Available online at http://acfa.apeejay.edu

APEEJAY JOURNAL OF COMPUTER SCIENCE AND APPLICATIONS

ISSN:0974-5742(P)
Vol. 2, January 2014

A Study of Applications of Wireless Sensor Networks

[1]Kawal Jeet, [2]Yadvirender Rana and [3]Rajinder Singh Minhas
1Department of Computer Science, DAV College, Jalandhar, India
2AScT-Elect., RTMgr, ASTTBC, Surrey, BC, Canada
3Department of Computer Science, MLUDAV College, Phagwara, India
1kawaljeet80@yahoo.com, 2vsrana@hotmail.com, 3minhas_rajinder@yahoo.com

Abstract
Wireless sensor networks are currently being employed in wide variety of applications ranging from medical to military, and from home to industry. This paper aims to provide an introduction about sensor network sand its applications which could act as a reference for the increasing number of researchers whose work depend upon reliable sensor networks. Sensors integrated into structures, machinery, and the environment, coupled with the efficient delivery of sensed information, could provide tremendous benefits to society. Potential benefits include: fewer catastrophic failures, conservation of natural resources, improved manufacturing productivity, improved emergency response, and enhanced homeland security.

Keywords: *Wireless Sensor Networks, Motes, Sensors, Environmental Monitoring, Volcano Mentoring, Structural Health Monitoring, Heavy Industrial Monitoring, Vehicle Tracking, Military Applications, Medical Applications.*

1. Introduction

A wireless sensor network (WSN) in its simplest form can be defined as a network of (possibly low-size and low-complex) devices denoted as *nodes* that can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links; the data is forwarded, possibly via multiple hops relaying, to a *sink* (sometimes denoted as *controller* or *monitor*) that can use it locally, or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. They can be aware of their location or not. They can be homogeneous or not.

This is a traditional single-sink WSN. There are different Sensors such as pressure, accelerometer, camera, thermal, microphone, etc. They monitor conditions at different locations, such as temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, the current characteristics such as speed, direction and size of an object.

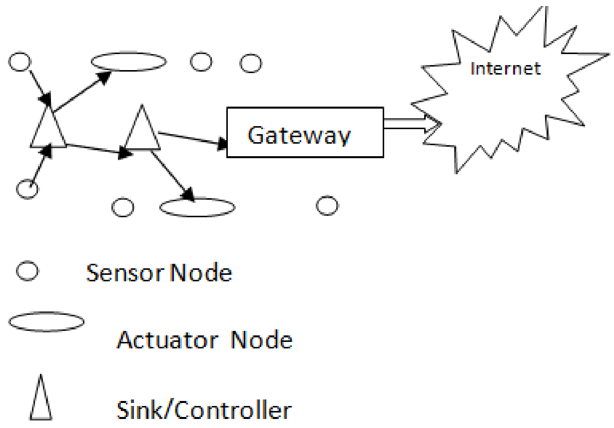

Figure 1 Single-sink WSN

1.1 The nodes' architecture

The basic elements of a WSAN are the *nodes* (either sensors or actuators), the sinks and the *gateways* [1]. Roles of Participants in WSN

- *Sources* of data: Measure data, report them "somewhere". Typically equip with different kinds of actual sensors
- *Sinks* of data: Interested in receiving data from WSN. May be part of the WSN or external entity, PDA, gateway, …
- *Actuators*: Control some device based on data, usually also a sink

Sinks, gateways and even actuator nodes are usually more complex devices than the sensor nodes, because of the functionalities they need to provide, or in some cases owing to the type of actuation mechanisms implied (e.g., mechanical actions). The sensor node is the simplest device in the network, and in most applications the number of sensor nodes is much larger than the number of sinks, or actuators. Therefore, their cost and size must be kept as low as possible. Also, in most applications the use of battery-powered devices is very convenient to make the deployment of such nodes easier. To let the network work under specified performance requirements for a sufficient time, denoted as network lifetime, the nodes must be capable of playing their role for a sufficiently long period using the energy provided by their battery, which in many applications should be not renewed for years. Thus, energy efficiency of all tasks performed by a node is a must for the WSAN design. The traditional architecture of a sensor node is reported in Figure 2. A microprocessor manages all tasks; one or more sensors are used to take data from the environment; a memory is included over the board which is used to store temporary data, or during its processing; a radio transceiver (with the antenna) is also present. All these devices are powered by a battery. Traditional batteries can provide initial charges in the order of 10,000 joules and they should be parsimoniously used for the whole duration of the network lifetime by all these devices. In some cases energy scavenging techniques can be introduced to enlarge lifetime of nodes, but in few applications can this be really considered as a viable technique.

As a result of this need to have energy-efficient techniques implemented over the board, all data processing tasks are normally distributed over the network; therefore, the nodes cooperate to provide the data to the sinks. This is also because of the low complexity that is accepted for the architecture of such nodes.

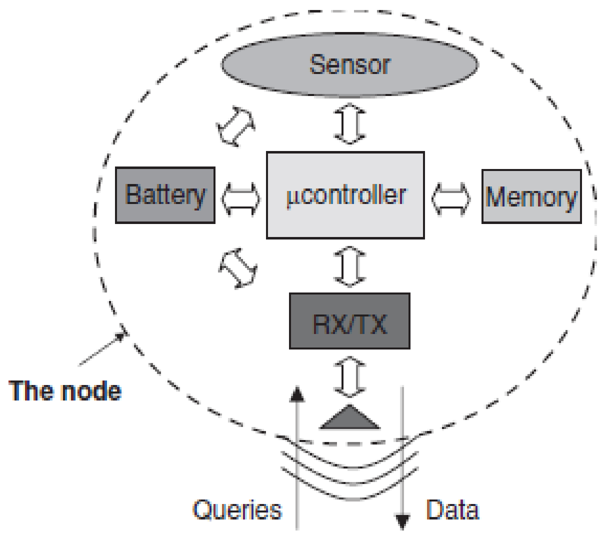

Figure 2: Architecture of sensor node

1.2 Main features of WSANs

The general description given in the previous sections already introduced the main features of a WSAN: scalability with respect to the number of nodes in the network, self-organization, self-healing, energy efficiency, a sufficient degree of connectivity among nodes, low-complexity, low cost and size of nodes are all very relevant features of WSANs; those protocol architectures and technical solutions providing such features can be considered as a potential framework for the creation of networks able to implement several types of applications. Unfortunately, the definition of such a protocol architecture and technical solution is not simple, and the research still needs to work on it. According to some general definitions, wireless ad hoc networks are formed dynamically by an autonomous system of nodes connected via wireless links without using an existing network infrastructure or centralized administration. Nodes are connected through 'ad hoc' topologies, set up and cleared according to user needs and temporary conditions. Apparently, this definition can include WSANs.

However, this is not true. This is the list of main features for wireless ad hoc networks: unplanned and highly dynamical; nodes are 'smart' terminals (laptops, etc.); typical applications include real time or non-real-time data, multimedia, voice; every node can be either source or destination of information; every node can be a router toward other nodes; energy is not the most relevant matter; capacity is the most relevant matter
Sensor nodes can be deployed in the environment:

Dropped from aircraft ⇒ ***Random deployment***

Usually uniform random distribution for nodes over finite area is assumed

Well planned, fixed ⇒ ***Regular deployment***

E.g., in preventive maintenance or similar

Not necessarily geometric structure, but that is often a convenient assumption

Mobile sensor nodes can move to compensate for deployment shortcomings.

1.3 Pros and Cons of Wireless Sensor Networking

There are many advantages of wireless sensor networking some of important prose's are: they can store a limited source of energy, they have no hassle of cables and has mobility, one of its major advantage is that it can work efficiently under the harsh conditions, and it has deployment up to large scale etc. Where it has advantages at the same time it also has some disadvantages which really take the moral of this technology down such as they have very insufficient speed of communication, it is to disturb the propagation of waves and hack your networking and the major disadvantage of wireless sensor networking is it is too costly to use.

1.4 Challenges of Sensor Networks

The nature of WSN's presents significant challenges in designing security schemes. A WSN is a special network which has many constraint compared to a traditional computer network.

Wireless Medium: The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary [12].
Ad-Hoc Deployment: The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Security schemes must be able to operate within this dynamic environment.
Hostile Environment: Motes face the possibility of destruction or capture by attackers due to hostile environment in which nodes function. This is because attackers can easily gain physical access to the devices.
Resource Scarcity: The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory [13].
Immense Scale: The proposed scale of sensor networks poses a significant challenge for security mechanisms. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.
Unreliable Communication: It is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication [14]
Unreliable Transfer: Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable.
Conflicts: Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network.
Unattended Operation: Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes [13]:

- *Exposure to Physical Attacks:* The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The probability that a sensor suffers a physical attack in such an environment is therefore much.
- *Managed Remotely:* Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues.

No Central Management Point: A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile

2 Applications

2.1 Volcano mentoring

Earlier volcano monitoring system will involve placement of one or more stations on various sites around a volcano [2]. Each station typically consists of a few (less than five) wired sensors distributed over a relatively small area (less than 100 m2), and records data locally to a hard drive or flash card. The data must be manually retrieved from the station, which may be inconveniently located. To demonstrate the use of wireless sensors for volcanic monitoring, we developed a wireless sensor network and deployed it on Volcano Tungurahua, an active volcano in central Ecuador. This network was based on the Mica2 sensor mote platform and consisted of three infrasonic (low-frequency acoustic) microphone nodes transmitting data to an aggregation node, which relayed the data over a 9 km wireless link to a laptop at the volcano observatory. A separate GPS receiver was used to establish a common time base for the infrasonic sensors. Individual infrasonic motes capture signals locally and communicate only to determine whether an “interesting” event has occurred. By only transmitting well-correlated signals to the base station, radio bandwidth usage is greatly reduced. Data from the various stations may be either recorded continuously or as triggered events and the acquisition bandwidth depends upon the specific data stream. More recently, spread-spectrum digital modems have been employed to transmit digital data from remote monitoring stations to an observatory.

System architecture

Our design consists of several components, shown in Figure 3. The first is a set of *infrasound monitoring nodes*, which sample low-frequency acoustic signals (up to 50 Hz). These nodes transmit their signals to an *aggregator node*, which relays the signals over a long distance wireless link to a *wired base station*, a laptop running various software tools to visualize, store, and analyze the real-time signals from the wireless array. To establish a common time base across the captured signals, a *GPS receiver node* is used, which receives a GPS time signal and relays the data to the infrasound and aggregator nodes through radio messages. The infrasound, aggregator, and GPS receiver nodes are based on the Mica2 mote, a typical wireless sensor device. It consists of a 7.3 MHz ATmega128L processor, 128KB of code memory, 4KB of data memory,and a Chipcon CC1000 radio operating at 433 MHz with a data rate of approximately 34 Kbps. The Mica2runs a lean, component-oriented operating system, called TinyOS.

Figure 3. Sensor arrays for volcanic monitoring.

2.2 Structural Health Monitoring

Health monitoring for civil structures has long been a research topic for industry and academia. Traditional methods include visual inspection, acoustic emission, ultrasonic testing, and radar tomography. The emergence of WSNs has prompted new, non-destructive, and cheap methods for many tasks related to structural health monitoring The volume of raw data to be gathered and transported for such applications is on the order of 1-10 Mbps. Thus, transmitting only useful information obtained from local signal processing becomes imperative for sustaining a long system lifetime [3].

2.3 Vehicle Tracking

These two scenarios belong to the PE applications. The aim of these scenarios is to make the traffic safer. To do this different information between devices located on the vehicles and on the road are transmitted: this information is, for example, related to vehicles speed, the distance between vehicles, etc [1]. Detecting a vehicle in the network begins with a node gathering and processing data leading up to the formation of a position estimate report. [4]

2.4 Real-time Wireless Sensing

The growing demand of enterprise-wide asset tracking and management has become a challenge for existing technologies. RFID technologies have been dominating this market for a long time and have been quite successful in supply-chain management. However, RFID technology does not many applications, because of its range limitations. RFID is suitable for pure identification applications where readers are located close to goods at reader points. Ultra-high frequency RFID tags promise longer identification range, however with an extremely high cost of readers. Sensinode's IP-based real-time Wireless Sensor Network (WSN) solution is the answer to full-fill the market need for asset tracking and management of the most critical assets such as personnel, machines and important goods. Unlike with RFID, WSNs are able to track active tags in real-time over large areas while combining sensor readings. Sensinode's IP-based WSN technology enables the integration of wireless sensor networks and enterprise networks, streamlining the asset data collection. This technology is targeted for versatile markets, and due to its openness and scalability, asset tracking and management achieves a whole new level of value. RFID readers can also be integrated into the WSN infrastructure which acts as a backbone for collecting readings [5]

2.5 Military Applications:

Because most of the elemental knowledge of sensor networks is basic on the defense application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defense Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing as shown in figure 4[6] Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems.

In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide following services: [6]

- Monitoring friendly forces, equipment and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces
- Targeting
- Battle damage assessment
- Nuclear, biological and chemical attack detection reconnaissance

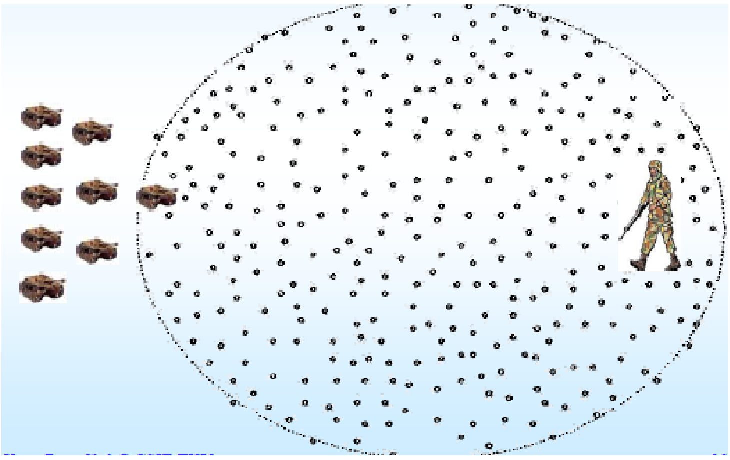

Figure 4: Military Surveillance

2.6 Environmental Applications

Nowadays sensor networks are also widely applied in habitat monitoring, agriculture research, fire detection and traffic control. [7] Because there is no interruption to the environment, sensor networks in environmental area is not that strict as in battlefield.

Environmental monitoring is another application for WSNs. The vast spaces involved in such applications require large volumes of low cost sensor nodes that can be easily dispersed throughout the region. For instance, WSNs have been studied for forest rescue alarm, soil moisture monitoring, microclimate and solar radiation mapping, and environmental observation and forecasting in rivers. Researchers at University of West Australia are developing a prototype WSN for outdoor, _ne-grained environmental monitoring of soil water. Such a network can be used to assist salinity management strategies, or to monitor irrigated crops, urban irrigation, and water movement in forest soils. In January 2005, a prototype network was built, which included 15 Mica2 nodes integrated with soil moisture sensors and other gateway and routing nodes. The system distinguishes itself by using a reactive data gathering strategy | frequent soil moisture readings are collected during rain, while less frequent readings are collected otherwise. This strategy helps increase the system lifetime.

Bush Fire Response: A low cost distributed sensor network for environmental monitor and disaster response. An integrated network of sensors combining on the ground sensors monitoring local moisture levels, humidity, wind speed and direction, together with satellite imagery and longer term meteorological forecasting will enable the determination of fire risk levels in targeted regions as well as valuable information on probable fire direction. Such a network will provide valuable understanding of bushfire development and most importantly assist authorities in organizing a coordinated disaster response that will save lives and property by providing early warning for high risk areas. [8]

Fancy Californian Winemaking: A project from Intel (the wireless vineyard) as shown in figure 5 [9]. "Imagine smart farmlands where literally every. vine plant will have its own sensor making sure that it gets exactly the right nutrients, exactly the right watering. Imagine the impact it could have on difficult areas of the world for agricultural purposes." Intel Chief Technology Officer Pat Gelsinger said. [9] In this project Berkeley motes are installed in the test site — an Oregon, USA vineyard located in a region famous for world-class pinot noir wine. They monitor temperature throughout the vineyard. Each mote in the vineyard currently takes one temperature reading per minute and stores the results. The mote records the highest and lowest temperature readings for each hour of the day. In the future these sensors may also act upon the environment. Imagine sensors that could monitor soil moisture to irrigate only the sections that needed it, or monitor crops to keep them free from pests and diseases. Information gathered by sensor networks could guide irrigation or harvesting to improve quality, providing vineyard owners and managers a better return on their investment. This potential extends to other crops where growers could use motes to maximize yields. The further aim of this project with the help of sensor networks the owner of vineyard can manage the vineyard works more efficiently and automatically. [10]

Figure 5 Wireless Vineyard

2.7 Medical applications – WSNs are used to form a so called Body Area Network (BAN), which consists of several sensors placed close to the human body measuring signals such as heart beat rate or breathe rate as shown in figure 6.

Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital. In spring 2004 some hospital in Taiwan even use RFID basic of above named applications to get the situation at first hand.

Long-term nursing home [11]: this application is focus on nursing of old people. In the town farm cameras, pressure sensors, orientation sensors and sensors for detection of muscle activity construct a complex network. They support fall detection, unconsciousness detection, vital sign monitoring and dietary/exercise monitoring. These applications reduce personnel cost and rapid the reaction of emergence situation.

2.8 Industrial applications

Sensors have already been widely used in industrial applications, such as the monitoring of automated assembly lines. Integrating wireless technology with these sensors enables condition based maintenance (CBM) to reduce downtime and enhance safety, with low installation and maintenance cost. CBM can replace traditional high-cost, schedule driven, manual maintenance for various industrial entities, including power plants, oil pipelines, transportation systems and vehicles, engineering facilities, and industrial applications. Industrial equipment are unique in their requirement of highly reliable operation in harsh environments.

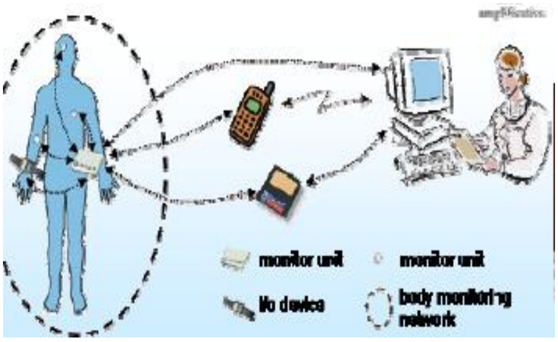

Figure 6 Body Monitoring System

For example, the electromagnetic radiation of machines may cause microcontroller malfunction or wireless communication interference. Also, the large variation in temperature and humidity demands reliable hardware components. Moreover, industrial applications often require the processing of large volumes of data with sophisticated signal processing algorithms. Thus, computation demand is usually high for these applications [3].

Intel Research has deployed a network with 160 Mica2 motes on a ship to measure the vibrations in the ship's pumps, compressors, and engines as an indicator of potential failure. These motes were organized into clusters, with Star gate gateways forming the backbone of the network. Without operator intervention, the deployed network operated for 4 months without major failures. This experiment was still preliminary since the diagnosis of the ship equipments was performed in a centralized way at the base station, instead of distributed within the network. However, it paved the path for WSNs to a broad range of applications in industrial environments.

WSNs can be designed and implemented by taking the specificities of each type of industry into account, and several applications can be identified in this framework. WSNs are capable to monitor the quality of the air, and the temperature of a building or on an oven. Besides, it controls the produced goods, the complex machinery set, and the conditions of the production system of a certain factory or a group of factories.
The following scenarios are related to this area [1]:
● Shopping at the store
● Smart shopping list
● Smart factory.

2.8.1 Shopping at the store

Let A is going to shop in the department store. As she enters the store her intelligent shopping application starts. The shopping list she made during the previous days is uploaded and displayed on her terminal. The system added some items to the shopping list that are needed at home and that A did not check (automatic update of the elementary ingredients for cooking at home, updating of products in the fridge and usual products for housekeeping, etc.). The system guides A through the store aisles to help her locate the products. The system considers the proximity of the products first and also the freshness constraints: fresh products are collected at the end of shopping. While A approaches the products, she gets a ranking of the comparable products that are in the section according to her profile preferences (with criteria like: price, quality, fat-free, organic and allergies to ingredients). It will also include information about the products' prices in other stores. Pointing the RFID reader (integrated in the terminal) at the products she gets additional information about the products such as origin and expiry date. If she takes a product that was not on the list, the device alerts her, for example that it contains nut traces and that it is not suitable for her daughter Lea because of her allergies. The check out and payment are automatic, therefore avoiding the lengthy queues at the check out point.

2.8.2 Smart shopping list

Let B's family is equipped with a system that monitors the family consumption of products (fridge, housekeeping products) thanks to a RFID-based system across their home. The system gathers information about the products' usage at home, the family preferences and behaviour (at least a geo localization system, but also body sensors enabling to monitor physical needs of each family member). The stock level of the food and housekeeping products at home is low. The system infers that a lot of products are needed. The system also notices that the yoghurt has expired. This time fewer types of yoghurt will be ordered. Lea ate all the peaches in one day. The system infers that she likes them and that peaches are good for her (profile, age, physical condition). This time more peaches will be ordered. The system detected that Tom has a bad cold. Tissues are added to the list. Friends are invited for dinner next Saturday (B and A' s diary). The quantity of the products is increased proportionally. The relevant shopping list made by A will be added to the automatic list. The automatic list of the missing/needed products is uploaded on the Internet via a server that submits the list to an e-shopping browser. This browser checks the best prices for the list among several retailers in the area. The products are ordered from a retailer who has the best offers. The delivery date and hour are planned according to B and A ' s availability.

2.8.3 Smart factory

The maintenance of equipment and quality control in a factory. Let A controls the processes of the food processing factory using a WSN-based system. The sensors are installed on the machines and take data about temperature, humidity, vibrations, lubrication, substance (e.g., moisture sensors) and other relevant parameters of the machines. Each sensor node is able to communicate its observations through other nodes to the gateway destination where data from the network is gathered and processed. A is equipped with a mobile device and she has access to the instantaneous values of the sensors. The remote monitoring, remote control, and data exchange is also enabled. A quick diagnosis of conditions will be realized. In case a relevant parameter on a machine is approaching a critical threshold, A will be alerted on her device by an alert message. For example, sensors could detect that the fruit press machine overheats and that the level of lubrication oil is abnormally low. An alert is sent to A with the information about the thresholds and the location of the machine.

3 Conclusion

In conclusion, a WSAN can be generally described as a network of nodes that cooperatively sense the environment and may control it, enabling interaction between people or computers and the surrounding environment. It has a bright future in the field of computer networking because we can solve the monitoring problems at an advanced level in the future with the help of such technology of networking. These days they could be used in every day life in lot of applications life fire forest detection, habitat monitoring. The list is end less.

References

[1] Wireless sensor and actuator networks, Technologies, Analysis and design, Roberto Verdone, Davide Dardari, Gianluca Mazzine, Andrea Conti, Jan 2008, Elsevier.

[2] Monitoring Volcanic Eruptions with a Wireless Sensor Network, Geoffrey Werner-Allen, Jeff Johnson, Mario Ruiz, Jonathan Lees, and Matt Welsh Harvard University,citiseex.ist,psu.edu.

[3] Information processing and routing in wireless sensor networks**,** Dr. Yang Yu, Viktor K. Prasanna, Bhaskar Krishnamachari, V. K. Prasanna Kumar World Scientific, 2006 - Computers.

[4] System for Vehicle Tracking and Autonomous Interception, Cory Sharp Shawn Schaffert Alec Woo Naveen Sastry Chris Karlof Shankar Sastry David Culler, *University of California at Berkeley, USA*, citiseex.ist,psu.edu.

[5] http://www.docstoc.com/docs/7923594/Asset-Tracking-For. IP-based Wireless Sensor Network for Asset Tracking and Management, Jukka Marttila, Sensinode,TechRepublic

[6] Chee-Yee Chong; Kumar, S.P., "Sensor networks: Evolution, opportunities, and challenges,"Proc IEEE, August 2003

[7] Akyildiz, I.F.,W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks",IEEE Communications Magazine, August, 102-114(2002).

[8] http://www.sensornetworks.net.au/applic_health.html

[9] Intel wireless vineyard, www.intel.com/technology/techresearch/research/ rs01031.htm

[10] J. Burrel, T. Brooke and R. Beckwith, “Vineyard Computing: Sensor Networks in Agriculture Production”, Pervasive Computing, IEEE Volume 3, Issue 1, Jan.-March 2004 Page(s):38 – 45.

[11] Polly Huang, “Sensor Networks Solutions to Real Life Problems” http://cc.ee.ntu.edu.tw/ ~phuang.

[12]]N. Tahir, L. Kok-Keongo, “Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks”, *International Journal of Digital Content Technology and its Applications*, Volume 3, Number 1, 2009,pp 89-90.

[13] P.W. Johns, L. Zhengqiang, S. Weisongi, C. Vipin, “Wireless Sensor Network Security: A Survey”, *Security in Distributed, Grid and Pervasive Computing Yang Xiao* (Eds), 2006, pp3-5, 10-15.

[14] Gupta, Munish, Paramjeet Singh, and Shveta Rani. "Cross Layer Energy Efficient Protocols For Wireless Sensor Networks: A Survey.*",Apeejay Journal of Computer Science and Applications”*, Vol. 1, 2013, pp 27-32.