ISSN 2278-7763

Management of Wireless sensor networks using cloud technology

Dipankar Mishra, Department of Electronics, Pusa Polytechnic, Pusa, New Delhi, India, Email : conf.mishra@gmail.com

Mrs Geeta Bhatia, Department of Electronics, Pusa Polytechnic, Pusa, New Delhi, India, Email : geetabhatia31@gmail.com

Abstract : Sensor networks are widely used to monitor vital parameters. Providing critical data in any field of application, sensor networks play a vital role in a wide range of applications. Advancement of technology in the field of sensors, wireless networks and VLSI, has resulted in the interfacing of sensors to the Information Technology sector or the “virtual world”. This has resulted in wireless sensor networks being used in a wide range of applications like toxic gas detection, health care, oil industries and environs management.

The monitoring of the wireless sensor networks is still manual in nature. Data from the sensor networks is analyzed at the base station by competent technical persons. Depending upon the situation, sensor nodes of the networks are manipulated manually to provide optimized performance. Manual monitoring comes with its own baggage of human errors. Fatigue, loneliness and other physical and emotional factors affect the performance of the monitoring personnel. This may lead to serious judgmental errors resulting in a critical situation of the system being monitored.

This paper presents a concept of remote and automated monitoring of wireless sensor networks with least amount of human intervention. The result is less human error while increasing the performance of the sensor network.

Keywords : WSN, cloud, network management, optimization of wsn, PSO, WSN management.

Introduction : Rapid advances in the areas of sensor design, information technologies, and wireless networks have paved the way for the proliferation of wireless sensor networks. These networks have the potential to interface the physical world with the virtual (computing) world on an unprecedented scale and provide practical usefulness in developing a large number of applications, including the protection of civil infrastructures, habitat monitoring, precision agriculture, toxic gas detection, supply chain management, and health care. In the past ten years there has been increasing interest in wireless sensor networks. This interest has been fueled, in part, by the availability of small, low cost sensor nodes (motes), enabling the deployment of large-scale networks for a variety of sensing applications [Akyildiz et al. 2002(1)].

A “node” in a wireless sensor network is capable of gathering information, processing and communicating with other connected nodes in the network. Typically the node may contain one or more sensors that can monitor the surroundings for specific parameters. Some of these sensors commonly used are to sense temperature, light, sound, position, acceleration, vibration, stress, weight, pressure, humidity, etc. The sensors measure data of the area

ISSN 2278-7763

to be monitored. The continual analog signal sensed by the sensors is digitized by an Analog-to-digital converter and sent to controllers for further processing. The nodes also contain the communication module which provides communication over wireless medium using transceivers. The nodes can be powered by using batteries. A large number of nodes hence communicate over wireless channel form an ad-hoc network. All the information can eventually be transmitted to a gateway node or base station.

A basic sensor network is shown in figure 1.

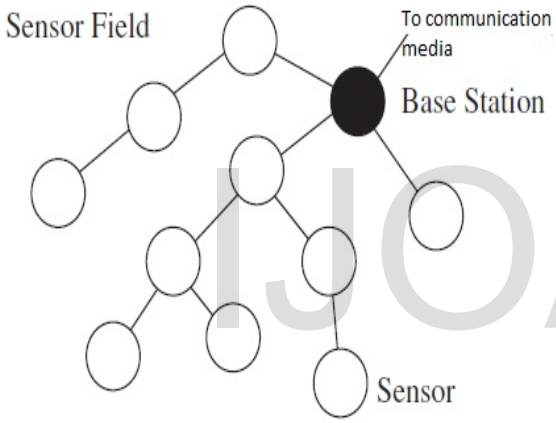

Figure 1

Network topologies : The development and deployment of wireless sensor networks (WSN) have taken traditional network topologies in new directions. Many of today's sensor applications require networking alternatives that reduce the cost and complexity while improving the overall reliability. Four basic types of wireless sensor data network topologies are;

(a) Peer-to-Peer networks allow each node to communicate directly with another node without needing to go through a centralized communications hub. Each Peer device is able to function as both a "client" and a "server" to the other nodes on the network. An example of a Peer-to-Peer network is shown in figure 2.

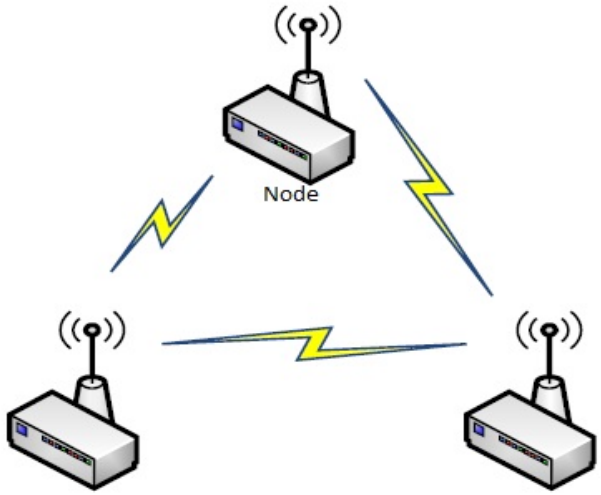

Figure 2

(b) Star networks are connected to a centralized communications hub. Each node cannot communicate directly with one another; all communications must be routed through the centralized hub. Each node is then a "client" while the central hub is the "server". An example of a **Star** network is shown in **figure 3**

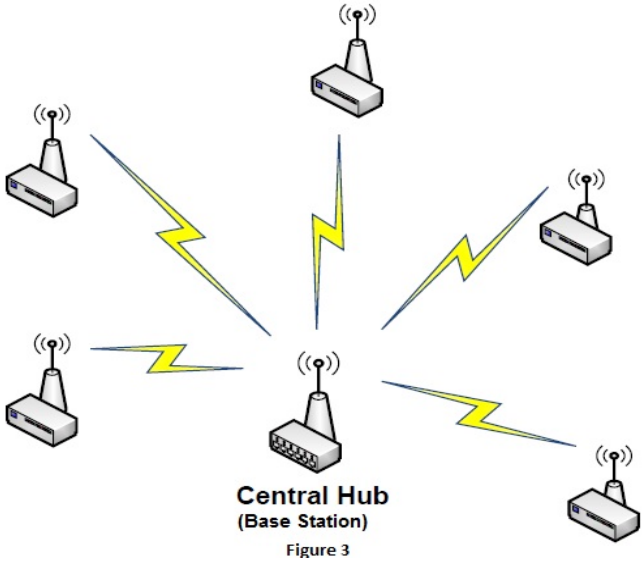

Figure 3

ISSN 2278-7763

(c) **Tree** networks use a central hub called a *Root* node as the main communications router. One level down from the *Root* node in the hierarchy is a *Central* hub. This lower level then forms a **Star** network. The **Tree** network can be considered a hybrid of both the **Star** and **Peer to Peer** networking topologies. An example of a **Tree** network is shown in **figure 4**.

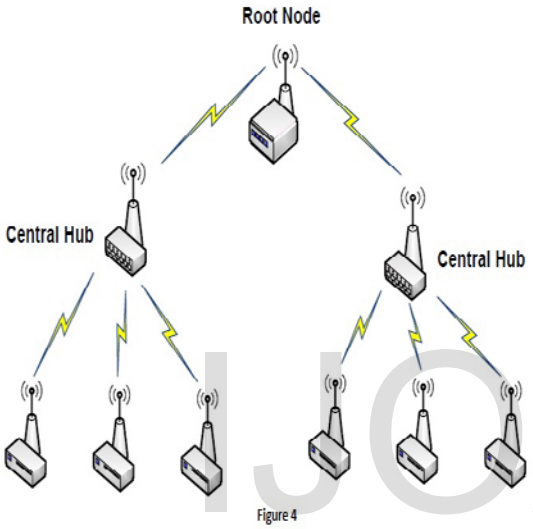

Figure 4

(d) **Mesh** networks allow data to "hop" from node to node, this allows the network to be self-healing. Each node is then able to communicate with each other as data is routed from node to node until it reaches the desired location. An example of a **Mesh** network is shown in **figure 5**. This type of network is one of the most complex and can cost a significant amount of money to deploy properly.

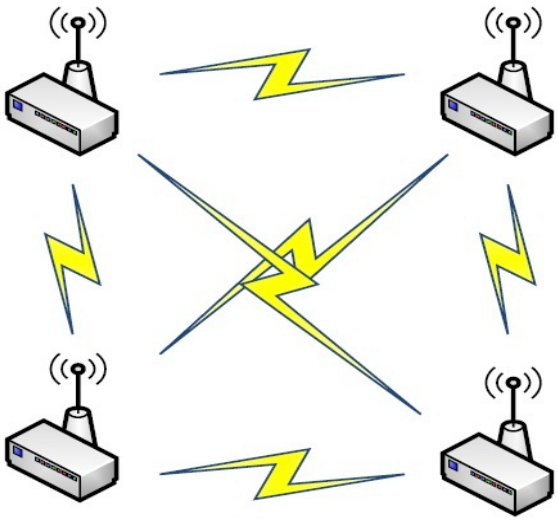
Figure 5

Network Management : Network management is the process of managing, monitoring, and controlling the behaviour of a network. Wireless sensor networks (WSNs) pose unique challenges for network management that make traditional network management techniques impractical. Thus a managing infrastructure is one of the most basic requirement for monitoring and controlling such networks [2].

A network management system can be defined as a system with the ability to monitor and control a network from a central location. Ideally there are four key functional areas that this system must support [3]:

(a) Fault Management: This area provides the facilities that allow the discovery of any kind of faults that the managed devices of the network will produce, determining in parallel the possible causes of such errors. Thus, the fault management function should provide mechanisms for error detection, correction, log reports and

ISSN 2278-7763

diagnostics preferably without the user interference.

(b) Configuration Management: Responsible for monitoring the entire network configuration information and also having access to all the managed devices in terms of reconfigure, operate and shut down if necessary.

(c) Performance Management: Responsible for measuring the network performance through analysis of statistical data about the system so that it may be maintained at an acceptable level.

(d) Security Management: This area provides all those facilities that will ensure that access to network resources cannot be obtained without the proper authorization. In order to do so, it provides mechanisms for limiting the access to network resources and provides the end user with notifications of security breaches and attempts.

Approaches to monitoring : The dominant methods that are generally followed are ;

(a) Passive Monitoring: The system role is to collect data during the lifetime of the network. The data will identify the state of the network in different time intervals without any action taking place during the data gathering. An analysis of the data will take place in later stages.

(b) Fault Detection Monitoring: The system dedicates its resources to identifying faults and errors during the lifetime of the network. All the information is gathered and reported back to the operator whose responsibility is to correct those problems in later stages. No action is taken by the system towards the resolution of those problems in real time.

(c) Reactive Monitoring: The system has a double role to accomplish during the lifetime of the network. Firstly, as we identified in the previous approaches, the collection of data that will provide information about the states of the network, is the main role. This time though, the system will be eligible to identify and detect any events and act upon them in real time mainly by altering the parameters of the fixed asset under its control.

(d) Proactive Monitoring: The system collects and analyzes all the incoming data concerned with the state of the network. Then an analysis is taking place similar to the one of the reactive monitoring with the big difference that certain events, de-scribed by the collected information, are stored. The system is then able to maintain better available network performance by predicting future events based on past ones.

Present Scenario: In the present scenario of WSN management, most network resort to either fault management or performance management. Some complex networks manage both. In both the scenarios, human intervention is the most crucial part. Analysis, detection and correction are all done manually with the help of IT systems. Automation is limited. The approach mainly consists of passive monitoring with some portion of fault detection monitoring. Data analysis of

ISSN 2278-7763

the sensor networks is done by the IT systems and depending on the analysis results, corrective procedures are adapted or performed. The corrective procedures may involve dropping of nodes from operation, enhancing or degrading the node parameters in manual mode.

Pros and Cons

1. The methods are less complex and relatively easy to implement
2. Cost effective methods
3. Human efficiency matters.
4. Fatigue and emotional disturbances affect the performance.
5. Time lag in analysis and implementation. May be a huge factor in critical applications.

Cloud Technology: Cloud technology, a recent development in the field of Information technology, is widely being used by the industries. It helps lower infrastructure cost, reduces deployment time while providing the latest of the services and infrastructure at a fraction of the traditional models.
As the area of cloud computing was emerging, the systems developed for the cloud were quickly stratified into three main subsets of systems: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

(a) Software as a Service (SaaS). The target user of this subset of systems is the end user. These applications, which we shall refer to as cloud applications, are normally browser based with predefined functionality and scope, and they are accessed, sometimes, for a fee per a particular usage metric predefined by the cloud SaaS provider. Some examples of SaaS are sales force customer relationships management (CRM) system [4], and Google Apps [5] like Google Docs and Google SpreadSheets.

SaaS is considered by end users to be an attractive alternative to desktop applications for several reasons. For example, having the application deployed at the provider's data center lessens the hardware and maintenance requirements on the users' side. Moreover, it simplifies the software maintenance process, as it enables the software developers to apply subsequent frequent upgrades and fixes to their applications as they retain access to their software service deployed at the provider's data center.

(b) Platform as a Service (PaaS), the provider supplies a platform of software environments and application programming interfaces (APIs) that can be utilized in developing cloud applications. Naturally, the users of this class of systems are developers who use specific APIs to build, test, deploy, and tune their applications on the cloud platform. One example of systems in this category is Google's App Engine [6], which provides Python and Java runtime environments and APIs for applications to interact with Google's runtime environment. PaaS class is generally regarded to accelerate the software development and deployment time. In turn, the cloud software built for the cloud platform normally has a shorter time-to-market.

(c) Infrastructure as a Service (IaaS). This class of systems,

ISSN 2278-7763

according to the SPI classification model, provides infrastructure resources, such as compute, storage, and communication services, in a flexible manner. IaaS providers control and manage efficient utilization of the physical resources by enabling the exploitation of both time division and statistical multiplexing, while maintaining the familiar and flexible interface of individual standard hardware computers and networks for the construction of services using existing practices and software.

Proposed Setup The proposed setup is shown in figure 6.

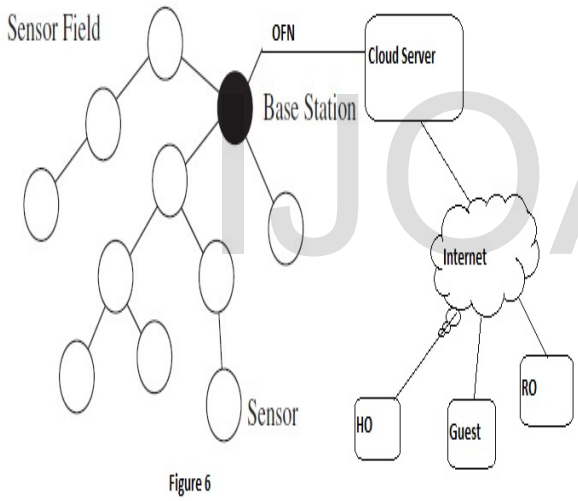

Figure 6

The base stations are connected to a cloud server through optical fiber network (OFN). The cloud server is connected to the Internet or Intranet of the company or office. The different locations from where monitoring is to be done are connected to the cloud server through Internet/Intranet.

The cloud server interfaces the nodes and the base stations with the ability to operate and manipulate the nodes with the capabilities of a base station. It can enhance the transmission power, shut down a node or shut down a node transmission.

The optimization algorithm, PSO, Ant colony or any genetic algorithm is executed in this server on a real time basics 24x7. The input parameters of the nodes that need to be monitored, communication, information, are continuously monitored on a real time basis. Depending upon the output of the optimization algorithm, the nodes are manipulated for increasing their lifespan.

Pros and Cons.

1. Being automated, the system is free of human errors during monitoring.
2. Non stop monitoring can increase the lifespan of the nodes manifold by conserving energy of the nodes on a real time basis.
3. Manpower requirement at hostile and remotely located base stations is reduced.
4. Any changes in requirement and operation can be implemented from either the head office (HO) or by the expert or at the regional office (RO) level through the public Internet or private Intranet medium.
5. On the flipside, security of the system can be compromised with intrusions being a possibility over the Intranet/ Internet medium.
6. Any mis-constructed algorithm effect cannot be isolated from the system.
7. Cloud server failure can be catastrophic as the same can damage the system beyond repair.

Conclusion: The proposed setup is highly effective in terms of increasing the effective lifespan of the WSN. A

ISSN 2278-7763

proper optimization algorithm can increase the efficicieny of the WSN to a level that cannot be matched by the manual monitoring model. Security issues are a concern in critical application areas, but these issues can be managed with a proper hardware security system in place. The proposed system can, in the long run, reduce costs, making it economically viable.

References : 1. Akyildiz, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E. 2002. A survey on sensor networks. IEEE Communications Magazine 40, 8 (August), 102–114.
2. Cisco Systems, “Network management systems organiza-tion,” 2000,
3. W. Stallings, “Wireless communications and networks,” ISBN-10: 0131918354, pp. 45–50, 2004
4. Salesforce Customer Relationships Management (CRM) system. http://www.salesforce.com
5.Google Apps. http://www.google.com/apps/business/index.html
6.Google App Engine. http://code.google.com/appengine

