Design Considerations for a Self-Managed Wireless Sensor Cloud for Emergency Response Scenario

Nithya Gopalakrishnan Nair  Philip J. Morrow  Gerard P. Parr
IU-ATC, School of Computing and Information Engineering
University of Ulster, Coleraine, UK
gopalakrishnnair-n@email.ulster.ac.uk, {pj.morrow, gp.parr}@ulster.ac.uk

Abstract—Wireless Sensor Networks (WSNs) have become widely used in various applications areas including environmental monitoring, surveillance and military applications. As the complexity of WSNs increase and the application areas in which they are used become more critical, the requirement of such networks to be self managing becomes necessary. Various aspects of a WSN like power management, event management, data aggregation, connectivity management, polling etc. have to be performed automatically by the sensor cloud. In this paper we give a brief taxonomical overview of the elements that influence the design of a WSN with reference to emergency response / critical applications. We also look at different scenarios that could occur and the various housekeeping functions each sensor node would adopt as part of the self management requirement of such a sensor cloud.

Key Words - Wireless sensor networks; self-management.

I. INTRODUCTION

Wireless Sensor Networks comprise of sensor nodes scattered across a large area. The nodes interact with their surrounding environment and have inherent communication and computational capabilities. WSNs are widely used in low bandwidth and delay tolerant applications such as healthcare monitoring [1]. Designing a WSN would mainly depend on the constituent nodes where each node has the principal task of computation, storage, collection and sensing. The sensor node consists of a controller which processes the data gathered by the sensor which is the interface to the physical world. The node would also contain memory to store programs and data. It also would have a radio device to communicate with a gateway or the backhaul network. An important component of the sensor node is the power supply which is required to perform any sort of operation in the node.

The characteristics of a WSN are that it is a multi hop wireless communication network, performs energy efficient operations to increase life time of the network and has auto configuration capability as there may be a number of nodes that could join the sensor cloud or nodes that shut down due to insufficient battery power [2]. A WSN also has a data centric communication approach as there are redundancies in the network in order to avoid network failure, because of which, identity of a particular node is irrelevant.

In recent years, the demand for WSNs has increased and research into the field has led to widespread use of WSNs in critical infrastructure monitoring /management and also in the area of emergency response applications. This has led to the requirement of designing better power, data and communication management techniques for the WSN.

There are several characteristics that are desirable in a wireless sensor network such as higher quality of service, higher fault tolerance, scalability of the network, lower power consumption/ better power management, better security, programmability, ease of maintenance and lower costs [2][3]. Depending on the application, certain characteristics hold precedence over others. In applications where random deployment of sensors occurs, the sensor node could be dropped from an aircraft or by means of artillery shells. Hence, the systems should be robust. If it is used in an application where accessibility is a problem, techniques to reduce the energy consumption should be adopted and also methods to replenish energy should be put in place. Reprogramming capability would also be required to improve flexibility in topology and scalability. In the case of data sensitive applications, access control along with message integrity, confidentiality and replay protection would be characteristics that would hold utmost importance.

The remainder of the paper is organised as follows: Section II gives some background information and a brief overview of related work across the literature; Section III provides an outline of different scenarios that may transpire within a WSN; Section IV identifies issues that need to be addressed in the different scenarios and proposes suitable design objectives and Section V provides conclusions and discusses planned future work.

II. BACKGROUND

The various elements that contribute to the design of a sensor network are the protocols used, data fusion techniques, operating systems, middleware, topology, deployment methods, polling and communication standards. As we are looking at self managed wireless sensor networks, the key elements, in light of critical infrastructure applications / emergency response scenarios are now discussed.

Table I shows the various elements, domains and applications in which WSNs are being used, each of which are reviewed below. Working from the table we have:-

A. Protocols

The protocol stack used by WSNs is divided into several planes including power, connection and task management planes [4]. Based on the management planes, protocols can be classified into routing or network protocols [5][6], MAC
protocols [7], Transport protocols [4][8] and several other protocols depending on their functions, for example power conservation mechanism [4], target tracking [9], network management [10], node clustering [4] and time synchronization [4] algorithms.

Routing protocols, depending on the network structure, protocol operation (i.e. proactive, reactive or hybrid), network flow and nodal constraints (such as energy, memory and computing power) have been categorized into Flat-Based routing (SPIN, Directed Diffusion) [6], Hierarchical-Based (LEACH, PEGASIS), QOS-Based (Breath - a self-adapting protocol, Minimum Energy Relay Routing - MERR), Location-based (SPAN, GOAFR) and Bio Inspired (Minimum Ant-based data diffusion tree algorithm) routing protocols [5]. Transport protocols for WSN are designed to deal with packet-loss and congestion as a result of the limited bandwidth and convergence of upstream data. They are classified into congestion control and reliability guarantee protocols (e.g. SCTP-Stream control transmission protocol, ART- Asymmetric Reliable Transport Mechanism) [8]. MAC layer protocols are needed to prolong the life time of the network and so energy efficiency has been the main requirement for protocol design. Thus MAC protocols currently available depend on duty cycle control techniques (S-MAC, TMAC), random access (B-MAC, CSMA/p*) and fixed access (ER-MAC) or a hybrid of both (Z-MAC) [7][11].

B. Data fusion/aggregation

A WSN is characterised by a node that is constrained on resources like energy, communication and computational capabilities and storage etc. The energy consumption in such WSNs is crucial and is mainly associated with the sensing, processing and communication functions. In order to improve the efficiency of data collection, bandwidth utilization, energy consumption, network lifetime, data fusion techniques need to be incorporated [12]. Examples of data fusion techniques used are aggregation tree related algorithms, relevance data processing, distributed database query methods, mobile agent based data fusion and processing according to message categories and data compression.

C. Operating Systems

The operating system (OS) forms a link between the simple hardware and complicated applications [13]. Design of an OS for a WSN depends on the resource constraints of a sensor node. The desired characteristics within an OS suitable for a wireless sensor node are that it should have a small footprint due to the memory constraints, be energy efficient due to limited battery life and be reliable to ensure proper functioning of the sensor node. The OS should also provide real-time guarantee as WSN may be used in scenarios like disaster management, emergency response etc. where real-time data processing would be required in addition to re-

<table>
<thead>
<tr>
<th>CRITICAL AREAS</th>
<th>OIL, GAS, WATER</th>
<th>ENVIRONMENT</th>
<th>RAILWAYS</th>
<th>POWER</th>
<th>TELECOM</th>
<th>ROADWAYS</th>
<th>SMART HOME/ MEDICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATIONS</td>
<td>Monitoring of oil wells</td>
<td>Indoor Air Pollution monitoring</td>
<td>Track monitoring,</td>
<td>Monitoring distribution</td>
<td>Monitoring link monitoring</td>
<td>Traffic Monitoring</td>
<td>Track a person’s</td>
</tr>
<tr>
<td></td>
<td>Water distribution monitoring</td>
<td>Underground water level</td>
<td>Train Tunnel Monitoring, Traffic</td>
<td>transformers, Monitoring power</td>
<td>Resource monitoring</td>
<td>Vehicle detection</td>
<td>behaviour through</td>
</tr>
<tr>
<td></td>
<td>Fault Detection</td>
<td>monitoring</td>
<td>scheduling</td>
<td>cables</td>
<td></td>
<td></td>
<td>actions</td>
</tr>
<tr>
<td></td>
<td>Corrosion Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Monitor health</td>
</tr>
<tr>
<td>PROTOCOLS</td>
<td>Routing, Transport, MAC protocols, Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>synchronization algorithms, network management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>protocols, target tracking, power</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>conservation, Node clustering algorithms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA FUSION</td>
<td>Aggregation tree based, Relevance data processing,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distributed Database Query method, Mobile Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Based Data Fusion, Processing according to message</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>categories, data compression</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPERATING SYSTEMS</td>
<td>TinyOS, Contiki, SOS, Mantis OS, Nano-RK, RETOS,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Magnet OS and LiteOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIDDLEWARE</td>
<td>Mate, MagnetOS, Sensorware, Sina, TinyDB, Cougar,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MiLAN, AutoSec, Reflective, Tiny Cubus, Tiny Lime,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agilla, Impala, DS Ware, Mires</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOPOLOGY</td>
<td>Star, Mesh, Ring, Tree, Peer to peer, Ad-Hoc, Hybrid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEPLOYMENT METHODS</td>
<td>Planned, Random, Depending on the application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMM. STANDARDS</td>
<td>Bluetooth, Zigbee, IEEE 802.11, IEEE 802.15.4,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WiBree, IEEE 1451, UBW, GSM, UMTS, WiMAX, ISA100,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wireless HART, IETF RPL, 6LoWPAN, EnOcean, EnviroNet,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MyriaNed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HARDWARE</td>
<td>WeC, Rene1, Rene2, Dot, MITes, Teleos, Mica, Mica2,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
configurability to provide ease of scalability to the WSN. Examples for sensor network OSs are TinyOS, Contiki, Mantis OS, Magnet OS and LiteOS.

D. Middleware

Middleware is an extension of the software used within the sensor node which is utilized by the WSN and the user applications [14]. It serves as the link between the network/OS and the applications and is responsible for managing resources and filtering and transmitting events. It provides standard interfaces, abstractions and services based on the applications while hiding the internal workings and heterogeneity of the system. Middleware provides support for development, maintenance, deployment and execution of WSN applications. It not only provides support to sensor networks but also covers the devices and networks connected to the WSN as well. There are several desirable characteristics that need to be incorporated when designing middleware for a wireless sensor node [15] including hardware resource management, scalability, network topology maintenance, network organisation, application knowledge, etc. Some examples of middleware used for sensor networks are SINA, MiLAN, Tiny Lime and Mires [16].

E. Topology

There are a number of different topologies that are used with wireless sensor networks. The three main types are the Star topology (Single point-to-multipoint), Mesh topology and Hybrid topology (Star-Mesh Topology). By adopting a hybrid network a versatile communication network can be achieved while maintaining lower power consumption. In this topology, the lower power sensors are not capable of forwarding information. They act as remote nodes within a star network with the base node being at a higher power level capable of multi-hop. An example of a hybrid network is Zigbee [17].

F. Deployment methods

Sensor deployment depends on the type of sensor, environment and application and is classified as being either deterministic or random [18]. A deterministic deployment is required when the cost of the sensor is high and their operation is significantly influenced by the location. For example, underwater applications or indoor applications. Random deployment is used where the cost of nodes is not of high priority and also where the environment is harsh as in the battle field or in disaster areas. The factors on which node deployment depends include area coverage, network connectivity and longevity and data reliability. Other deployment strategies available depend on the functions of the node as well.

G. Communication Platforms

There are several communication platforms available for use in WSNs. The platform or standard chosen depends on the environment in which it is deployed and also the application [19][20]. Zigbee and Wiobee can be used in applications which require short range, low energy communication. Bluetooth can be used in short range (100m), random deployments as the transceivers are not expensive. IEEE 802.11 is used in applications that require high data rate (upto 54Mbps) and long distance communication (250m).UBW is used for low energy, short range communications as well. GSM, UMTS, WiMAX are suitable for long range, low data rate applications. Some of the application specific platforms are ISA100, WirelessHART used for industrial control and process monitoring applications, IETF RPL, 6LoWPAN used for transmission for IPv6 packets, EnOcean, EnviroNet, MyriaNed used for environmental, medical and building automation.

H. Hardware

A wireless sensor node can be described as a part of an autonomous network dispersed over a large area which uses sensors to monitor physical or environmental conditions e.g. temperature, sound, vibration, motion, pressure, etc. [21] The node functions either as a gateway that passes all the data to the collection point or as a node that collects the data, processes it and transmits. The other factors that need to be taken into consideration when choosing a sensor node are its physical size and cost [22]. Examples of sensor nodes are WeC, Renel1, Rene2, Dot, MITes, Teleos used for large scale environmental monitoring and Mica, Mica2, Ant used in industrial applications [22].

The elements discussed here consider the various design aspects of a WSN under normal conditions. As mentioned earlier, we are interested in considering the problems that arise when using a WSN for emergency responses. Hence, we take a look at the routing, power, event and topology management along with the sensing frequency, data aggregation and message passing operations in different scenarios as discussed in the following section.

III. WIRELESS SENSOR NETWORK SCENARIOS

In this paper, we examine a number of different scenarios that wireless sensor networks deal with. We assume that the WSN is deployed for event monitoring application such as earthquake, landslide or flash flood detection. We first take a look at the ideal world situation where the events management, power management, data management, and communication and polling methods are considered. This provides a baseline for future comparison with the subsequent real world scenarios. The real world scenarios discussed here are similar scenarios that could occur within Ad-Hoc wireless networks.

A. Ideal World (Scenario 1)

In the ideal world, there is no possibility of loss of connectivity, shortage of data storage or energy available to the sensor. Sensor nodes can be deployed randomly or in a deterministic manner and are connected to the gateway / base
station which is connected to the core network. No disruption in communication links occurs and minimalistic power management and data aggregation techniques are adopted. Polling occurs at a set interval until an event occurs.

Figure 1. Illustration of an Ideal World scenario

Once an event is triggered, the polling frequency is increased to determine if it was random or not. If an event trigger is received for more than a set number of times, an alert is sent upstream to the core network.

B. Real World Scenarios

In the real world, anything can go wrong. Here we take a look at two main types of scenarios as shown in figures 2 and 3 which can be further divided into two subsections each depending on their housekeeping functions discussed in Section IV.

1) Scenario 2: Dynamic topology where there is a break in the connection between the node and gateway but the connection to backhaul still exists.

Case (i): When the sensor goes out of range and loses connectivity or loses connectivity due to some other reason.

Case (ii): The house keeping functions that needs to be adopted by a sensor node and the corresponding gateway, when another sensor node that has no connectivity to the base station gets in range and requests that data gathered by it is sent upstream to the gateway.

2) Scenario 3: Dynamic topology where backhaul connection is lost to a gateway.

Case (i): When a gateway loses connectivity with the backhaul or to the bridging gateway.

Case (ii): The house keeping functions that needs to be adopted by a sensor node and/or a gateway when another gateway that has no connectivity to the backhaul gets in range and requests a route to the backhaul.

Figure 2. Illustration of the scenario where a sensor would lose connectivity to the gateway.

Figure 3. Illustration of the scenario when a gateway loses connectivity to the backhaul through a bridging gateway.

Each of these scenarios gives rise to a number of issues which must be considered if continuous operation of the WSN is to be maintained. The various management operations the wireless sensor network would have to perform are routing power and event management, sensing management, topology management, data aggregation and message passing processes. Each scenario discussed here would have different operating intervals for each of the management processes. Taking the case of power management, the frequency at which the power management operation takes place within an isolated subnet (consisting of several nodes connected to a gateway which has lost connectivity to the backhaul) would be higher than the frequency at which power management would take place in an isolated node.

IV. DESIGN OBJECTIVES

Several issues arise from the real world scenarios that have been discussed in the previous section. They are mainly power management, data management and aggregation, topology management etc. These issues give rise to several design objectives that are discussed below.

A. Scenario 2 Case (i)

In the case where a sensor loses connectivity either due to moving out of transmission range of the gateway or because of some fault in the gateway, there are several housekeeping processes that would have to be carried out. Initially it could reduce the polling frequency to conserve storage space and power until such time when it could transmit the collected data upstream. Depending on the energy reserves, it could scan its
surroundings to check for a gateway or another sensor node present within transmission range.

In the occurrence of an event triggering, the sensor would have to increase its polling frequency and store the data in the expectation that when a link is established at any time through a gateway or another sensor with a link to the backhaul, it could send the recorded data upstream. If the situation is such that the memory on the sensor is running short, then the oldest data it had would be deleted to make space for the most recent recordings. Data aggregation is necessary in this situation since the link to the backhaul may be established either through a gateway or through another node and they would have their own data that would need to be transmitted upstream. When considering the energy aspect, if in an emergency situation, if the sensor energy is depleted, data gathering would be of utmost priority. In such a case, it would have to forego the link to the gateway and adopt a shorter distance communication like (Bluetooth or IR) to save on transmission energy.

B. Scenario 2 Case (ii):

When a neighboring sensor node (SN1) has lost connectivity to its gateway as discussed above, it would try and establish connection with another gateway or another node that has connectivity to the backhaul. In this case, the sensor node (SN2) or gateway that has the link to the backhaul would need to perform certain housekeeping functions to be able to accept the new addition to the network. Power management would be of utmost importance in this case for SN2 as it would have to establish a link with SN1 as well as maintain the existing link to its gateway. Also energy would be needed to do aggregation of data received from SN1 in order to transmit it upstream. Data aggregation would be necessary on SN2’s own data in order to accommodate the excess of data needed to be transmitted to the gateway. If SN2 is able to establish a connection directly to a gateway then the gateway would have to do further data aggregation and also let the sensor nodes present in the network know about the addition to the network.

C. Scenario 3 Case (i):

The case where a gateway loses connectivity to the backhaul is very similar to the case where a sensor node loses connection to the gateway. The main difference here is the level of data aggregation that is required. In this scenario, when an event occurs and the sensors associated with the linkless gateway have a considerable amount of data to send upstream, data management and in turn energy management becomes an issue.

Data aggregation would need to take place at both the sensor node and gateway but at a higher level. The gateway as well as the sensors linked to the gateway scan for other sensors or gateways in the vicinity to establish a connection to the backhaul. The sensors that would be assigned the task of scanning for other nodes or a gateway would be the ones that have higher energy reserves whereas the nodes with lower energy levels would poll for data.

D. Scenario 3 Case (ii):

This is an extension of Scenario 2 Case (ii) where a gateway e.g. (G1) or a sensor node (SN1) with a link to a gateway that has no connection to the backhaul requests a connection to a gateway (G2) or to a sensor node (SN2) linked to a gateway that has connectivity to the backhaul. As is the case with the scenarios discussed previously, SN2 or G2 will have to perform power management to compensate for the addition to the network. Data aggregation has to be done at higher levels as the data from an entire subnet would have to be transmitted upstream. The bridging node (SN2) would be chosen according to the energy levels and the amount of free memory available.

The issues discussed here are in conjunction with an event occurrence where there would be large amounts of data needed to be collected by the sensors and transmitted to the backhaul. The main issues identified are power efficiency and data management. As in previously mentioned scenarios, the sensor could be isolated for long periods of time which could result in the sensor running out of power and storage and also when a link is re-established, in order to transmit the collected data, aggregation techniques would need to be adopted. The different types of protocols and data aggregation techniques discussed in section II will be applicable to these situations for power management and data management.

From these scenarios and the identification of the issues to be addressed, we can propose a number of design objectives for a resilient WSN:

- Efficient power management techniques required to conserve energy in isolated nodes.
- Alternate communication methods need to be chosen to reduce the transmission power
- Data aggregation is required to reduce the transmission load when re-routing traffic.
- Data management needed to conserve storage space in isolated nodes.

The aim of the project is to develop a novel energy efficient data aggregation technique which would be employed in designing a Wireless Sensor Network for fast response applications like disaster management etc.

V. CONCLUSION AND FUTURE WORK

We have investigated the various aspects of designing a self manageable network and also the different scenarios and the issues related with each scenario. Further planned work includes testing of hardware setups which consists of Libelium Waspmotes along with simulation of a larger network using the different protocols, middleware, topologies, data.
aggregation techniques that exist currently. In the case where self management is not achieved, a mechanism may need to be devised in order to achieve a fully self managed wireless sensor network. We have also proposed a number of design objectives which should be addresses when designing a resilient WSN.

ACKNOWLEDGEMENT

The authors wish to thank Dr. Basim Majeed, EBTIC, ETISALAT BT Innovation Centre, UAE for his valuable comments and suggestions.

REFERENCES


