# A Survey: Wireless Sensor Networks

**M. Umashankar**

*Department of Computer Applications, Sona College of Technology, Salem, Tamilnadu , INDIA Email-id: tmus2009@gmail.com*

## Abstract

Wireless sensor networks consists of inexpensive sensor nodes, each node has continuous sensing capability with limited communication power. They can be used for several applications such as commercial, civil, and military applications including vehicle tracking, climate monitoring, intelligence, medical, agriculture, etc. Their deployment in environments disaster areas, earthquake/rubble zones or in military battlegrounds can be seriously affected by any kind of sensor failure or malicious attack/security threats from an enemy. The amount of power carried by the sensor itself is very limited; replacing sensor or sensor battery is a very time-consuming and costly process, in certain application environment. Energy efficient operation, channel contention, latency, management, and security of such networks are complex and critical issues that have to be addressed.

**Key Words : Wireless sensor networks, security, Data fusion.**

## 1. INTRODUCTION

A Wireless Sensor Networks (WSNs) are massively distributed systems consisting of a large number of autonomous, interconnected sensory nodes, which can continuously sense data of locally occurring phenomena (Akyildiz et. al. 2002). They can be deployed on a large scale in resource-limited and harsh environments such as seismic zones, ecological contamination sites or battlefields, etc (Jaydip Sen 2009). Each sensor of a sensor network can be programmed to perform specific function to complement other sensor operations. However, sensor networks are relatively more insecure repository and routers of data, which raises the need for new security schemes. Their deployment in environments disaster areas, earthquake/rubble zones or in military battlegrounds can be seriously affected by any kind of sensor failure or malicious attack/security threats from an enemy. Sensor nodes are self powered and equipped with low computational power CPU allowing the sensor to execute some specific treatment before sending a report to the centralized authority. Therefore, energy saving mechanism is also an important issue for research in WSNs. All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

Wireless Sensor networks have been proposed for a wide variety of application areas, including industrial, military, biomedical, and environmental areas. Some examples of sensor network applications are as follows:

Intrusion detection and tracking: Sensors are deployed along the border of a battlefield to detect, classify, and track intruding personnel and vehicles.

Environmental monitoring: Specialized sensor nodes that are able to detect temperature changes and/or smoke can be deployed in high-risk areas of a forest, to give out early warning of forest fires.

Indoor surveillance: Surveillance sensor networks can be used to provide security in an art gallery, shopping mall, or other facilities. Traffic analysis: Traffic sensor networks can monitor vehicle traffic on a highway or a congested part of a city.

### 1.1 Classification Of Sensor Networks

Sensor networks can be classified into three types based on their mode of operation or functionality and the type of target applications:

**Proactive Networks**

In this scheme the nodes periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest. Thus, they provide a snapshot of the relevant parameters at regular intervals and are well suited for applications that require periodic data monitoring.

**Reactive Networks**

In this scheme the nodes react immediately to sudden and drastic changes in the value of a sensed attribute and are well suited for time critical applications.

**Hybrid Networks**

In this scheme the features of proactive and reactive networks have been combined while minimizing their limitations to create a new type of network called a Hybrid network. In this network, the nodes not only send data periodically but also respond to sudden changes in attribute values.

## 1.2 Wireless Sensor Networks Applications

WSNs applications can be classified into two categories: monitoring and tracking (Jennifer et al. 2008). Monitoring applications include indoor/outdoor environmental monitoring, health and wellness monitoring, power monitoring, inventory location monitoring, factory and process automation, and seismic and structural monitoring. Tracking applications include tracking objects, animals, humans and vehicles. While there are many different applications, below a few example applications that have been deployed and tested in the real environment are discussed.

PinPtr (G. Simon et al. 2004) is an experimental counter-sniper system developed to detect and locate shooters. The system utilizes a dense deployment of sensors to detect and measure the time of arrival of muzzle blasts and shock waves from a shot.

Macroscope of redwood (Tolle.G et al. 2005) is a case study of a WSN that monitors and records the redwood trees in Sonoma, California. Each sensor node measures air temperature, relative humidity and photo-synthetically-active solar radiation.

Semiconductor plants and oil tanker application reported by L. Krishnamurthy et al. (2005) was to focus on preventive equipment maintenance using vibration signatures gathered by sensors to predict equipment failure. Based on application requirements and site survey, the architecture of the network is developed to meet application data needs.

Underwater monitoring study (Vasilescu.I et al. 2005) developed a platform for underwater sensor networks to be used for long term monitoring of coral reefs and fisheries. The sensor network consists of static and mobile underwater sensor nodes. The nodes communicate via point-to-point links using high speed optical communications.

MAX (Yap.K.K et al.2005) is a system for human-centric search of the physical world. MAX allows people to search and locate physical objects when they are needed. It provides location information reference to identifiable landmarks rather than precise coordinates. MAX was designed with the objectives of privacy, efficient search of a tagged object, and human-centric operation.

Connection-less sensor-based tracking system using witness (CenWits) (Huang.J.H, et. al. 2005) is a search-and-rescue system designed, implemented and evaluated using Berkeley Mica2 sensor motes. The system uses several small radio frequencies (RF)-based sensors and a small number of storage and processing devices.

CenWits is not a continuously-connected network. It is designed for intermittent network connectivity. It is comprised of mobile sensors worn by subjects (people), access points that collect information from these sensors and GPS receivers, and location points to provide location information to the sensors. A subject will use the GPS receivers and location points to determine its current location. The key concept is the use of witnesses to convey a subject's movement and location information to the outside world. The goal of CenWits is to determine an approximate small area where search-and-rescue efforts can be concentrated.

Cyclops (Rahimi.M, et. al. 2005) is a small camera device that bridges the gap between computationally-constrained sensor nodes and Complimentary Metal-Oxide Semiconductor (CMOS) imagers. This work provides sensor technology with CMOS imaging. Cyclops contains programmable logic and memory circuits with high speed data transfer. It contains a microcontroller to interface with the outside world. Cyclops is useful in a number of applications that require high speed processing or high resolution images.

Volcanic monitoring (Werner-Allen.G, et. al. 2006) with WSN can help accelerate the deployment, installation, and maintenance process. WSN equipments are smaller, lighter and consume less power. The challenges of a WSN application for volcanic data collection include reliable event detection, efficient data collection, high data rates, and sparse deployment of nodes.

Industrial GS-11 Geophone with corner frequency of 4.5 Hz while the other two sensor nodes carried triaxial Geospace Industries GS-1 seismometers with corner frequencies of 1 Hz. The custom hardware interface board was designed with four Texas Instruments AD7710 analog-to-digital converters to integrate with the T-mote sky devices.

Health monitoring applications (Baker.C.R et. al. 2007) using WSN can improve the existing health care and patient monitoring. Five prototype designs have been developed for applications such as infant monitoring, alerting the deaf, blood pressure monitoring and tracking and fire-Fighter vital sign monitoring. The prototypes used two types of motes: T-mote sky devices and SHIMMER (Intel Digital Health Group's Sensing Health with Intelligence, Modularity, Mobility, and Experimental Re-usability). Because many infant die from sudden infant death syndrome (SIDS) each year, Sleep Safe is designed for monitoring an infant while they sleep. It detects the sleeping position of an infant and alerts the parent when the infant is lying on its stomach. Sleep Safe consists of two sensor motes. One SHIMMER mote is attached to an infant's clothing while a T-mote is connected to BS computer. The SHIMMER node has a three-axis accelerometer for sensing the infant's position relative to gravity. The SHIMMER node periodically sends packets to the BS for processing.

FireLine is a wireless heart rate sensing system. It is used to monitor a fire Fighter's heart rate in real-time to detect any abnormality and stress. FireLine consist of a Tmote, a custom made heart rate sensor board, and three re-usable electrodes. All these components are embedded into a shirt that a fire Fighter will wear underneath all his protective gears. The readings are taken from the T-mote is then transfer to another T-mote connected to the BS. If the fire Fighter's heart rate is increasing too high, an alert will be sent.

Heart@Home is a wireless blood pressure monitor and tracking system. Heart@Home uses a SHIMMER mote located inside a wrist cuff which is connected to a pressure sensor. A user's blood pressure and heart rate is computed using the oscillometric method. The SHIMMER mote records the reading and sends it to the T-mote connected to the user's computer. A software application processes the data and provides a graph of the user's blood pressure and heart rate
over time.

LISTSENse enables the hearing impaired to be informed of the audible information in their environment. A user carries the base station T-mote with him. The base station T-mote consists of a vibrator and LEDs. Transmitter motes are place near objects (e.g., smoke alarm and doorbell) that can be heard. Transmitter motes consist of an Omnidirectional condenser microphone. They periodically sample the microphone signal at a rate of 20 Hz. If the signal is greater than the reference signal, an encrypted activation message is sent to the user. The base station T-mote receiving the message actives the vibrator and its LED lights to warn the user. The user must press the acknowledge button to deactivate the alert.

ZebraNet (Zhang.P et. al. 2004) system is a mobile wireless sensor network used to track animal migrations. ZebraNet is composed of sensor nodes built into the zebra's collar. The node consists of a 16-bit TI microcontroller, 4 Mb off-chip flash memory, a 900 MHz radio, and a GPS unit. Positional readings are taking using the GPS and sent multi-hop across zebras to the base station. The goal is to accurately log each zebra's position and use them for analysis.

## 2 SECURITY REQUIREMENTS

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. The requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to WSNs (John et al. 2006).

### Data Confidentiality

Data confidentiality is the most important issue in network security. In sensor networks, the confidentiality relates to the following (Carman D.W. et al. 2000, A. Perrig et al. 2002):

- A sensor network should not leak sensor readings to its neighbors. Especially, in a Military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore, it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

### Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this does not mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

### Data Freshness

Even if confidentiality and data integrity are assured, it is also needed to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design.

### Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches are chosen to modify the code to reuse as much code as possible. Some approaches are tried to make use of additional communication to achieve the same goal.

### Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

### Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor’s radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. Ganeriwal S. et al. (2005) proposed a set of secure synchronization protocols for sender-receiver, multihop sender-receiver, and group synchronization.

### Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault.

### Authentication

It ensures that the communicating node is the one that it claims to be an adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks. From the above, it can be seen that message authentication is important for many applications in sensor networks, Umashankar et.al. (2010). Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism the sender and the receiver shares a secret key to compute the Message Authentication Code of all communicated data.

## 3. CONCLUSION

Wireless sensor networks are still under development for cost effectiveness, self organization, with the various constraints like power consumption, fault tolerance, environment and topology. We surveyed the architectural and synthesis issues related to wireless sensor networks. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper, we summarize typical applications on wireless sensor networks and surveyed the literatures on several important applications and security issues relevant to the wireless sensor networks.

## References

[1] . Akyildiz I. F., et. al., (2002), "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102–114.

[2]. Jaydip Sen., (2009), "A Survey on Wireless Sensor Network Security" International Journal of Communication Networks and Information Security (IJCNIS), Vol.1, No.2.

[3]. Umashankar M and Chandrasekar C., "Power Efficient Data Fusion Assurance Scheme for Sensor Network Using Silent negative Voting", International journal of Computer Applications, Vol.1, No. 4, pp. 75-80, February - 2010.

[4]. Jennifer Yick, et. al., (2008), "Wireless sensor network survey" , Computer Networks, Vol. 52 , pp. 2292-2301.

[5]. Simon G., et. al., (2004), "Sensor network-based countersniper system", Proceedings of the Second International Conference on Embedded Networked Sensor Systems, Baltimore, MD, pp.1-12.

[6]. Umashankar M ., " Power Efficient Data Fusion Assurance Mechanism for Wireless Sensor Networking", International Journal of Advanced Research in Computer Science, Volume 5, No. 5, May-June 2014, ISSN No. 0976-5697 .

[7]. Tolle G., et. al., (2005), "A macroscope in the redwoods", Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, pp.51-63.

[8]. Vasilescu I., et. al., (2005), "Data collection, storage, retrieval with an underwater sensor network", Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, pp.154-165.

[9]. Yap K. K., et. al., (2005), "MAX: Human-centric search of the physical world", Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, pp.166-179.

[10]. Huang J. H., et. al., (2005), "A sensor-based loosely coupled search and rescue system using witnesses", Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, pp.1-5

[11]. Rahimi M., et. al. (2005), "Cyclops: in situ image sensing and interpretation in wireless sensor networks", Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys), San Diego, CA, pp.192-204.

[12]. Werner-Allen G., et. al., (2006), "Deploying a wireless sensor network on an active volcano", IEEE Internet Computing, Vol.10, pp.18–25

[13]. Baker C. R., et. al., (2007), "Wireless sensor networks for home health care", Advanced Information Networking and Applications Workshops, 21st International Conference on 21-23 May 2007 pp. 832 – 837

[14]. Carman D. W., et. al. (2000), "Constraints and approaches for distributed sensor network security". Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD.