II. HARDWARE COMPONENTS

When choosing the hardware components for a wireless sensor node, the application's requirements play a decisive factor with regard to size, costs and energy consumption of the nodes-communication and computation facilities as such are often considered to be of acceptable quality, but the trade-offs between features and costs is crucial.

Basic sensor node consists of 5 main components (Fig.1):

Controller –to process all the relevant data, capable of executing arbitrary code.

Memory – to store programs and intermediate data, usually different types of memory are used for programs and data.

Sensors and actuators - the actual interface to the physical world, devices that can observe or control physical parameters of the environment.

Communication – turning nodes into a network requires a device for sending and receiving information over a wireless channel.

Power supply – some form of batteries are necessary to provide energy. Sometimes, some form of recharging by obtaining energy form the environment is available as well (e.g. solar cells).

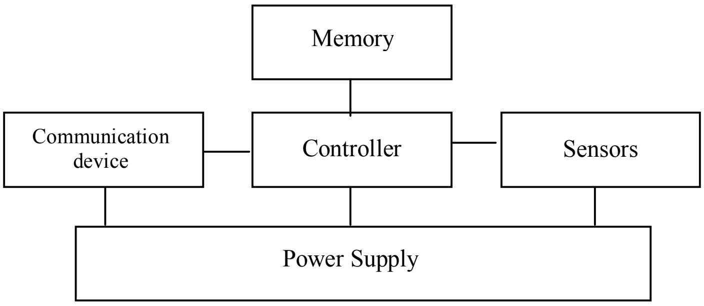

Fig.1 Main sensor node hardware components

Each of these components has to operate balancing the trade-off between as small energy consumption as possible on the one hand and the need to fulfill their tasks on the other hand. Both the communication device and the controller should be turned off as long as possible. To wake up again, the controller could use a preprogrammed timer to be reactivated after some time [1].

The radio subsystem is the most important system on a wireless sensor node since it is the primary energy consumer in all three of the application scenarios. Modern low-power, short range transceivers consume between 15 and 300 miliwatts of power when sending and receiving.

The overall setup of sensor node prototypes that have been developed and are currently used by different groups for experimental research is in principle very similar. Examples for such nodes include Mica motes, the nodes developed locally at Teschnische Universitt Karlsruhe, Freie Universitt Berlin. Typical microcontrollers are the Atmel, Motorola microcontrollers or the Texas Instruments MSP 430; usable radio modems include those by RFM, Chipcon, Maxim, Infineon; also, Bluetooth chipsets are sometimes used.

Typical block scheme of microcontroller is shown in Fig.2.

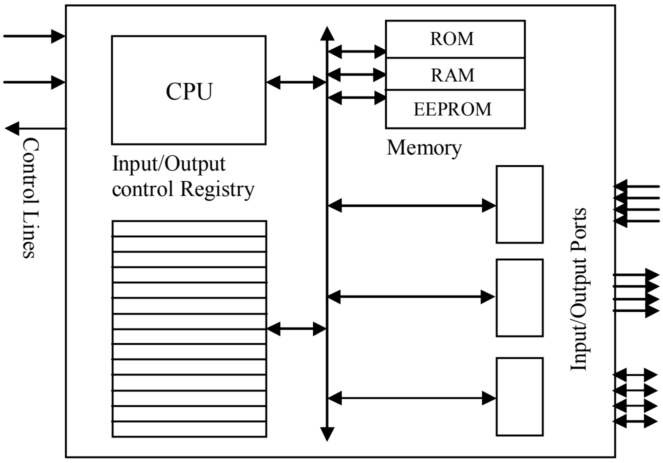

Fig.2 Typical block scheme of microcontroller

While all of these nodes have their individual advantages and disadvantages and the level of diversity is natural for the current state of WSN research, a lot of synergy could be gained if a convergence to a single prototype could be achieved. The economies of scales alone would make such an effort worthwhile by making prototype nodes available in larger quantities at low cost. The Mica Motes offerings by Crossbow [1] are a step in this direction. The Mica platform includes a low power transceiver, a power management subsystem, extended storage and an embedded microcontroller. The most advanced hardware platform is a single-chip device that integrates the processing, storage and communication capabilities to form a complete system node. This single chip node contains a microcontroller, transmitter, ADC, general purpose I/O ports, UART, memory and encryption engine. The tiny chip only needs to be supported by a 32 kHz watch crystal and a power supply, a battery and a 4MHz clock.

III. SOFTWARE ARCHITECTURE FOR WIRELESS SENSORS

A critical step towards achieving the vision behind wireless sensor networks is the design of a software architecture that bridges the gap between raw hardware capabilities and a complete system. The demands placed on the software of wireless sensor networks are numerous. It must be efficient in term of memory, processor and power so that it meets strict application requirements. It must be also agile enough to allow multiple applications to simultaneously use system resources such as communication, computation and memory. TinyOS is an operating designed explicitly for networked sensors.

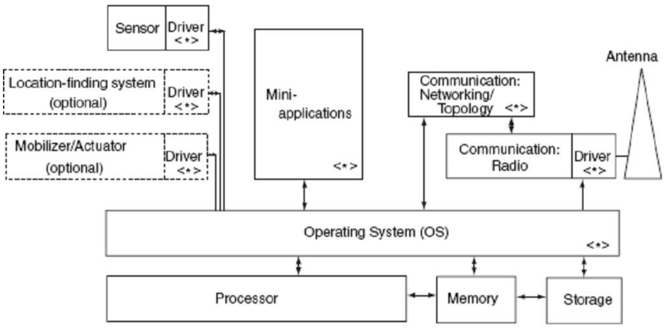
Sensor
Driver <*>
Location-finding system (optional)
Driver <*>
Mobilizer/Actuator (optional)
Driver <*>
Mini-applications <*>
Communication: Networking/ Topology <*>
Antenna
Communication: Radio
Driver <*>
Operating System (OS) <*>
Processor
Memory
Storage

Fig.3 Software components of wireless nodes

Sensors typically have five basic software subsystems:

- Operating system (OS) microcode (Fig.3). This is the board –common microcode that is used by all high-level node-resident software modules to support various functions.
- Sensor drivers. These are the software modules that manage basic functions of the sensor transceivers; sensors may possibly be of the modular/plug in type, and depending on the type and sophistication, the appropriate configuration and setting must be uploaded into the sensor.
- Communication processors. This code manages the communication functions, including routing, packet buffering and forwarding, topology maintenance, medium access control, encryption, and FEC.
- Communication drivers. These software modules manage the minutia of the radio channel transmission link, including clocking and synchronization, signal encoding, bit recovery, bit counting, signal levels and modulation.
- Data processing. These are numerical, data-processing, signal-value storage and manipulations, or other basic applications that are supported at the node level for in-network processing.

IV. COOPERATION IN WSN

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous tiny devices (nodes) using several sensors to cooperatively monitor physical or environmental conditions, such as temperature, lighting, sound, vibration, pressure, motion or pollutants, at different locations. Localization is very important for self-configuring WSN and is essential to process the sensed data properly.

The cooperation [3] between these autonomous tiny devices introduces a new domain of research, which is the distributed physical layer. The difference between embedded transmitters and locations of each node cooperatively transmitting to a desired node introduce new scenarios and challenging technical questions to be answered. As a fundamental design objective in WSN, transceivers embedded in each node must remain simple, low cost, and power consumption.

V. SECURITY CHALLENGES IN WSN

The deployment on WSNs for monitoring, data gathering, collaborative communication and computing, these networks must be able to provide authentic information. While the wireless networks and their flexibility to form ad hoc networks with minimal or no prior infrastructure is desirable, the wireless medium is also vulnerable to unwanted eavesdropping, and other attacks such as wormholes. Such attacks have no counter part in wired/wireless networks. Moreover, due to new scenarios have emerged for WSN applications, solutions that have been developed for wired and wireless networks are often not applicable.

VI. LOCALIZATION ALGORITHMS

Localization in WSNs is an integral part in any application that requires monitoring, control and/or tracking functionality. Localization availability will open a new direction to find security solutions based on location aware.

Hence, localization is mandatory for practical WSNs. Traditional localization techniques are sometimes inadequate for some of these applications. For instance, using GPS (Global Positioning System) receiver on each device is energy prohibitive, and is limited to outdoor applications. Moreover, the cost becomes a major issue, especially if HSGPS (High Sensitivity Global Positioning System) is utilized.

Lots of localization algorithms require a distance to estimate the position of unknown devices. In addition to mere connectivity information, the communication between two nodes often allows to extract information about their geometric relationship. Using elementary geometry, this information can be used to derive information about node positions.

The characteristics of wireless communication are partially determined by the distance between sender and receiver, and if these characteristics can be measured at the receiver they can serve as an estimator of distance. The most important characteristics are Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), and Time Difference of Arrival (TdoA).

- Received Signal Strength Indicator (RSSI) techniques measure the power of the signal at the receiver. Based on the known transmit power, the effective propagation loss can be calculated. Theoretical and empirical models are used to translate this loss into a distance estimate. This method has been used mainly for RF signals.

The RSSI [1], [2] is a very important indicator for wireless networks, since it can be used to characterize the channel status. Generally, the received signal strength gradually decreases as the receiver moves away from the transmitter. The relationship between RSS and transmitter-receiver (T-R) separation distance is described as a propagation model.

- Time based methods (ToA,TDoA) record the time-of-arrival (ToA) or time difference-of-arrival (TDoA). The propagation time can be directly translated into distance, based on the known signal propagation speed. These methods can be applied to many different signals, such as RF, acoustic, infrared and ultrasound.

- Angle -of -Arrival (AoA) systems estimate the angle at which signals are received and use simple geometric relationships to calculate node positions.

The low complexity and the fast calculation recommend this localization algorithm as very popular and often used in wireless sensor networks.

VII. Conclusion

WSNs (Wireless Sensor Networks) represent a shift toward a new and exciting proactive computing model in which hundreds of tiny computers working together on the user's behalf. It is a model where people and businesses reap technology's benefits by getting more data that are useful when needed. There are many challenges in implementing WSN ranging from hardware, software, mechanical and even human-related. Keeping the power usage sufficiently low so that they operate for enough time involves careful power management and in some cases managing charging. Radio communication hardware has to be small enough while using a suitable network algorithm. These concerns illustrate the careful balance and compromises that are needed in WSN and designs. Wireless sensor networks are a new technology that can change distributed measurement systems and are ready to implement in commercial systems. The success of a new technology is not only determined by the technology itself, but many other factors as well.

References

[1] M.Srbinovska, “Model for position estimation of smart sensors in distributed measurement systems”, Master Thesis, Ss. Cyril and Methodius University, Skopje, 2008

[2] Mostafa I. Abd-El-Barr, Mohamed A. Youssef and Maryam M. Al- Otaibi, Wireless Sensor Networks - Part I: Topology and Design Issues, 18th IEEE Annual Canadian Conference on Electrical and Computer Engineering CCECE 2005

[3] Neal Patwari, Joshua N. Ash, Spyros Kyperountas, Alfred O. Hero III, Randolph L. Moses, and Neiyer S. Correal, "Locating the Nodes [Cooperative localization in wireless sensor networks]", IEEE Signal Processing Magazine, July 2005

[4] Marina Petrova, Janne Ruhijärvi, Petri Mähönen and Saverio Labella, “Performance Study of IEEE 802.15.4 Using Measurements and Simulations”, RWTH Aachen University, Germany, 2004.

[5] Holger Karl and Andreas Willig, “Protocols and Architectures for Wireless Sensor Networks”, John Wiley & Sons, 2005

[6] Neal Patwari, "LOCATION ESTIMATION IN SENSOR NETWORKS", PhD Thesis, The University of Michigan, 2005

[7] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, “Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks,” *IEEE Communications Magazine*, vol. 40, no. 8, pp. 70–77, August 2002.

[8] J. Nicholas Laneman, "Cooperative Diversity in Wireless Networks: Algorithms and Architectures", PhD Thesis MIT 2002

[9] Kazem Sohraby, Daniel Minoli, Taieb Znati, “Wireless Sensor Networks: Technology, Protocols and Applications, 2007

[10] Bernhard H. Walke, Stefan Mangold, Lars Berlemann, “IEEE 802 Wireless Systems: Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence, 2006

[11] Ralf Grossmann, Jan Blumenthal, Frank Golatowski, Dirk Timmermann, “Localization in Zigbee based Sensor Networks, Technical Report, University of Rostock, April 2007

[12] S. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE J. Select. Areas Commun., vol. 16, pp. 1451 1458, Oct. 1998.