Wireless Sensor Network and their General Issues

Roopal Mishra
Banasthali University
Jaipur,India

Soniya Bhatnagar
Banasthali University
Jaipur,India

ABSTRACT

Wireless sensor networks can be used by various applications such as surveillance, forest management, weather prediction, Avalanche land-slide prediction, road safety, marine movement control, etc. These applications pose a set of common difficulties. Specifically, in the remote large-scale networks, network topology, security, self-configuration, connectivity, maintenance, power management, time synchronization etc. are major challenges. In this paper we present an overview of issues related of wireless sensor networking. Different aspects of sensor networking are discussed and sensor network architecture is proposed that can satisfactorily overcome these problems.

Index Terms

Power management, QOS, Security, Time Synchronization, WSN

1. INTRODUCTION

Wireless sensor network consist of geographically distributed autonomous sensor devices that communicate the sensed information to a central computing centre for data processing. Main components of these networks are sensors, communication setup, and a host system that may be distributed or clustered, client interface and client side network.

With the advancement in the technology, modern wireless sensor networks (WSN) are becoming popular especially in the scenarios where processing or sensing systems are geospatially distributed.

WSN consist of sensors placed as nodes which may be connected to one or more node depending on specific application demanding specific network topology. Placement of sensors is usually guided by the application. Some applications demand the sensor position to be precise and predefined whereas in some other applications statistical analysis of the environment and locations may be required for optimising sensor placement.

In a WSN, the sensor nodes can be deployed in controlled and uncontrolled environment. In controlled surroundings each sensor is directly and easily accessible and its position and configuration is constantly monitored. In case of uncontrolled environment sensors are not easily accessible and are not predefined in terms of configuration or location. They are not regularly monitored.

The network (WSN) in both cases is required to swiftly react to any incidence happening over the area/ system. Security in a WSN is extremely important for both controlled and uncontrolled environment Fig. 1 shows a typical sensor network layout. The major issues related to WSN arediscussed in the remaining sections.General idea about requirements of WSN is described in section II. Section III describes a proposal of WSN based on GSM network. Section IV illustrates architecture of proposed WSN. Section V elucidates applications of sensor networks.

Fig. 1. Typical Wireless Sensor Network environment.

2. REQUIREMENTS

The application under implementation and the extent of functionalities to be embedded are the guiding channels in the design of wireless sensor network. The ideal characteristics of a typical wireless sensor network are scalability, low power consumption, remote configuration of nodes, programmability, fast data acquisition, reliability, security, and fidelity of data flow over the long term and with little or no maintenance [1]. Each of these issues is broadly defined below:

2.1 Availability

Availability ensures that service and information can be accessed at the time that they are required.

2.2 Reliability

The reliability of the network is also of special interest because many applications require the WSN to operate in uncontrolled environment. Reliability in case of a WSN is essentially the capability to maintain the functionality of WSN even if some sensor nodes fail [2].

2.3 Energy Efficiency

The sensors deployed over a WSN and the communicating components used in the WSN are battery operated sensor devices. Energy preservation is an important issue because battery is the source available to power the sensors. Each device which we use should be energy aware and proficient

2.4 Fault tolerance

Failure of one or more nodes should not bring down the entire system. Redundancies to the extent that shall support basic essential operations in the event of isolated devices must be built in.

2.5 Heterogeneity

The entire system should appear as a single unit and the complexity and interaction between nodes should be hidden from end user.

2.6 Scalability

The system should work efficiently without getting affected by increase in the number of nodes.

2.7 Speed of data acquisition

In case of WSN it implies the total process used to collect information and analyze the data to document an observable fact. Information through sensor devices should be accurate and precise. The data shall be available for analysis only after it reaches the server through communication setup. Thus, while estimating the speed of data acquisition the response time of communication channel has to be included for WSN.

2.8 Remote configuration

It implies the process in which a person can alter the setting of remotely located device from local terminal. Possibility of remote configuration must exist in the sensor and software tools must exist in the host.

2.9 Remote programming

It provides the mechanism for modification in sensor program. Again, remote programming feature must exist in the sensor and software tools must exist in the host.

2.10 Quality Of Service

Data type in WSN can be classified as following[3]

2.10.1 Emergency Data

Critical information should be guaranteed to deliver to the gateway with both low delay and high reliability.

2.10.2 Monitoring and tracking

WSN should monitor and track all target with guarantee of low delay until the target become identified.

2.10.3 Periodic simple data

A condition of sensor node such as remaining energy could be simple data type.

For deploying an application over wireless sensor network the necessities of the application under development needs to be analyzed in conjunction with customizes WSN that are available as shown in Fig. 2,. This analysis shall lead to the configurations of application specific WSN well suited for the end use.

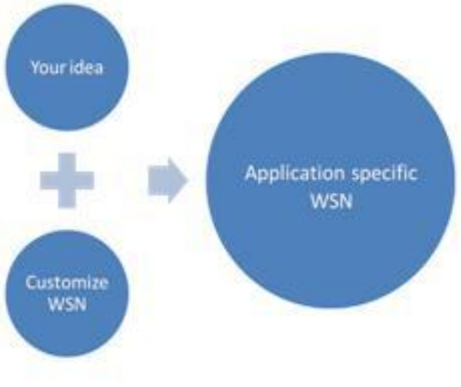

Fig 2. Process of Arriving at application specific WSN

3. USE OF GSM

Two types of communication modes are recommended in WSN for transmitting sensed information. These are RF and GSM based. Chip level components are available for both of them and the communications can be easily integrated with any sensor mechanism. The Radio Frequency (RF) module inserted in the sensor node can be programmed to continue in sleep mode and operate only when GSM module is not able to transmit information. RF communication has the advantage of hopping that provides multiple channels to communicate to the destination node. Ordinarily GSM texting or data can be used for sensor communication and GSM voice channel with FSK may be used for online processing.

GSM systems provide a number of useful features:

1) Uses encryption to make transmission more secure.
2) Data networking.
3) Group III facsimile services.
4) Short Message Service (SMS) for text messages and paging.

4. FACTS ABOUT GSM DATA CALLS

1) GSM modules have on serial communication ports, enabling easy connectivity to either a PC or to an embedded environment.
2) Devices can be programmed to communicate with a remote server for data transfer.
3) The capability of data transfer can help in reducing pre-processing.
4) It provides wireless solution keeping the existing firmware intact.
5) The client firmware continues to work without any modification (no change in the existing software required).
6) GSM data calls also be a good solution where data has to be transmitted from a hand –held device to a central server.
7) The interface on two sides can be between PC’s as well as embedded devices.[4]

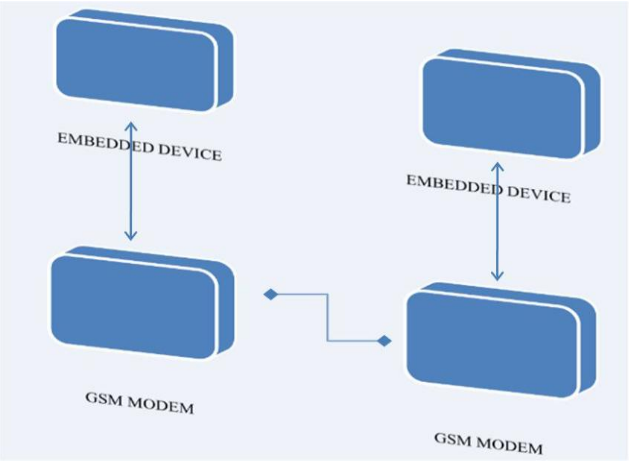

Fig 3. - Schematic for GSM based WSN

5. PROPOSED ARCHITECTURE

The proposed WSN architecture, with heterogeneous sensor devices that are dispersed in remote uncontrolled environment, need to account for all the above listed features. Major issues which need emphatic consideration are reliability, time synchronization, security and power management.

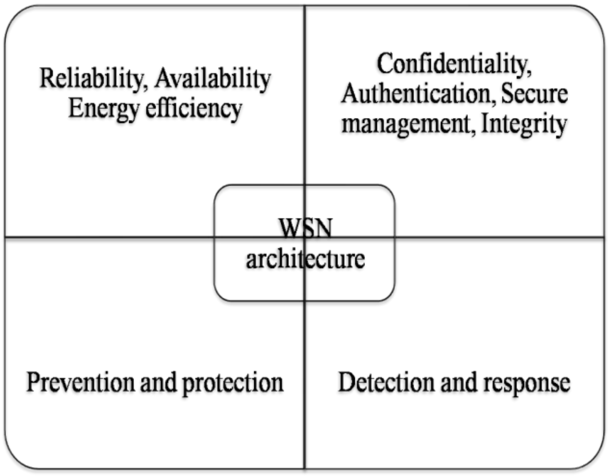
Reliability, Availability Energy efficiency
Confidentiality, Authentication, Secure management, Integrity
WSN architecture
Prevention and protection
Detection and response

Fig.4. - Architectural Overview of GSM

5.1 Reliability

For secure transmission of sensed data over network we employ IEEE802.15.4 standard in wireless sensor network IEEE802.15.4 is a standard that is designed for the requirement of wireless sensing application. The standard supports following characteristics [5].

1) Transmission frequencies, 868MHz/ 902-928MHz/ 2.48-2.5GHz

2) Data rates of 20Kbps (868MHZ band), 40Kbps (902MHz band) and 250 Kbps (2.4 GHz band).

3) Support star and peer to peer (mesh) network connection.

4) Use AES-128 security for encryption of transmitted data.

5.2 Time synchronization

For time synchronization we employ Global System of Mobile (GSM). This uses voice channel for online communication of information. If there is any time variation between the sender and base station it can be corrected without human intervention.

5.3 Security

Security in GSM can be define by the three level of authentication

5.3.1 User level authentication

It can be achieved by identification of user example: caller ID.

5.3.2 Device level protection

At this level of protection we define identification of sensor devices. A preregistered sensor code can be used for identification. The caller ID mentioned above confirms the communication channel, whereas the device identification confirms the sensor connected at the node.

5.3.3 Data Encryption level authentication

At this level of authentication we uses encryption algorithm for sending/ receiving message

Security can be provided by implementing encryption and/ or decryption technique for secure transmission. VLSI chip or microcontrollers at the sensor end can be reprogrammed to further improvise this feature.

5.4 Power Management

Main focus is on increasing battery life at sensor node through power preservation and power Management. One of the suggest way is use of solar panel in the sensor node. The consumption and recharge cycle should be such that scattered sun light should be able to recharge the battery in four hour exposure and the charge should support for forty eight hours.

6. APPLICATIONS

6.1 Distributed process management (E.g. refineries, large scale chemical manufacturing etc.)

At large scale manufacturing like refineries, sensors are placed in distributed locations. The WSN can immensely help in such situation. Sensor/ nodes that communicate to central server with a command/ control software can allow monitoring of the complete environment from a single centre.

It provide monitoring of each event from the starting point of manufacturing to supplying of product like temperature, chemical dispersion, chemical detection, Quality assessment, and all GUI based dataflow in plant. All the abnormalities can be predefined in host software and if any of them is present in the environment it can used to trigger an audio-visual alarm for any defined/ eventual abnormality.

6.2 Forest Resource management

WSN can prove to be an extremely useful tool to protect wildlife and forest resources. The uncontrolled distributed sensor network with sensors for shot/ metallic noise, temperature etc. Can be successfully employed to protect the wild life resources.

6.3 Mining

When underground mine accidents occur, availability of following information could enhance mine safety. Networking of gas sensors, humidity sensors, ultrasound depth measurement devices, SOS gadgets can immensely improve mine security and ensure prompt action from supervising authorities.

7. Acknowledgement

The authors wish to gratefully acknowledge the permission accorded by the Director, Defence Laboratory, Jodhpur; to carry out M. Tech. project work in this institute. Thanks are also due to Mr. R.T. Paturkar and Mrs. Manjulata Sharma for guidance, encouragement, and helpful comment.

8. REFERENCES

[1] Wireless Sensor Network F.L.Lewis Associate Director for Research Head, Advanced Controls, Sensors, and MEMS Group Automation and Robotics Research Institute The University Of Texas at Arlington

[2] A Design For Secure And Survivable Wireless Sensor Networks Yi Qian and Kejie Lu, University of Puerto RICO at Mayaguez David Tipper, University of PITTSBURGH

[3] Wireless Sensor Network Design for Tactical Military Application: Remote Large-Scale Environments Sang Hyuk Lee, Soobin Lee, Heecheol Song, and Hwang Soo Lee Department of Electrical Engineering, KAIST Daejeon, South Korea.

[4] Bioenable is available at http://www.bioenabletech.com/technical_introduction_to_gsm_modem_technology.htm

[5] Wireless Sensor Networks: Principles and Applications, Chris Townsend, Steven Arms MicroStrain, Inc.