International Journal on Emerging Technologies (Special Issue on ICRIET-2016) **7**(2): 293-298(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Resource Management in Wireless Sensor Network

Anand Rakshe, B. Prasad, V. Akshay and C. Channaveer
Department of Electronics & Communication Engineering,
BKIT, Bhalki, Karnataka

(Corresponding author: Anand Rakshe)
(Received 28 September, 2016 Accepted 29 October, 2016)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Sensor network is the most recent and most ongoing research. The data retrieved by the sensors are large and they have to be managed properly to enhance the network lifetime. Usually sensor networks are operated by battery power and have very less computational power. Resource management is the process to which the data are processed sufficiently and managed as per the requirements. Many algorithms have been proposed for the resource management in sensor network. This paper gives the review of existing resource management schemes and their comparison.

Keywords: Resource Management, Sensor node, energy, data retrieval.

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using Sensors to co-operatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutions at different locations. These sensors networks are formed by hundreds or thousands of modes that communicates with each other and pass data along from one to another. Wireless sensor network (WSN) consists of a number of sensor nodes and one or more sink nodes. A sensor node senses its environment and collects data which is sent to the sink node. The sink node processes data received from sensor nodes. The processes data may be automatically interpreted to action or it may be displayed to the user for making decision about the environment. Resource management is the efficient and effective deployment and allocation of an organizations resource when and where they are needed. Such resources may include financial resources, inventory, human skills, production resources, or information technology. The expectation of resource management in wireless sensor network (WSN) has been the investigated based on the premise of resilient architecture and communication paradigms of WSN's with autonomous nodes that are typically small in size, equipped with computational and communication capabilities, and the flexibility of coordinated and self healing operation there was much to expect. coupled with remote operation and significant research covering its operation in terrines so far deemed inaccessible, the push for adopting WSNs continues to rise; both in diversity and quantity. There are no cost boundaries and margins of feasibility for real-life adoption of WSNs. The core problem of design in WSNs understanding the environment the network will operate in, the available resources (nodes, their cost, components and their accuracies, etc), lifetime expectancy among other requirements, the involvement in operation and required maintenance. The design process is complicated by Coupling between application requirements and interfaces, and the underlying components and topology. To bridge the gap between applications and architectures, the field of middleware in WSNs has evolved as an interface. Protocols residing in the domain of middleware focus on abstracting the resource available in a node, and porting their functionality to the application layer in the nodes operational stack. This forms a decoupling strategy to better exposure of network resources to aid in their utilization at the design phase.

II. COMPONENTS OF WSN

A Wireless sensor networks consist of three main components:

- Nodes
- Gateways and
- Software

The spatially distributed measurement nodes interface with sensor to monitor assets or their environment.
Tiers Sensor nodes Gateways, Repeaters Application Service Field comm.
Out-of-field communication.

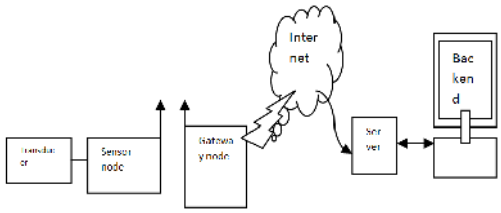

Fig. 1. WSN Architecture.

The components of a wireless sensor network enable wireless connectivity within the network, connecting an application platform at one end of the network with one or more sensor or actuator devices in any part of the network. As shown in Fig. 2, using specific components such as gateways and nodes, a transparent data path is created between the application platform and the physical world. Wireless sensor networks are used to exchange information between an application platform and one or more sensor nodes. This Exchange takes place in a wireless fashion. In the example of Fig. 2, the data path between the gateway and the node is referred to as a single-hop network link. To extend the range of a network or circumvent an obstacle, a wireless relay node can be added between a gateway and a leaf node, making a mesh network, as shown in Fig. 3. In this example we represent a multi-hop data path, in which data packets are sent from one node to the next node before reaching their destination (gateway, other node. Now we will describe each network component illustrated in Fig. 3 (gateway, relay node, leaf node and sensor/actuator) [5].

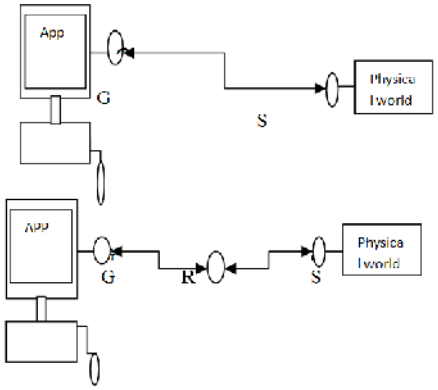

Fig. 2. Network Components.

Issues [4]

- Sensor nodes are randomly deployed and hence do not fit into any regular topology.
- Sensor network are infrastructure-less. Therefore all routing and maintenance algorithm need to be distributed.
- Sensor usually rely only their battery power.
- Sensor nods should be able to synchronize with each other.
- Sensor network should be capable of adapting to changing the connectivity due to the failure, or new powering up.
- Hardware and operating system for WSN
- Wireless Radio Communication characteristics.
- Medium Access Schemes
- Deployment
- Localization
- Synchronization
- Calibration
- Data Aggregation and data dissemination
- Architecture
- Programming models for Sensor Networks
- Middleware
- Quality of Service
- Security

Advantages of WSN

- It avoids a lot of wiring
- It can accommodated new device at any time
- Its flexible to go through physical partitions
- It can be accessed through a centralized monitor
- Network setups can be carried out without fixed infrastructure
- Suitable for the no0n reachable places such as over the sea, mountains, rural areas or deep forest

Disadvantages Of WSN

It is easy for hackers to hack it as we can't control propagation of waves

- Comparatively low speed of communication
- Gets distracted by various elements like Bluetooth
- Still costly at large
- This has enable the mankind to excel in every field of the life, but at the same time it has any threats as well
- Wireless is a public frequency network therefore its interface is highly risky to be used for official private information
- The speed and the viability of the wireless signals drop as more users use the same frequency

Application Of WSN [1]

- Military application: WSN is used to monitor the resources, track enemies and targets, to assess the damage, detection of attacks such as nuclear, biochemical etc.
- Environmental application: WSN is used to monitor the weather conditions, soil conditions, in precision agriculture, forest fire detection, and Volcano, Flood and pollution detection.

- Home application: Sensors are buried in the appliances to help automate. Aids in ease to Manage and monitor these appliances locally or remotely.
- Medical applications: The Sensors can be implanted or attached to the patient to observe the Physiological parameters and other conditions and provide appropriate treatment at the right time.
- Industrial monitoring applications: To monitor the condition of the structures, bridges, tunnels, machinery used in industry. To estimate wear and tear.
- Inventory control applications: Inventory monitoring, to keep track of the items in the inventories. To check the supply chain system
- Vehicle tracking: Location estimation of the vehicles
- Smart spaces
- Process monitoring
- Disaster relief operations
- Air pollution monitoring
- Water quality monitoring
- Data center monitoring
- Data logging
- Waste water monitoring
- Structural health monitoring

Resource Management in WSN

Due to the critical resource constraints, it is important to optimize the utilization of the deployed resources (e.g., sensor nodes) for reliable communication in wireless sensor networks (WSNs). One of the main challenges is to develop a scalable and distributed method to identify the resource deficiency and redundancy and also control the corresponding scheduling/balancing activities within a local area, i.e., a cost-effective localized solution for the maximum-minimum problem. In wireless sensor network, resource constrained nodes are expected to operate in unattended high dynamic environments. Hence, the need for adaptive and autonomous resources/task. Management in wireless sensor networks is well recognized. We present Distributed Independent Reinforcement Learning (DIRL), A Q learning based framework to unable autonomous self learning /adaptive applications with inherent support for efficient resource/task management. The proposed scheme based on DIRL, learns the utility of performing various tasks over time using mostly local information at nodes and uses the utility value along with application constraints for task management by optimizing global system wide parameter like total energy usage, network life time etc…

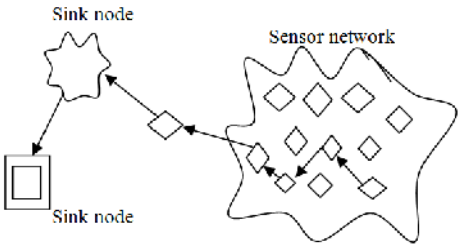

Fig. 3. Wireless Sensor Network Scenario[1].

Security

Security in sensor networks is as much an important factor as Performance and low energy consumption in many Applications. Security in a sensor network is very challenging as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, and burglaral arms and in critical systems such as airports and hospitals. Since sensor networks are still a developing technology, researchers and developers agree that their efforts should be concentrated in developing and integrating security from the initial phases of sensor applications development; by doing so, they hope to provide a stronger and
Complete protection against illegal activities and maintain stability of the systems at the same time.
Following are the basic security requirements to which every WSN application should stick to

- Confidentiality is needed to ensure sensitive information is well protected and not disclosed to unauthorized third parties. Confidentiality is required in sensor networks to protect information traveling between the sensor nodes of the network or between the sensors and the base station; otherwise it may result in eavesdropping (to listen security to someone's private conversation) on the communication.
- Authentication techniques verify the identity of the participants in a communication. In sensor networks it is essential for each sensor node and the base station to have the ability to verify that the data received was really sent bya trusted sender and not by an adversary that tricked regular nodes into accepting false data. A false data can change the way a network could be predicted.
- Lack of integrity may result in inaccurate information. Many sensor applications such as pollution and healthcare monitoring relay on the integrity of the information to function; for e.g., it is unacceptable to have improper information regarding the magnitude of the pollution that has occurred.
- One of the many attacks launched against sensor networks is the message reply attack where an adversary may capture messages exchanged between nodes and reply them later to cause confusion to the network.

So sensor network should be designed for freshness; meaning that the packets are not reused thus preventing potential mix-up.

- In sensor networks secure management is needed at the base station level, since communication in sensor network ends up at the base station. Issues like Key distribution to Sensor nodes in order to establish encryption and routing information need secure Management. Also, clustering techniques require secure management as well, since each Group of nodes may include a large Number of nodes thatneed to be authenticated with each other and exchange datain a secure manner.
- Security and QoS are two opposite poles in sensor networks. Security mechanisms like encryption should be lightweight so that the overhead is minimized and should not affect the performance of the network. Different types of threats in sensor networks are Spoofing and altering the routing information, passive information gathering, node subversion, sinkhole attacks, Sybil attacks, Denial of service attack and jamming.

Netonline Algorithm [2]

Net Online is a distributed low-complexity algorithm heuristically developed for maximizing the throughput over a finite time horizon, in a sensor network with energy replenishment.

The main motivation for this development is the fact that, while the finite-horizon throughput optimization problem can be formulated as a convex optimization problem, its solution suffers from high complexity brought about by strong dependence of current decisions in future performance, time coupling property.

The Net Online algorithm is comprised of two stages:

(1) Finding a through-put maximizing energy allocation through T slots,

(2) Routing.

In part (I), it is assumed that the energy replenishment (energy harvesting) profile can be estimated (predicted) for that period, ahead of time.

Then, based on these estimations and current amount of recharging (harvesting), determine the energy to be allocated for each slot.

In Part (2), the main concern is to determine the amount of data in the outgoing links of each node for the corresponding destination node in time slot.

The routing in each slot is determined by solving a simple linear programming (LP) problem.

Since the defined problem is also a convex optimization problem, the authors use duality and the Lagrange multiplier method to get the optimal solution.

The Net Online algorithm is shown to be optimal under homogeneous replenishment profiles with perfect estimation for all nodes. In a time-slotted system, if energy is overused in a previous period, the total through-put attainable over the time horizon will decrease as a result. On the other hand, if energy is underused in a previous period, the total throughput will also decrease, even though there is no wasted energy.

The shortest path is calculated using the linear time algorithm in, whose complexity is O (T).

Performance close to optimal.

Quick Fix/Snapit Algorithms [2]:

QuickFix and SnapIt were proposed as two different algorithms thatwork in tandem, to maximize the network utility, i.e., the sum of the utility functions of the nodes, with the aim of achieving proportional fairness in a slotted-time system. The system is designed in such a way that the time during a day is broken into multiple time intervals called epochs, where each epoch consists of Tslots.

Quick fix is an efficient dual decomposition and sub-gradient method based algorithm that operates within each epoch, to reveal the feasible region and the optimum solution differing in each epoch.

Quick Fix offers a distributed solution that does not require any knowledge of the future recharging rates. Moreover, it can efficiently track instantaneous optimal sampling rates (for every slot) and routes in the presence of time-varying recharging rates. However, Quick Fix's solution to the proposed utility maximization problem depends on the average (long term) energy replenishment rate of a node and not the state of the battery.

Hence, if fluctuations in recharging happen at a faster time-scale than the convergence time of Quick Fix, undesired battery outage and overflow scenarios may arise, causing missed samples and lost energy harvesting opportunities respectively.

Therefore, Liu et. al. introduce a localized scheme called Snap It that uses the current battery level to adapt the rate computed by Quick Fix with the goal of maintaining the battery at a target level, i.e., chosen as the half of the local battery state in.

Snap It chooses the rate, independently at each node i based on the current state of the battery as follows: the rate found by QuickFix is reduced by δi(different for each node) if the battery is less than half full, and, is increased by the same amount when it is more than half full. We refer the interested reader to, for the effect of δ on the performance of Quick Fix/SnapIt. In, Quick Fix/SnapIt is compared to a modified version of IFRC (Interference-aware Fair Rate Control), a backpressure-based protocol, which aims to achieve max-min fairness in WSNs.

The results show that the two algorithms, working in tandem, can increase the total data rate at the sink by 42% on average when compared to IFRC, while significantly improving the Network utility.

Algorithms For High Performance Scheduling In a WSN [7]

The scheduling algorithm determines the order in which the application requests submitted at the proxy node will be scheduled. The performance of the proposed algorithms is compared with the First Come First Served (FCFS) scheduling algorithm. The FCFS scheduling algorithm is a knowledge free algorithm. It does not use any information about the characteristics of the various applications while scheduling job requests corresponding to the various applications. With the FCFS algorithm, the application requests are scheduled in the order in which they arrive at the proxy. The job requests corresponding to an application request are sent to the wireless sensor network in the order in which the corresponding application request arrives at the proxy. This research investigates the importance of using knowledge based scheduling as compared to knowledge free scheduling and the gains in performance that can be achieved by using knowledge of application and/or the knowledge of network while making scheduling decisions.

Two simple algorithms:

- Least Number of Sensors First (LNSF) and
- Least Number of Hops First (LNHF)

➢ LNSF algorithm:

Uses information only about the number of sensors required by the applications and schedules requests for applications in non-decreasing order of the number of sensors required by the applications. The application indicates the area to be monitored and the phenomenon to be monitored associated with the application. Using this information and the accuracy of measurement required, the proxy can determine the number of sensors required to serve an application request.

➢ LNHF algorithm:

Uses information about network alone while scheduling requests for applications. The requests for applications for which the required sensors are placed closer to the cluster head of a clustered WSN are scheduled first. The LNHF algorithm schedules the application requests in non-decreasing order of the average distance of the

Sensors required by an application from the cluster head. This algorithm does not use any information about the number of sensors required by the applications. The performance of the algorithms is compared in terms of overall mean response time. Mean Response Time is the mean of the response times of the application requests submitted to the proxy. Response time of an application request is the difference between the times the proxy receives the last response for a job request corresponding to an application request from a sensor and the time when the application request arrives at the proxy.

The performance of LNSF and FCFS is compared. Both the applications vary in their resource requirements. The two applications require 25 and 40 sensor nodes respectively.

The LNHF algorithm demonstrates a better performance than the FCFS algorithm and provides a better overall mean response time.

Two classes of algorithms are considered:

- ➢ Knowledge based and
- ➢ Knowledge free.

FCFS is a knowledge free algorithm that schedules the requests in the order in which they arrive. Knowledge based algorithms either use knowledge of applications or network or both the knowledge of application and network while making a scheduling decision and following are the scheduling algorithms

- ➢ Least Number of Sensors First (LNSF) algorithm takes scheduling decisions based only on the number of sensors required by the applications and
- ➢ Least Number of Hops First (LNHF) algorithm takes scheduling decisions based on the average distance of the sensors required by the applications from the cluster head.

Algorithms	Distributed/ Centralized/Node level	Prediction	Type of Allocation	Batter Buffer (finite,infinite)	Harvesting Method
QuickFix/SnapIt 42%	Distributed	No	Rate	Finite	Solar
NetOnline	Distributed	Assumes	Energy	Finite	Solar
Scheduling	Node	Assumes	Resource	Finite	Solar

The LNSF and the LNHF algorithms have been prevents to be suitable for networks hosting. Network topology in scheduling leads to a performance improvement is an important question.

- ➢ Least Number Distance Product First (LNDPF) algorithm,
- ➢ Least Farthest Number Distance Product First (LFNDPF) algorithm, and
- ➢ Least Weighted Farthest Number Distance Product First (LWFNDPF) algorithm:

It is combine the knowledge of the network and application while making a scheduling decision. The priority queue maintains separate queues based on the number of priority levels of the packets.

III. CONCLUSION

In this paper some of the issues and algorithms related to resource management of depicted here.

The review report shows that few algorithms have good resource management and enhances the network lifetime. From review it has been observed that high performance scheduling in WSN is better presently.

REFERENCES

[1]. Shantala Devi Patil1, Vijaya Kumar B P, "Overview of Issues and Challenges in Wireless Sensor Networks", International journal of Application or Innovation in Engineering & Management (IJAIEM), May 2016 ISSN 2319 - 4847

[2]. Neyre Tekbiyik, Elif Uysal-Biyikoglo, "Resource Management and Scheduling in WSN's", Powered by Ambient Energy Harvesting, This work was supported by TUBITAK Grant.

[3]. PI: Zhen Jiang," A new method for resource management in wireless sensor networks".

[4]. Gowrishankar. S, T. G. Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in Wireless Sensor Networks", *Proceeding of the World Congress on Engineering 2008* Vol. **1**WCE 2008, July 2-4, 2008, London, U.K.

[5]. J. Cecílio, P. Furtado, "Wireless Sensors in Heterogeneous Networked Systems, Computer Communications and Networks", DOI 10.1007/978-3-319-09280-5_2, © Springer International Publishing Switzerland 2014.

[6]. Navdeep Kaur Kapoor, M.A.Sc (ECE), B.E (EE), "Resource Management in Wireless Sensor Networks Hosting Multiple Applications", ©2013