Routing Protocols of Wireless Sensor Network

Raja Meena S and Prof. Poornima Talwai, Department of Electronics,
Ramrao Adik Institute of Technology
Nerul, Navi Mumbai

***Abstract*--Many advances have been made in sensor technologies which are as varied as the applications and many more are in progress. It has been reasonable to design and develop small size sensor nodes of low cost and low power. Wireless sensor networks (WSNs) are large networks made of a numerous number of sensor nodes with sensing, computation, and wireless communication capabilities. The reasons for using wireless network are cost effectiveness of network deployment and its applicability to environments where wiring is not possible or it is preferable solution compared with wired networks. The software tool Network Simulator (Version 2), widely known as NS-2, is described and used for the evaluation and comparison of selected Flat Routing Protocols of wireless networks on the basis of certain metrics with different network sizes under four different scenarios.**

***Index Terms*--*NS2, Wireless Sensor Network, Routing Protocols, Simulation, Flat Routing, Hierarchical Routing, Location-based Routing, throughput, delay.*

I. Introduction

With the recent technological advances in wireless communications, processor, memory, low power, highly integrated digital electronics, and micro electro mechanical systems (MEMS), it becomes possible to significantly develop small size, low power, and low cost multifunctional sensor nodes. These nodes are capable of wireless communications, sensing and computation. So, it is clear that wireless sensor network is the result of the combination of sensor techniques, embedded techniques, distributed information processing and communication mechanisms. A wireless sensor network (WSN) is a network that is made of hundreds or thousands of these sensor nodes which are densely deployed in an unattended environment with the capabilities of sensing, wireless communications and computations (i.e., collecting and disseminating environmental data).

Many different routing, power management and data dissemination protocols have been designed for Wireless Sensor Networks (WSNs), dependent on both the architecture of Wireless Sensor Network (WSN) and the applications that WSN is intended to support. These protocols support the practical existence of WSNs and efficiently make them an integral part of our lives in the real world. These protocols are different from conventional ones; in essence they need to support various unique requirements and constraints to make wireless sensor networks practically useful and operating. The requirements and constraints are introduced by factors such as: memory, small-size, low-power consumption, fault-tolerance, low-latency, scalability, adaptivity, and robustness. In this dissertation, different routing protocols of WSN are presented. When designing wireless networks and/or studying their behaviors under various conditions, software simulation tools are often used. The software tool Network Simulator (Version 2), widely known as NS-2, is described and used for the evaluation of Flat Routing WSN protocols and their performances are compared on the basis of Throughput, Delay and Packet loss with different network sizes under four different scenarios.

II. Wireless Sensor Network (WSN)

A wireless sensor network is an active research area with numerous workshops and conferences arranged each year. A Wireless Sensor Network (WSN) is a set of hundreds or thousands of micro sensor nodes that have capabilities of sensing, establishing wireless communication between each other and doing computational and processing operations [1]. Sensor networks have a wide variety of applications and systems with vastly varying requirements and characteristics. The sensor networks can be used in Military environment, Disaster management, Habitat monitoring, Medical and health care, Industrial fields, Home networks, detecting chemical, biological, radiological, nuclear, and explosive material etc. Deployment of a sensor network in these applications can be in random fashion (e.g., dropped from an airplane) or can be planted manually (e.g., fire alarm sensors in a facility). For example, in a disaster management application, a large number of sensors can be dropped from a helicopter. Networking these sensors can assist rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in the disaster area.

2.1 Communication Architecture for Wireless Sensor Network

We mentioned above that a wireless sensor network (WSN) is a network made of a numerous number of sensor nodes with sensing, wireless communications and computation capabilities. These sensor nodes are scattered in an unattended environment (i.e., sensor field) situated far from the user. Figure 1 represents the communication architecture for WSN [2].

The main entities that build up the architecture are:

1 The Sensor nodes that form the sensor network. Their main objectives are making discrete, local measurement about phenomenon surrounding these sensors, forming a wireless network by communicating over a wireless medium, and collect data and route data back to the user via sink (Base Station).

2 The Sink (Base Station) communicates with the user via internet or satellite communication. It is located near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the sink by a multi-hop infrastructure less architecture.

3 Phenomenon which is an entity of interest to the user to collect measurements about. This phenomenon is sensed and analyzed by the sensor nodes.

4 The User who is interested in obtaining information about specific phenomenon to measure/monitor its behavior.

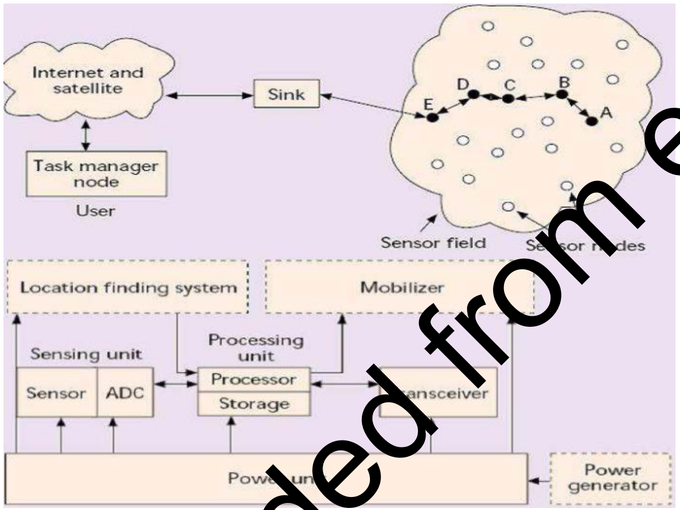

Figure 1: Sensor nodes scattered in a sensor field and the Components of a single sensor node [2]

2.2 Network Characteristics

As compared to the traditional wireless communication networks such as Mobile Ad hoc NETwork (MANET) and Cellular systems, wireless sensor networks have the following unique characteristics and constraints [3].

Dense sensor node deployment: Sensor nodes are usually densely deployed and can be several orders of magnitude higher than that in a MANET.

Battery-powered sensor nodes: Sensor nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to change or recharge the batteries. Sensors nodes are having highly limited energy, computation, and storage capabilities.

Self-configurable: Sensor nodes are usually randomly deployed and autonomously configure themselves into a communication network.

Unreliable sensor nodes: Sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.

Data redundancy: In most sensor network applications, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

Application specific: A sensor network is usually designed and deployed for a specific application. The design requirements of a sensor network change with its application.
Many-to-one traffic pattern: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.
Frequent topology change: Network topology changes frequently due to the node failures, damage, addition, energy depletion, or channel fading.
QoS support: In sensor networks, different applications may have different Quality- of-Service (QoS) requirements in terms of delivery latency and packet loss.

2.3 Need for routing protocol

Routing in sensor networks is very challenging due to several characteristics [2] that distinguish them from contemporary communication and wireless ad-hoc networks. First of all, it is not possible to build a global addressing scheme for the deployment of sheer number of sensor nodes. Therefore, classical IP-based protocols cannot be applied to sensor networks. Second, in contrary to typical communication networks almost all applications of sensor networks require the flow of sensed data from multiple regions (sources) to a particular sink. Third, generated data traffic has significant redundancy in it since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and band width utilization. Fourth, sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage and thus require careful resource management. Due to such differences, many new algorithms have been proposed for the problem of routing data in sensor networks. These routing mechanisms have considered the characteristics of sensor nodes along with the application and architecture requirements. The design challenges in sensor networks involve the following main aspects.
Limited energy capacity: Since sensor nodes are battery powered, they have limited energy capacity. Energy poses a big challenge for network designers in hostile environments, for example, a battlefield, where it is impossible to access the sensors and recharge their batteries. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime, and hence prolong the network lifetime while guaranteeing good performance overall.
Limited hardware resources: In addition to limited energy capacity, sensor nodes have also limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks.
Sensor locations: Another challenge that faces the design of routing protocols is to manage the locations of the sensors. Most of the proposed protocols assume that the sensors either are equipped with Global Positioning System (GPS) receivers or use some localization technique to learn about their locations.
Massive and random node deployment: Sensor node deployment in WSNs is application dependent and can be either manual or random which finally affects the performance of the routing protocol. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region.
Network characteristics and unreliable environment: A sensor network usually operates in a dynamic and unreliable environment. The topology of a network, which is defined by the sensors and the communication links between the sensors, changes frequently due to sensor addition, deletion, node failures, damages, or energy depletion. Also, the sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. Therefore, routing paths should consider network topology dynamics due to limited energy and sensor mobility as well as increasing the size of the network to maintain specific application requirements in terms of coverage and connectivity.
Diverse sensing application requirements: Sensor networks have a wide range of diverse applications. No network protocol can meet the requirements of all applications. Therefore, the routing protocols should guarantee data delivery and its accuracy so that the sink can gather the required knowledge about the physical phenomenon on time.
Scalability: Since the numbers of sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.
Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.
Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

Fault tolerance: Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self-testing, self-calibrating, self-repairing and self-recovering.

III. CLASSIFICATION OF ROUTING PROTOCOLS

There are different ways by which we can classify the routing protocols [3]. According to network structure, these routing protocols can be classified as flat, hierarchical and location-based protocols. In flat-based routing, all nodes are assigned the same roles or functionalities. In hierarchical-based routing, nodes will play different roles or functionalities, aiming at routing techniques clustering the nodes with different roles so that the heads of the cluster can do some data aggregation in order to save power. In location based routing, sensor nodes' positions are exploited to route the data to specific regions other than the whole network.In flat-based routing, all nodes are assigned the same roles or functionalities. In hierarchical-based routing, nodes will play different roles or functionalities, aiming at routing techniques clustering the nodes with different roles so that the heads of the cluster can do some data aggregation in order to save power, while in location based routing, sensor nodes' positions are exploited to route the data to specific regions other than the whole network.

Typical flat routing algorithm includes Flooding algorithm, Gossiping, Directed Diffusion (DD), Sequential Assignment Routing (SAR), Sensor Protocols for Information via Negotiation (SPIN), Cougar, etc.
Hierarchical routing protocols mainly include Low Energy Adaptive Clustering Hierarchy (LEACH), Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN), Power-Efficient GAthering in Sensor Information Systems (PEGASIS), etc.
Location-based protocols includes Geographic Adaptive Fidelity (GAF), Geographic and Energy Aware Routing Protocol (GEAR), etc

IV. FLAT ROUTING

The first category of routing protocols is the multihop flat routing protocols. In flat networks, each node typically plays the same role and sensor nodes collaborate together to perform the sensing task. Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. SPIN [2] [3] is the first data centric protocol, which considers data negotiation between nodes in order to eliminate redundant data and save energy. Later, Directed Diffusion [5] [6] has been developed and has become a breakthrough in data-centric routing. Then, many other protocols have been proposed either based on Directed Diffusion or following a similar concept. In this section, description of these protocols in detail and their key ideas are given.

A. Sensor Protocols for Information via Negotiation (SPIN)

Sensor Protocols for Information via Negotiations (SPIN) [3] is a family of adaptive protocols for WSNs. Their design goal is to avoid the drawbacks of flooding protocols mentioned above by utilizing data negotiation and resource adaptive algorithms. SPIN is designed based on two basic ideas:
1 to operate efficiently and to conserve energy by sending metadata (i.e., sending data about sensor data instead of sending the whole data that sensor nodes already have or need to obtain)
2 nodes in a network must be aware of changes in their own energy resources and adapt to these changes to extend the operating lifetime of the system.
SPIN has three types of messages as shown in Fig.2. namely, ADV, REQ, and DATA.
ADV: when a node has data to send, it advertises via broadcasting this message containing meta-data (i.e., descriptor) to all nodes in the network.
REQ: an interested node sends this message when it wishes to receive some data.
DATA: Data message contains the actual sensor data along with meta-data header.
SPIN is based on data-centric routing where the sensor nodes send ADV message via broadcasting for the data they have and wait for REQ messages from interested sinks or nodes. The semantics of SPIN's meta-data format is

application dependent and not supported by SPIN. In another words, SPIN uses application specific meta-data to name the sensed data.

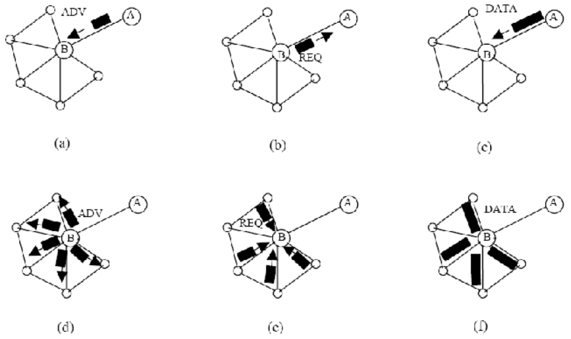

Figure 2: Data Transmission in SPIN [3]

Advantages
1 Solving the problems associated with classic flooding protocols, and
2 Topological changes are localized.
Disadvantages
1 Scalability, SPIN is not scalable,
2 If the sink is interested in too many events, this could make the sensor nodes around it deplete their energy and
3 SPIN's data advertisement technique cannot guarantee the delivery of data if the interested nodes are far away from the source node and the nodes in between are not interested in that data.

The SPIN family of protocols includes many protocols. The main two protocols are called SPIN-1 and SPIN-2, which incorporate negotiation before transmitting data in order to ensure that only useful information will be transferred. Also, each node has its own resource manager which keeps track of resource consumption, and is polled by the nodes before data transmission. The SPIN-1 protocol is a 3-stage protocol, as described above. An extension to SPIN-1 is SPIN-2, which incorporates threshold-based resource awareness mechanism in addition to negotiation. When energy in the nodes is abundant, SPIN-2 communicates using the 3-stage protocol of SPIN-1. However, when the energy in a node starts approaching a low energy threshold, it reduces its participation in the protocol, i.e., it participates only when it believes that it can complete all the other stages of the protocol without going below the low-energy threshold.

B. Directed Diffusion

Directed diffusion is another data dissemination and aggregation protocol. It is a data-centric and application aware routing protocol for WSNs. It aims at naming all data generated by sensor nodes by attribute-value pairs [4]. In order to construct the route between the sink (inquirer) and the sensors that interest to the sink's request, there are four stages [5];

1. Interest propagation,
2. Gradient setup,
3. Reinforcement and
4. Data delivery.

Below is a detailed description for each stage:

Interest propagation: When a sink detects an event, it initiates the interest messages and floods them to all nodes in the network. These messages are exploratory messages indicating the nodes with matching data for the specific task. During this stage, the sink periodically broadcasts the interest message. Once the interest message is received, each sensor node saves it in an interest cache. After that, the nodes flood this message to the other nodes until the node that is interested in this interest message is reached as shown in Figure 3(a).

Gradient setup: Based on local rules, different techniques are used in gradient setup. For example, the nodes with highest remaining energy could be chosen when setting up the gradient. During the interest propagation through the network, the gradients from source back to sink will be setup. A node becomes a source node if its observation matches the interest message and sends its data through the gradient path back to the sink as shown in Figure 3(b).

Reinforcement: During the gradient setup phase, many paths have formed from the source to the sink. This means the source can send the data to the sink through multiple routes. However, as shown in Figure 3(c), the sink reinforces one specific path by resending the same interest through the specified path, which is chosen based on many rules, like the best link quality, number of packets received from a neighbor or lowest delay. Along this path, each node just forwards the reinforcement to its next hop. Finally, during this phase, the sink could select multiple paths in order to provide multi-path delivery.

Data delivery: After the reinforcement phase, as shown in Figure 3(d), the route between the source and the sink has been constructed and the data is ready for transmission.

Directed diffusion assists in saving sensors' energy by selecting good paths by caching and processing data in-network since each node has the ability for performing data
aggregation and caching. On the other hand; Directed diffusion has its limitations such as, implementing data aggregation requires deployment of synchronization techniques which is not realizable in WSNs. Also, the overhead in data aggregation involves recording information. These two drawbacks may contribute to the cost of sensor node, which is not desired. In addition, the naming schemes used in Directed Diffusion are application dependent and each time should be defined a priori.

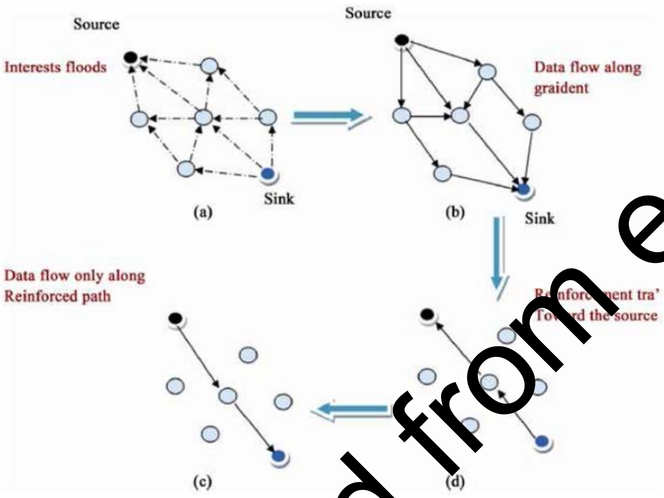

Figure 3: Operation of the directed diffusion protocol [5]

Advantages
1. It is designed to retrieve data aggregates from a single node.
2. Data is named by attributed value pairs.
3. It works well in multipurpose wireless sensor net-works and in sensor networks that query.
4. Unlike other routing algorithms, in Directed Diffusion more than one sink can make queries and receive data at the same time; hence simultaneous queries could be handled inside a single network.
5. The interests/queries are issued by the sink not by the sources, and only when there is a request. Moreover, all communication is neighbor-to-neighbor, which removes the need for addressing and permits each node to aggregate data. As a result, both points contribute to reduce energy consumption.
6. It provides application-dependent routes based on the interests of the user.
7. It requires neither a global node addressing mechanism nor a global network topology. Moreover, the routes are formed only when there is an interest. As a result, it achieves energy efficiency.
Disadvantages
1. It is generally based on a flat topology. Hence, scalability and congestion (especially in the nodes that are near to the sink) problems exist.
2. An overhead problem occurs at the sensors during the matching process for data and queries.
3. In Directed Diffusion, the initial interest contains a low data rate. However, an important overhead is caused during flooding operation of interest propagation phase.

4. Due to the flooding required to propagate the interest on each node, it is not optimized for energy efficiency and need high amounts of memory to store interest gradients and received messages.
5. It mostly selects the shortest path between the source and the destination, which leads to quick death of nodes on that path.
Directed diffusion differs from SPIN in two aspects. First, directed diffusion issues on demand data queries as the BS send queries to the sensor nodes by flooding some tasks. In SPIN, however, sensors advertise the availability of data allowing interested nodes to query that data. Second, all communication in directed diffusion is neighbor-to-neighbor with each node having the capability of performing data aggregation and caching. Unlike SPIN, there is no need to maintain global network topology in directed diffusion. However, directed diffusion may not be applied to applications (e.g., environmental monitoring) that require continuous data delivery to the BS. This is because the query- driven on demand data model may not help in this regard. Moreover, matching data to queries might require some extra overhead at the sensor nodes.

C. Cougar

A data-centric protocol that views the network as a huge distributed database system is proposed in [6]. The main idea is to use declarative queries in order to abstract query processing from the network layer functions such as selection of relevant sensors etc. and utilize in-network data aggregation to save energy. The abstraction is supported through a new query layer between the network and application layers. Cougar proposes architecture [3] for the sensor database system where sensor nodes select a leader node to perform aggregation and transmit the data to the gateway (sink). The architecture is depicted in Figure 4. The gateway is responsible for generating a query plan, which specifies the necessary information about the data flow and in-network computation for the incoming query and send it to the relevant nodes. The query plan also describes how to select a leader for the query. The architecture provides in-network computation ability for all the sensor nodes. Such ability ensures energy efficiency especially when the number of sensors generating and sending data to the leader is huge.
Although Cougar provides a network-layer independent solution for querying the sensors, it has some drawbacks:
First of all, introducing additional query layer on each sensor node will bring extra overhead to sensor nodes in terms of energy consumption and storage.
Second, in network data computation from several nodes will require synchronization, i.e. a relaying node should wait every packet from each incoming source, before sending the data to the leader node.
Third, the leader nodes should be dynamically maintained to prevent them from failure.

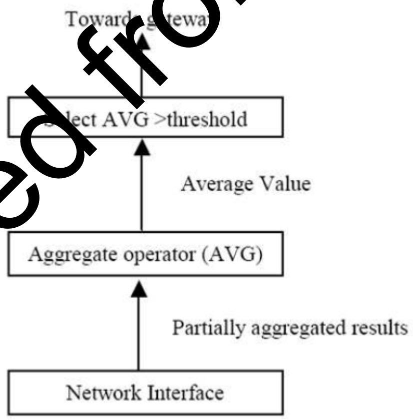

Figure 4: Query plan at a leader node [3]

V. System Implementation

Network Simulator 2 (NS-2) [7] is one of the most popular non-specific network simulators and supports a wide range of protocols in all layers. Following are the steps [8] for writing a script in NS-2.
1. Create a new simulator object.
2. Turn on tracing [Open your own trace files].
3. Create network (physical layer).
4. Create link and queue (data-link layer).
5. Define routing protocol.

6. Create transport connection (transport layer).
7. Create traffic (application layer).
8. Insert errors.

Table 5.1 gives the input parameters that are used in our simulation scenario along with their range values.

Input Simulation Parameters used are as follows:

Parameters	**Details**
Node Deployment	Fixed/Random
Initial Energy	20 joules
Transmitting Power	0.mW
Receiving Power	0.2mW
Network Area	300m X 300m
No of Nodes	20-120
Range of each node	15 m radius
Packet size	500/1000 bytes
Bandwidth	3 Mbps
Traffic Interval	0.005 sec

PARAMETERS USED FOR PERFORMANCE EVALUATION

In order to check the performance of protocols in terms of its effectiveness there are different metrics to be used. In this study, throughput, packet loss and End-to-End delay are used for the evaluation of protocols. The reasons behind the selection of these metrics are their importance in any data communication network. Furthermore, any protocol needs to be evaluated against these metrics to check its performance. In order to check the protocol effectiveness in finding routes towards destination, it is interesting to check how much packets it sends successfully. This metric used to measure the internal algorithms efficiency of routing protocol. The larger is routing overhead of a protocols (in packets/ bytes), larger will be the wastage of the resources (bandwidth). Thus throughput shows protocols successful deliveries for a time. This means the higher is throughput the better is protocol performance. Also lower is the delay, finer is the protocol performance.

Throughput:

Throughput is the rate of successfully delivered data per second to individual destinations during network simulation. Throughput is associated with the efficiency of the protocol. A low delay in the network translates into higher throughput. Delay is one of the factors effecting throughput, other factors are routing overhead, area and bandwidth. Throughput gives the fraction of the channel capacity used for useful transmission and is one of the dimensional parameters of the network.

Packet Loss

Packet loss is the failure of one or more transmitted packets to arrive at their destination. The effects of severe packet loss are

1. It produces errors
2. It can cause severe mutilation of received data or even complete absence of a received signal.

The causes of packet loss include inadequate strength at the destination, excessive system noise or overburdened network nodes.

End-to-End Delay

The term end-to-end delay refers to the time taken by a packet to be transmitted across a network from source node to destination node that includes all possible delays caused during route discovery latency, queue in data packet transmission, retransmission delays, propagation and transfer times. The protocol which shows higher end-to-end delay means the performance of the protocol is not good due to network congestion. The lower value of end -to-end delay means the better performance of the protocol.

RESULTS AND ANALYSIS

In this project, four test scenarios are taken. In the first scenario, three Flat routing protocols are implemented with fixed nodes. Simulation results are evaluated and compared on the basis of throughput, delay and packet loss with different no of nodes.

In the second scenario, Protocols are implemented with mobile nodes and the results are evaluated. In the third scenario, Protocols are simulated with different packet sizes. In the fourth scenario, simulation is done under the fixed deployment of nodes.

Scenario I: Fixed Nodes

The nodes in WSNs may be static or dynamic. Most of the routing protocols assume that the sensor nodes and the base

stations are fixed i.e., they are static. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that is, the sensor nodes are deployed randomly, and after deployment their positions do not change.

Network Throughput

SPIN uses the shortest path algorithm. As the no of nodes increases, the node links to shortest path increases. SPIN operation will transport almost zero redundant data packet and decrease the operation of sending wasted data packets.

In DD, with larger sensor nodes, each node transmits the same packet multiple times, once to each neighbor. Diffusion is less impacted by this because it performs in-network suppression of identical data. Finally with large sensor field, the event delivery ratio falls. This can be attributed to suppression. Nodes that links to the shortest path nodes and the gradient links use a lot of energy for transmitting and receiving packet. Thus, they generate overhead and reduce the life time of the nodes in the network. When this occurs, the topology and links for every node will change. The distance for transmitting and receiving packet will be a bit larger and will consume a lot of energy.

In Cougar, Dynamic selection of aggregation points minimizes overall data movement. The nested query localizes data traffic near the triggered event rather than sending it to the sink, thus reducing network traffic and latency.

Data aggregation reduces the no of transmissions.

Figure 5.a shows the Throughput for Fixed Nodes of the three protocols.

End to End Delay

Delay value for SPIN is less because it uses the shortest path algorithm. As the no of nodes increases, the node links to shortest path increases. SPIN operation will transport almost zero redundant data packet and decrease the operation of sending wasted data packets.

In DD, the Reinforcement rules find the low delay path. In-Network processing can reduce data traffic. The larger network has longer alternate paths. These alternate paths are pruned by negative reinforcement because they consistently deliver events with higher latency.

In Cougar, in network data computation from several nodes will require synchronization, i.e. a relaying node should wait every packet from each incoming source, before sending the data to the leader node. The intermediate nodes suppress duplicate data by simply not propagating it. The intermediate nodes simply delay and aggregate data from multiple sensor nodes.

Figure 5.b shows the Delay for Fixed Nodes of the three protocols.

Packet Loss

SPIN protocol has very less dead nodes. SPIN will start with advertise its interest, and then waiting for a request from any node before start transmitting data again. SPIN nodes negotiate with each other before transmitting data. Negotiation helps to ensure that only useful information will be transferred. Packet loss for SPIN remains constant even though the no of nodes increases. SPIN's data advertisement technique cannot guarantee the delivery of data if the interested nodes are far away from the source node and the nodes in between are not interested in that data.

In DD, One would expect that DD would expend energy to find alternate paths. But several reinforced paths- high-quality paths are kept alive in normal operation. Thus DD does not need to do extra work. In smaller sensor fields, it can suppress duplicates. In larger sensor fields, less aggregation. In the absence of negative reinforcement, more paths are used and without suppression more copies of data are sent, resulting in subsequent delays.

In Cougar, packet loss is less due to the query based approach which reduces the irrelevant data transfers and also the aggregate operator directly sends its data to the BS.
Figure 5.c shows the Packet Loss for Fixed Nodes of the three protocols.

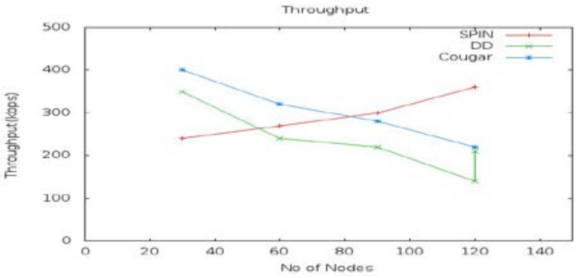

Figure 5.a Throughput for Fixed Nodes

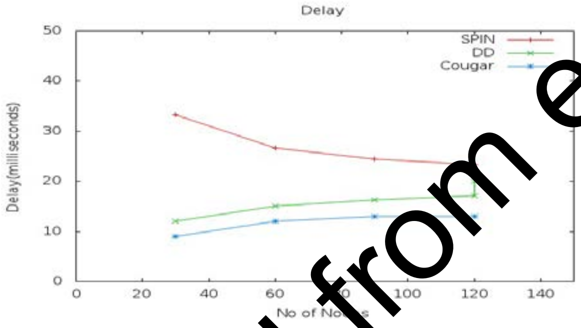

Figure 5.b Delay for Fixed Nodes

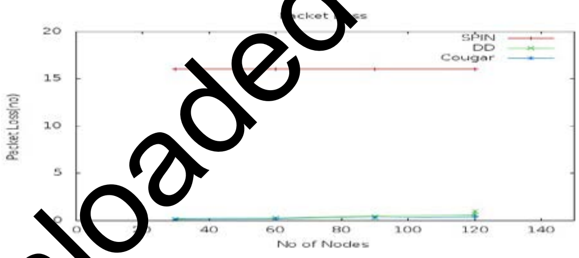

Figure 5.c Packet loss for Fixed Nodes

Scenario II: MobileNodes

In mobile wireless sensor networks, the sensor nodes can move on their own, and after deployment, they can interact with the physical environment by controlling their own movement. Advances in robotics have made it possible to develop such mobile sensors which are autonomous and have the ability to sense, compute, and communicate like static sensors. The prime difference between static and mobile WSNs is that mobile nodes are able to reposition and organize themselves in the network, and after initial deployment, the nodes spread out to gather information. Mobile nodes can communicate with one another when they are within the range of each other, and only then they can exchange their information gathered by them. In this scenario, movement of node is performed with the speed of 15m/s after the interval of 0.5 sec.

Due to the mobility of nodes, increased link failures in SPIN protocol results in reduced throughput and higher packet losses. The path has to be set up again from the beginning.

DD has good latency properties and not delayed because of failure of links. The other paths stored in the cache can be used for further routing.

In Cougar, the mobility nodes will be traced by its corresponding aggregate operator and hence not much affected by the mobility of nodes.
Figure 6.a,6.b and 6.c shows the Throughput, Delay and Packet Loss for Mobile Nodes of the three protocols respectively.

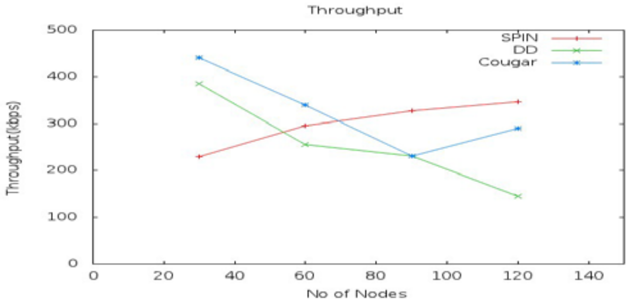

Figure 6.a Throughput for Mobile Nodes

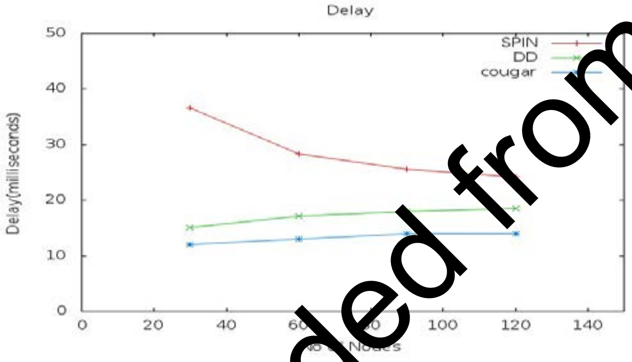

Figure 6.b Delay for Mobile Nodes

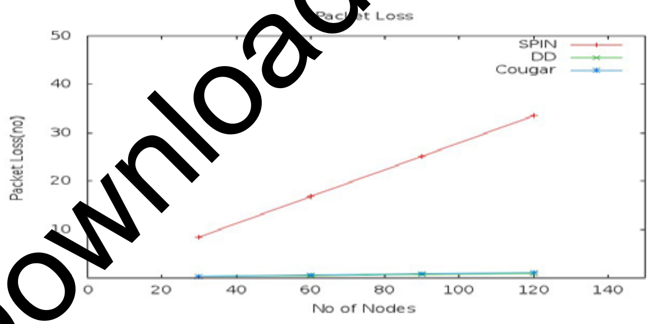

Figure 6.c Packet Loss for Mobile Nodes

Scenario III: Different Packet Sizes

It is a known fact in WSN that the data packet size could directly affect the reliability and the quality of the communication between the wireless nodes. Hence throughput performance is affected by the packet size.

As the packet size increases, more bytes of data will be transmitted resulting in higher throughput. Here we have considered two different packet sizes of 500 bytes and 1000bytes and results are obtained showing higher throughput for higher value of packet size.
Figure 7.a and 7.b shows the Throughput for Packet size of 500 and 1000 bytes respectively of the three protocols.

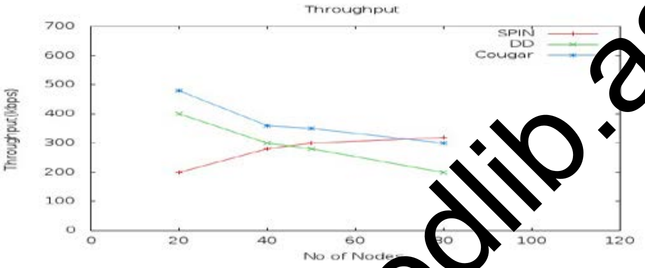

Figure 7.a Throughput for Packet size =500 bytes

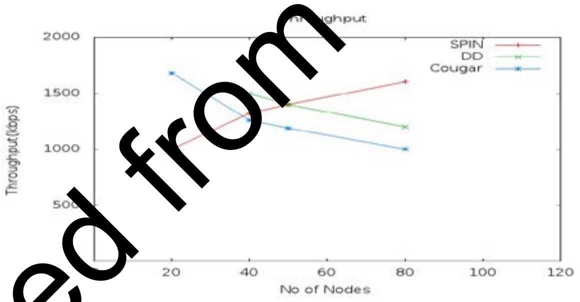

Figure 7.b Throughput for Packet size =1000 bytes

Scenario IV: Fixed Deployment of Nodes
There are two deployment strategies mentioned in the literature which are deterministic and random. In deterministic deployment, sensors are manually placed. The main deployment objectives of any sensor network are coverage, lifetime, and routing. In this scenario, node positions i.e, x and y co-ordinates are entered manually and kept as constant for all the protocols and the results are obtained.
Under the same conditions, i.e., with the same position of nodes, Cougar and DD are showing better performance in terms of throughput, delay and Packet loss.
Figure 8.a. 8.b and 8.c shows the Throughput, Delay and Packet loss respectively for Fixed Deployment of Nodes of the three protocols.

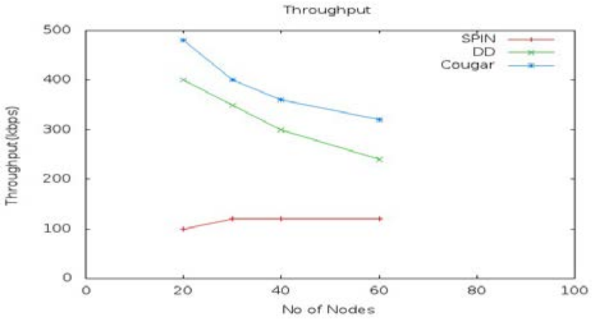

Figure 8.a Throughput for Fixed Deployment of nodes

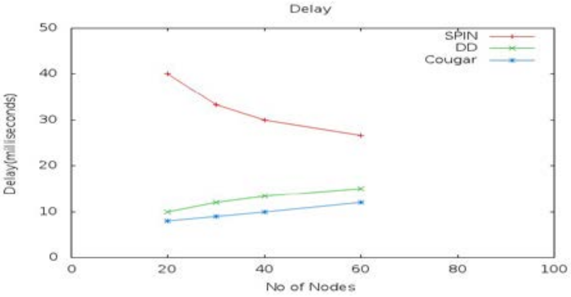

Figure8.b Delay for Fixed Deployment of nodes

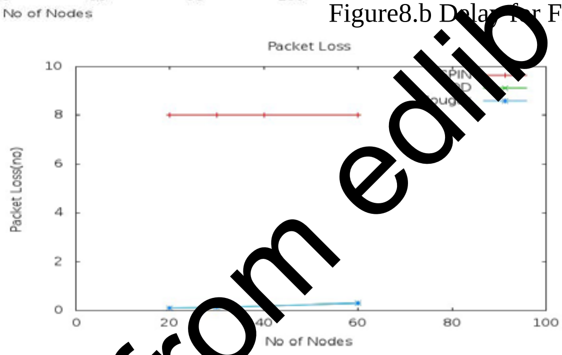

Figure 8.c Packet Loss for Fixed Deployment of nodes

CONCLUSION

The past few years have witnessed a lot of attention on routing for wireless sensor networks and introduced unique challenges compared to traditional data routing in wired networks. Routing in sensor networks is a new area of research. Since sensor networks are designed for specific applications, designing efficient routing protocols for sensor networks is very important. In this dissertation, a comprehensive survey of routing techniques in wireless sensor networks is given. Depending on the network structure, these protocols are categorized as Hierarchical, Flat and Location based. Flat Routing Protocols include SPIN, DD and Cougar.

Since the sensor networks are application specific, it cannot be said that any particular protocol is better than other. We can compare these protocols with respect to some parameters only. For designing wireless networks and for studying their behavior under various conditions, software simulation tool, NS 2 is used. Performance evaluation and analysis of Flat Routing Protocols has been done with different network sizes under four scenarios with respect to parameters such as throughput, packet loss and end-to-end delay.

Due to the aggregation and reinforcement rules, DD and Cougar are showing better performance than SPIN. Redundancy is reduced by means of suppression in case of DD and Cougar and by meta-data negotiation for SPIN.

SPIN's data advertisement technique cannot guarantee the delivery of data. SPIN protocol is inappropriate when there is a need for constant monitoring by the sensor network. Whereas Cougar provides the facility of constant monitoring. Thus DD and cougar are showing better overall performance than SPIN.

.

REFERENCES

[1] Shio Kumar Singh, MP Singh and D K Singh, "Routing Protocols in Wireless Sensor Networks - A Survey", International Journal of Computer Science and Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[2] Yazeed Al-Obaisat and Robin Braun," On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management", Institute of Information and Communication Technologies University of Technology, Sydney.

[3] Jamal N. Al-Karaki and Ahmed E. Kamal,"Routing Techniques in Wireless Sensor Networks: A Survey", ICUBE initiative of Iowa State University, Ames.

[4] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed Diffusion for Wireless Sensor Networking", IEEE/ACM Transactions on Networking, Feb. 2003.

[5] Neha Singh, Prof.Rajeshwar Lal Dua and Vinita Mathur, "Wireless Sensor Networks: Architecture, Protocols, Simulator Tool", International Journal of Advanced Research in Computer Science and Software Engineering, May 2012.

[6]Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks ", University of Maryland, Baltimore.

[7] Almargni Ezreik and Abdalla Gheryani," Design and Simulation of Wireless Network using NS-2", 2nd International Conference on Computer Science and Information Technology, Singapore, April 2012.

[8] Kristoffer Clyde Magsino and H. Srikanth Kamath," Simulations of Routing Protocols of Wireless Sensor Networks", World Academy of Science, Engineering and Technology, 2009.