A Perspective Analysis of routing protocols in wireless sensor network

V.Vasanthi[1], P.Nagarajan[2], B.Bharathi[3] and Dr.M.Hemalatha[4]

[1, 2&3] Research Scholars, Department of Computer Science, Karpagam University
[4] Assistant professor, Dept of Software Systems, Karpagam University, Coimbatore- 21

Abstract

The Recent Advances in Wireless Sensor Networks which have led to many new protocols specifically designed for sensor networks where energy awareness is an essential consideration. It is necessary to identify the performance challenges of WSN and analyze their impact on the performance of routing protocols. It surveys recent routing protocols for sensor networks and presents a classification for the various approaches pursued. Due to the limited processing power, finite power available to each sensor node, regular ad hoc routing techniques cannot be directly applied to sensor networks domain. These energy-efficient routing algorithms suitable to the inherent characteristics of these types of networks are needed. Routing algorithms must also be robust to failures, and provide low latency. This paper makes a performance comparison of three sensor network routing protocols, namely, Rumor routing, Stream Enable Routing (SER) and SPIN (Sensor Protocols for Information Via Negotiation). These protocols are classified on the based on data-centric, hierarchical and location-based. The performance of these protocols are compared by Simulation Parameters like Agents per Events, Agent TTL, Query Delivery, Cycle rate

Keywords— Rumor routing, Stream Enable Routing (SER), Sensor Protocols for Information Via Negotiation(SPIN).

I. INTRODUCTION

As the popularity of the laptops, cell phones, PDAs, GPS devices, RFID, and intelligent electronics in the post-PC era, computing devices have become cheaper, more mobile,

more distributed, and more pervasive in daily life. A wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components. These components are integrated on a single or multiple boards, and packaged in a few cubic inches. With state-of-the-art, low-power circuit and networking technologies, a sensor node powered by 2 AA batteries can last for up to three years with a 1% low duty cycle working mode.

Sensor nodes are responsible for self-organizing an appropriate network infrastructure, often with multi-hop connections between sensor nodes. Location and positioning information can also be obtained through the global positioning system (GPS) or local positioning algorithms. This information can be gathered from across the network and appropriately processed to construct a global view of the monitoring phenomena or objects.

In September 1999, WSNs were identified by Business Week as one of the most important and impactive technologies for the 21st century [31]. Also, in January 2003, the MIT's Technology Review stated that WSNs are one of the top ten emerging technologies [125]. In December 2004, a WSN with more than 1000 nodes was launched inFlorida by the ExScal team [61], which is the largest deployed WSN to date. In order to find out about users' experiences with such privacy policies, a small analysis was conducted for this paper that which of the routing protocol is suited for which network.

I 1.1 CHALLENGES ARE FACED BY WSN

Recent advances in micro-electro-mechanical systems and low power and highly integrated digital electronics have to be in the development of micro-sensors. These sensors are generally equipped with data processing and communication capabilities. The sensing circuitry measures ambient conditions related to the environment surrounding the sensor and transform them into an electric signal. Processing such a signal reveals some properties about objects located, events happening in the vicinity of the sensor.

The sensor sends such as collected data and files, usually via radio transmitter, to a command center (sink) either directly or through a data concentration center (a gateway). The decrease in size and cost of sensors, resulting from such technological advances, has fueled interest in the possible use of large set of disposable unattended sensors. Here, interest has motivated intensive research in the past few years addressing the potential of collaboration among sensors in data gathering and processing and the coordination and management of the sensing activity and data flow to the sink. Sensor nodes are constrained in each energy supply and bandwidth.

Such constraints are combined with a typical deployment of large number of sensor nodes have posed many challenges to the design and management of sensor networks. The challenges necessitate energy awareness at all layers of networking protocol stack.

I 1.2 CLASSIFICATIONS OF ROUTING PROTOCOLS IN WSN

The routing protocols can be classified as follows

- Data-centric, hierarchical/location based although there are few distinct ones based on network flow or quality of service awareness.
- Data-centric protocols are query-based protocol and it depend on the naming of desired data, which helps in eliminating many redundant transmissions.
- Hierarchical protocols aim at clustering the nodes , cluster heads can do some aggregation and reduction of data in order to save energy.
- Location based protocols is utilized the position information to relay the data to the desired regions rather than the whole network.

The last category includes routing approaches that are based on general network-flow modeling and protocols that strive for meeting some QoS (quality of service), requirements along with the routing function. This paper is to help better understanding of the current routing protocols for wireless sensor networks and point out open issues that can be subject to further research. It concludes with a comparative summary of the surveyed approaches and points out open research problems.

II. ROUTING CHALLENGES AND DESIGN ISSUES IN WSN

In general, routing in WSNs can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure. In addition to the above, routing protocols can be classified into three categories, namely,

- Proactive protocol
- Reactive protocol
- Hybrid protocol

These protocols depending on how the source finds a route to the destination. In proactive protocols, all routes are computed before they are really needed. In reactive protocols, the routes are computed on demand. Hybrid protocols uses the combination of these two ideas.

When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols. Another class of routing protocols is called the cooperative routing protocols.

In order to streamline this survey, I use a classification according to the network structure and protocol operation (routing criteria). The classification is shown in Figure 1

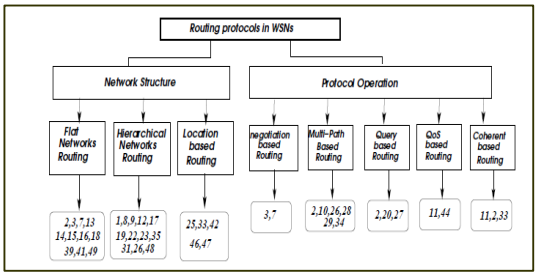


Fig 1: Routing protocols in WSNs : A taxonomy

In this paper we will present three different protocols is compared. Flat type rumor routing protocols are the multi-hop at routing protocols. Due to the large number of such nodes, it is not able to feasible to assign a global identifier to each node .Data is being requested through queries, attribute based naming are necessary to specify the properties of data. Rumor routing is controlled by different parameters used in the algorithm such as time-to-live (TTL) pertaining to queries and agents. Since the nodes become aware of events through the event agents, the heuristic for defining the route of an event agent highly affects the performance of next hop selection in rumor routing.

The SPIN family of protocols used the data negotiation and resource-adaptive algorithms. The main disadvantage of SPIN is to send data for same nodes. Gossiping avoids the problem of implosion by just selecting a random node to send the packet to rather than broadcasting the packet blindly. However, it causes delays in propagation of data through the nodes. In SPIN3-stage protocol messages are used to communicate.

- SPIN-BC: This protocol is designed for a broadcast channels.
- SPIN-PP: This protocol is designed for a point to point communication, hop-by-hop routing.
- SPIN-EC: This protocol works similar to SPIN-PP, with an energy heuristic added to it.
- SPIN-RL: When a channel is lossy , a protocol called SPIN-RL is used where adjustments are added to the SPIN-PP protocol to account for the lossy channel.

The SER Routing protocol requires the sinks to specify the sensor nodes that perform the tasks in their instructions. If the nodes do not have a global positioning system (GPS), then they can use a location awareness protocol. To analyze these three protocols wireless sensor simulator v.1 is used. The paper also presents future

trends of research.

IV. RELATED WORKS

The new architectural techniques inspired some previous efforts for surveying the characteristics, applications and communication protocols for such a technical area [1, 13]. In this subsection I highlight the features that distinguish our survey and hint the difference in scope. Although a number of routing protocols for sensor networks are covered, this paper does not make a classification for such routing protocols and the list of discussed protocols is not meant to be complete given the scope of the survey.

Sensor networks are classified by considering several architectural factors such as network dynamics and a data delivery model. Such classifications are helpful for a designer to select the appropriate infrastructure for his/her application. However, this paper neither describes any routing protocol nor talks about the potential effects of infrastructure design on route setup. It is a dedicated study of the network layer, describing and categorizing the different approaches for data routing. In addition, I summarize different architectural design issues that may affect the performance of routing protocols.

The main challenge of this paper is to discover new protection techniques that can be applied to existing routing protocols, without forfeiting connectivity, coverage or scalability. Perrig et al [38] made a first attempt to design its secure protocols for sensor networks. This protocol is known as SPINS: (Security protocols in Sensor Networks) provides data authentication, replay protection, semantic security and low overhead. This work has been turned to use the secure cluster based protocols such as LEACH [39].

Karlof and Wagner [15] has provided an extensive analysis on the routing vulnerabilities of WSNs and possible countermeasures. According to their study, common sensor network protocols are vulnerable due to their simplicity and then security should be built into these protocols during design time. In particular, their study targets of TinyOs beaconing, directed diffusion and geographic routing. Although this study is the basic for much of the research to follow, the attacks they focus on are still theoretical and have not been implemented practically on any type of hardware.

V. ROUTING TECHNIQUES IN WSN

A Wireless Sensor Network (WSN) contains hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy. In Figure 2, shows the schematic diagram of sensor node components. Basically, each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units (some of these components are optional like the mobilizer). The same figure 2 shows the communication architecture of a WSN. A base-station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data

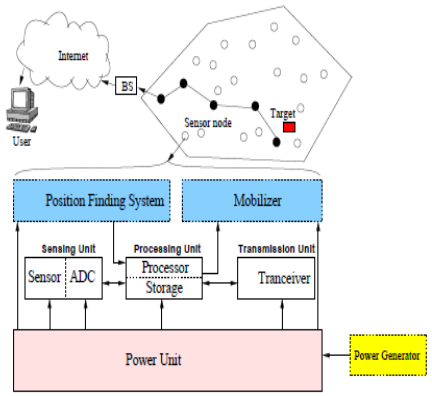


Fig2: The components of a sensor node

Networking unattended sensor nodes may have profound effect on the efficiency of many military and civil applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management.

VI. RUMOR ROUTING

Rumor routing [14] is a variation of directed diffusion and is mainly intended for applications where geographic routing is not feasible. In general, directed diffusion uses flooding to inject the query to the entire network when there is no geographic criterion to diffuse tasks. However, in some cases there is only a little amount of data requested from the nodes and thus the use of coding is unnecessary. An alternative approach is to flood the events if the number of events is small and the number of queries is large.

The key idea is to route the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about the occurring events. In order to flooding events through the network, the rumor routing algorithm employs long-lived packets, called agents. When a node detects an event, it adds such event to its local table, called events table, and generates an agent. In order to propagate information in agents travels the network about local events to distant nodes. When a node generates a query for an event, the nodes that know the route, may respond to the query by inspecting its event table. Hence, there is no need to flood the whole network, which reduces the communication

cost.

Rumor routing maintains only one path between source and destination as opposed to directed diffusion where data can be routed through multiple paths at low rates. Simulation results showed that rumor routing can achieve significant energy savings when compared to event flooding and can also handle node's failure. However, rumor routing performed well only when the number of events is small. For a large number of events, the cost of maintaining agents and event-tables in each node becomes infeasible if there is not enough interest in these events from the BS. Moreover, the overhead associated with rumor routing is controlled by different parameters used in the algorithm such as time-to-live (TTL) pertaining to queries and agents. Since the nodes become aware of events through the event agents, the heuristic for defining the route of an event agent highly affects the performance of next hop selection in rumor routing. The greedy's shortest path algorithms are usually better.

Nodes do not have any distinct identification numbers or knowledge of their neighboring nodes identifications then flooding needs to be used.

Nodes is been having a hierarchy of different transmission abilities.

Rumor routing's beneficial range between two thresholds of number of queries per event is demonstrated in figure 3

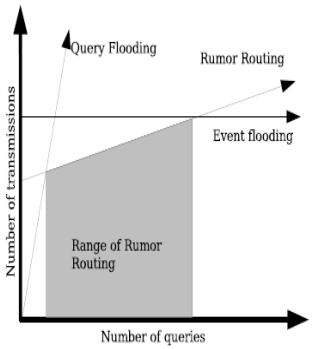


Fig 3: Rumor Routing Range

VII. Stream Enable Routing (SER)

The routing protocol requires the sinks to specify the sensor nodes that perform the tasks in their instructions. If the nodes do not have a global positioning system (GPS), then they can use a location awareness protocol, such as [12], to approximate their locations. SER can be integrated with the application layer very easily, because it is based on instructions or tasks. Instead of assigning attributes to a task as in [7], an instruction is predefined as an identifier value. This way only the identifier is sent and not the whole attribute list in order to conserve memory.

.

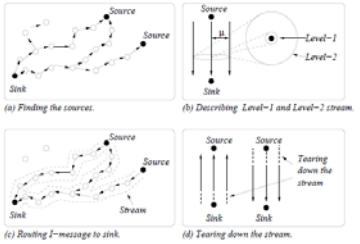
One of the advantages is that it can be integrated with the application layer easily since it is based on instructions and tasks. An instruction is defined as an identifier value. This conserves memory because only the identifier is sent rather than the whole attribute list.

There are four types of messages that are sent through the network, such as

- information message (Imessage)
- scout message (S-message)
- neighbor-neighbor message (N-message)
- update message (U-message)

The S-message is broadcast for the sources to select routes between themselves and sinks based on the quality of service requirements of the instructions. SER also takes into account the memory limitations of nodes, energy of nodes, and the QoS of the instruction. After the routes are established, the sink node can give new instructions to the sources without setting up another route.

Overview of SER protocol:



(a) To find the sources that will carry out the instruction specified in the S-message.

(b) The combination of type and level of routes gives rise to a new concept called stream.

(c)The streams are selected then the source sends an N message to establish the streams back to the sink.

(d) Both sink and sources can also terminate the streams by the U-message

VIII. Sensor Protocols for Information via Negotiation (SPIN)

Sensor Protocols for Information via Negotiation (SPIN) are a family of protocols used to efficiently distribute information in a wireless sensor network. Conventional data dissemination approaches such as flooding and gossiping waste valuable communication and energy resources by sending redundant information throughout the network.

In addition, these protocols are not resource-aware /resource-adaptive. SPIN solves those shortcomings of conventional approaches using data negotiation and resource adaptive algorithms. Nodes running in SPIN, assign a high level name to their data, called meta-data,

and perform meta-data negotiations before any data is transmitted.

The SPIN family of protocols is using a three messages for communication are.

ADV: When a SPIN node has some new data, it sends an ADV message is to its neighbors containing metadata (data descriptor).

REQ: When a SPIN node wishes to receive the data, it sends an REQ message.

DATA: These are actual data messages with a metadata header.

The SPIN family of protocols is made up of four protocols,

SPIN-PP: (a three–stage handshake protocol for point-to-point media).

SPIN-EC: (SPIN-PP which has low energy threshold).

SPIN-BC: (a three–stage handshake protocol for broadcast media).

SPIN-RL: (SPIN-BC for a lossy networks).

Motivation of SPIN

Dissemination is the process of distributing individual sensor observations to the whole network, treating all sensor protocol as sink nodes

- Replicating complete view of the environment
- Enhance fault tolerance
- Broadcast critical piece of information.
- Limited supply of energy
- Energy-Conserving communication and computation
- Limited computational power
- Sophisticated network not suitable
- Limited communication resources
- Communication bandwidth is limited to a few hundred Kbps

IX. PERFORMANCE ANALYSIS

This Wireless Sensor Network Simulator v1.1 is a simulation of a wireless sensor network used to conduct assessment of performance. Such a network is used to detect and report certain events across an expanse of a remote area i.e., a battlefield sensor network that detects and reports troop movements [1]. This application is a simulation of wireless sensor network described hereinabove. The network may be deployed based on a wide range of parameters like network size (number of nodes), communications distance, energy costs for transmitting and receiving packets, etc. The network can be used to simulate the detection of vectors traveling across the sensor network field. In this simulation, when a vector trips the sensor of a network node and the node are generates a data packet and sends it to a downstream network node.

The application has the ability to run successful testes on a network and report the mean network lifetime across 1,000 trials. The network routing parameters can be tweaked to allow testing of different network configurations. This application is worked in simulation on a wireless sensor network. Such a network is used to detect and report certain events across an expanse of a remote area (ie., a battlefields sensor network that detects and reports troop movements).The idea behind this network is that it can be deployed simply by scattering sensor units across that are communications packets toward a data collector.

This simulation consists of two stages:

- Deploying the network.
- Running the simulation.

Before deploying the network, the properties of the network should be set using the configuration sliders.

The network configuration properties are grouped into two categories:

1. Network Configuration: These factors determine the hardware properties of the network. The following variables can be configured:

- Network Size: The number of nodes in the network.
- Sensor Radius: The proximity range of the sensors in the network.
- Sensor Period: The delay period between sensor detection events
- Sensor Cost: The energy cost in detecting a vector and generating a packet.
- Transmission Radius: The maximum distance within which two network nodes can communicate.
- Transmitter Period: The amount of time required to send a packet.
- Transmit Cost: The energy cost in sending a packet.

2. **Routing Parameters**: These factors determine the software properties of the network: essentially, the packet-routing method to be used. If routing is set to "Random," each node selects a downstream connection randomly for each packet. If set to "Directed," the network routes packets based on the algorithm described in the Chang and Taissulas article[5].

When the network parameters are set, the network can be deployed by clicking the "Deploy Network" button. The nodes of the network will be randomly scattered and connected, as shown on the main map. The communications of the network are directed from left to right, and nodes in the "uplink zone" (zone at the right

side of the map) are presumed to be in direct contact with the data collector. An alternative random scattering of nodes may be created by clicking the "Deploy Network" button again.

Once the network has been deployed, the simulation may be run by clicking "Start Simulation." The map will show vectors moving through the field and triggering sensors. The sensors may run out of power and drop out of the network, and eventually, all nodes will be powered down. The progress of the network can be monitored via the "Simulation Status" box. A new simulation may be run by stopping and restarting the simulation. The previous simulation may be reviewed by clicking the "Replay Simulation" button.

The simulation parameters used are:

- **Agents per event**: The amount of agents generated per event. An agent's basic purpose is to travel around the network, constantly updating nodes' routing tables with the shortest route available to a destination.
- **Agent TTL**: Agents have a TTL field, that limits the lifetime of the agent in the network, hence preventing indefinite looping of agents.
- **Query cycle**: The nodes generate queries which target events; these queries circulate in the network. When a node in the network receives a query, it checks to see if it has a route towards the target event, which is specified in the query. If there is a route, it forwards the query along the path. Otherwise, it sends the query to a random neighbor. Every time a node forwards the query, the query's TTL field is reduced, such that the query w ill be dropped when this value reaches zero.

IX. 1. Simulation Result

The network was flooded with queries to guarantee high delivery rate; however, additional N * (1000 – Q_f) sends were performed, where Q_f is the number of delivered queries. The average energy used for each query (in a network of 1000 nodes) was

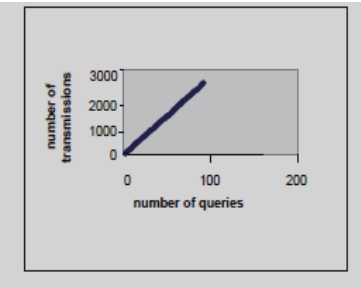


Fig 1: Simulation of 200 nodes with 5 agents per events.

This resulted in a 97:9% delivery rate
Equation 1: (E (q) +N*(1000-f/1000)) where $E(q)$ is the energy spent routing the queries. The average energy per query and the setup energy can be used to find the total energy utilized by the network to route Q queries as follows

Equation 2:
E=E(setup)+Q(E(q)+N*(1000-Qf/1000))

where *E* was set at 10*;* 50 and 100 events. The Agent TTL and Query TTL remained constant. The agents per event were set for the values of 5*;* 10*;* 50 and 100.

It should be noted that since Rumor routing uses data dissemination to send data from sources to sink, the energy of the network is depleted faster than some other protocols.

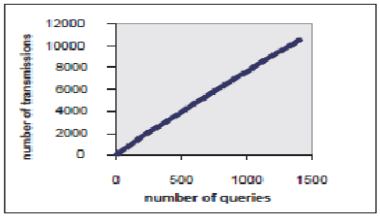


Fig 2: Simulation of 200 nodes with 100 agents per events. However, this resulted in only a 90% delivery rate.

Table 1: Simulation parameters values

Net work	Agent s Per Event	Agent TTL	Query Deliv ery	Cycle rate(%)
100	10	57	70	97.2%
200	18	30	24	97.9%
400	15	73	50	97.3%
600	28	78	80	97.2%
1000	31	100	80	98.3%

The Table 1 represents the parameters used in the simulations to determine delivery rates. The parameters given are found to obtain the optimum possible delivery rates for particular size networks. Although there is no set formula to determine the optimal values to use, Rumor routing has the ability to *tune* to a variety of different applications and network sizes.

It is important to compare the number of participating nodes in routing messages from source to sink for each of the routing protocols at hand. Since the lower amount of nodes participating in the routing would mean the lower the energy depletion of the network. From Figure 3, it is shown that SPIN has used 1000 nodes to send data from source to sink, while Rumor and SER used only 680 and 30 sensornodes respectively [1]. I can conclude that SPIN may not be suitable if the aim is to deploy the sensor network for long periods of time since the energy of the network would be depleted much faster. From these results, Rumor routing would work the best from small to medium scale networks.

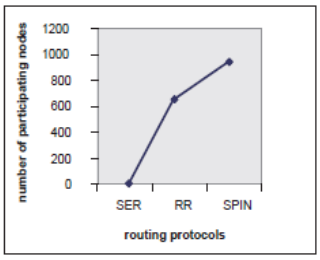


Fig 3: The average number of nodes participating in various routing protocols

Another important feature of any routing protocol is the time it requires to send a data from the source to the sink (see Figure 4). The shortest time was achieved with Rumor routing although jitter could not be measured directly for this protocol. The data has reached to sink on the average of 0:39 seconds in Rumor routing, while the SER protocol takes 0:73 seconds with about 0:02 seconds of jitter and SPIN takes 2:15 seconds for data to reach the sink . The results produced by the Rumor routing may possibly vary if the jitter can be properly measured

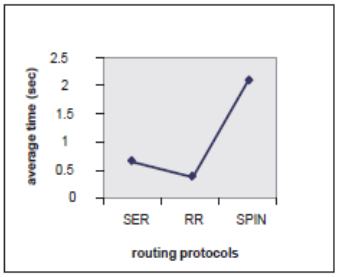


Fig 4: The average travel time of data from the source to the sink

X. Conclusion and future works.

This paper is compared the performances of three routing protocols, namely, Rumor routing, SER, and SPIN. SER is a protocol particularly suited to large scale networks due to its excellent efficiency, latency and jitter properties. The fact that SER does not require nodes to have unique IDs further strengthens the argument of its suitability to large scale networks. SPIN was found to perform better in smaller size networks because of its efficiency and high latency properties. The use of SPIN in large scale networks could potentially exhaust system resources in a much faster pace. Rumor routing is considered an alternative protocol to the various flooding protocols presented. The results have shown that it is an efficient protocol with a high delivery rate. It was also concluded that Rumor routing may be most suitable for networks with small to medium in size.

REFERENCES

[1] Akyildiz,I.F., and Su,W. "An Stream Enabled Routing (SER) Protocol for Sensor Networks", *Med-hoc-Net 2002*, September 2002.

[2] Awad, Abdalkarim and Sommer, Christoph and German, Reinhard and Dressler, Falko. [Virtual Cord Protocol (VCP): A Flexible DHT-like Routing Service for Sensor Networks]. 5th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2008), Atlanta, Georgia, USA, September 2008

[3] Eduardo Nakamura, Antonio A. F. Loureiro, Alejandro C. Frery. Information fusion for wireless sensor networks: Methods, models, and classifications, ACM Computing Surveys, Volume 39, Issue 3, Article 9, September 2007.

[4] Estrin, D., Intanagonwiwat, C., and Govindan, R. "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", *MobiCOM 2000*.

[5] Hill, J., Szewczyk, R.,Woo, A., Hollar, S., Culler, D., and Pister, K. "System architecture directions for networked sensors", *ACM ASPLOS IX*, 2000. http://pi4.informatik.uni-mannheim.de/~haensel/sn_book.Retrieved2006-08-29. http://sourceforge.net/projects/lecssim http://www.vs.inf.ethz.ch/publ/papers/wsn-designspace.pdf. http://www.wherifywireless.com

[6] Ratnasamy, Sylvia and Karp, Brad and Shenker, Scott and Estrin, Deborah and Govindan, Ramesh and Yin, Li and Yu, Fang [Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table]. ACM/Springer Mobile Networks and Applications (MONET), Special Issue on Wireless Sensor Networks, August 2003

[7] Romer, Kay; Friedemann Mattern (December 2004). "The Design Space of Wireless Sensor Networks". *IEEE Wireless Communications* **11** (6): 54–61. doi:10.1109/MWC.2004.1368897

[8] Savvides, A., Han, C., and Srivastave, M. "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors", *MobiCOM 2001*, pp. 166-179.

[9] Thomas Haenselmann (2006-04-05). *Sensornetworks*. GFDL Wireless Sensor Network textbook

Dr. M. Hemaltha completed MCA MPhil., PhD in Computer Science and Currently working as a Asst Professor and Head , dept of software systems in Karpagam University. Ten years of Experience in teaching and published Twenty seven paper in International Journals and also presented seventy papers in various National conferences and one international conferences Area of research is Data mining, Software Engineering, bioinformatics, Neural Network. Also reviewer in several National and International journals

V.Vasanthi was born on 28th,Jan 1984. She received her Bachelor of Computer Application from Nirmala College for women in 2005 and Master degree in Computer science from Hindusthan college of Arts and Science in 2008. She completed her M.Phil from karpagam University in 2009. Currently perusing Ph.d in computer science at karpagam university under the guidance of Dr.M.Hemalatha Head, Dept of Software System, Karpagam university, Coimbatore.

P. Nagarajan has presented six papers in National conferences and one paper in International Conference. I have completed MCA., M.Phil and currently working as a

Lecturer in Karpagam University. I have 2 years experience in teaching I am Pursuing Doctorate Degree in computer Science under the guidance of Dr.Hemalatha, Professor and Head, dept of software systems in Karpagam University. My area of research is Network Security

B.Bharathi born on 22nd,Feb 1982. Completed MCA.,M.Phil in Computer Science. Working as a Lecturer, Software System in Karpagam University. The Area of Research is on Network and currently Pursuing Ph.D in computer science Karpagam University under the guidance of Dr.M.Hemalatha.